VANET 을 위한 CRT 기반 메시지 인증 기법의 메시지 신선성 분석

정엘리야*, (교신저자) 김현성*,**
*경일대학교 컴퓨터사이언스학부, **말라위대학교 수학과

*elliya0407@gmail.com, **kim@kiu.ac.kr

Cryptanalysis on Message Freshness for CRT-based Message Authentication Scheme over VANET

Elliya Jung*, Hyunsung Kim*,**
*School of Computer Sci., Kyungil Univ., **Mathmatical Sci. Dept., Univ. of Malawi

요 약

VANET(Vehicular ad-hoc network) 기술의 발전과 빠르게 성장하는 무선 통신 기술로 보안의 중요도가 높아지고 있다. 특히, VANET 은 원활한 교통, 자율주행 등을 위한 서비스를 제공하므로 운전자와 보행자의 안전을 위해 메시지 인증, 프라이버시 보호기능 등이 반드시 선행되어야 한다. 최근 Bong 등은 RSU 에 의존적이지 않은 CRT-기반의 그룹키를 이용한 메시지 인증기법을 제안하였다. 하지만 본 논문에서는 Bong 등의 기법이 재전송공격에 취약함을 보이고 이를 통해 메시지 신선성을 제공이 인증 기법에 있어서 왜 중요한지를 살펴본다. 또한, Bong 등의 기법에 존재하는 문제를 해결하기 위한 해결 방안의 개요를 제시한다.

Ⅰ. 서 론

VANET(Vehicular Ad-Hoc Network)은 MANET (Mobile Ad-Hoc Network)의 한 형태로 차량으로 구성된 차량 간 통신을 위한 네트워크이다[1]. 그룹서명 기반 VANET 을 위한 다양한 보안과 프라이버시를 위한 연구가 진행되었다[2-3]. 특히, VANET 에서 사용되는 무선 통신의 특성으로 인해 VANET 의 메시지 교환은 악의적인 공격자에 의해 가로채기, 수정 및 복제와 같은 보안 위험에 노출될 수 있다. 그러므로 인증과 메시지 무결성을 위한 기법은 VANET 의 보안 및 안전성 제공에 있어서 매우 중요하다[4]. 최근에 Bong 등은 CRT 기반 그룹키를 이용한 메시지 인증 기법을 제안하였다[2]. 하지만, 본 논문에서는 Bong 등의 메시지 인증 기법이 메시지의 신선성(Freshness)을 제시하지 못하는 문제를 도출한다.

Ⅱ. Bong 등의 CRT 기반 메시지 인증기법

Bong 등의 시스템 모델은 TA(Trusted Authority), 키 서버(KS, Key Server), RSU(Road Side Unit), 차량(vehicle)으로 구성된다. 각 차량과 RSU 는 네트워크 상에 배포되기 전 TA에게 사전 등록 과정을 거친다.

이들의 사전등록은 안전한 네트워크상에서 수행됨을 가정하고, 고속도로와 같이 그룹의 멤버가 언제든 바뀔 수 있는 상황을 가정한다.

Bong 등의 인증 기법은 그룹 가입 요청 및 인증, 그룹 생성 및 시스템 초기화, 메시지 전송 및 검증, 그룹 구성의 변경, 신원 확인 및 차량 철회 단계로 구성된다[2]. 각 단계는 다음과 같다.

그룹 가입 요청 및 인증

1) 차량은 TA 의 공개키로 그룹 가입 요청 메시지를 암호화하고 RSU 를 통해 TA 에게 전송한다. 2) TA 는 자신의 비밀키로 복호화한 후 차량의 공개키로 복호화 후 차량 정보를 확인 및 저장하고, KS 에게 키 분배를 요청한다.

그룹 생성 및 시스템 초기화

1) KS 는 큰 소수 p 를 선택하고, 예비 그룹을 위하여 곱셈군 Z_p^* 에서 n 대의 차량을 수용할 수 있는 합동 시스템의 비밀 키(CK_i)들을 선택하고 초기화 한다. 2) KS 는 각 차량의 비밀키(CK_i), 익명아이디(PID_{vi}) 및 그룹아이디(ID_{Gj})를 차량의 공개키로 암호화하여 각 차량에 전송한다. 익명아이디는 중복을 허용하여 비연결성을 보장한다. 3) KS 는 그룹키로 사용될 값(GK_j)을 랜덤하게 선택하고(단, $GK_j < \forall CK_i$), 각 차량이 그룹키를 계산할 수 있도록 하는 초기값(GK_{js})을 계산한 후 이 값을 브로드 캐스팅한다.

메시지 전송 및 검증

1) 각 차량은 그림 1 과 같이 그룹키를 검증하고, 메시지와 그룹키를 이용한 HMAC 과 메시지의 추적을 위해 자신의 ID(ID_{vi})를 개인키(SK_{vi})로 암호화한 값을 첨부한다. 3) 메시지를 수신한 차량도 메시지와 그룹키를 이용하여 HMAC 을 생성 및 검증 후 메시지를 수용한다.

그룹 구성의 변경

KS 는 변경대상이 되는 차량에 해당하는 var_i 값을 더하거나 빼서 μ' 를 계산하고 그룹 생성 및 초기화 과정을 반복한다.

신원 확인 및 차량 철회

1) 거짓 메시지를 받은 차량은 이를 KS 에게 전송하고, KS 는 ID_{Gj} 와 PID_{vi} 를 이용하여 실제 아이디들을 검색하여 TA 의 공개키로 암호화하여 전송한다. 2) TA 는 자신의 비밀키로 복호하고, 신원을 확인후 KS 에게 확인

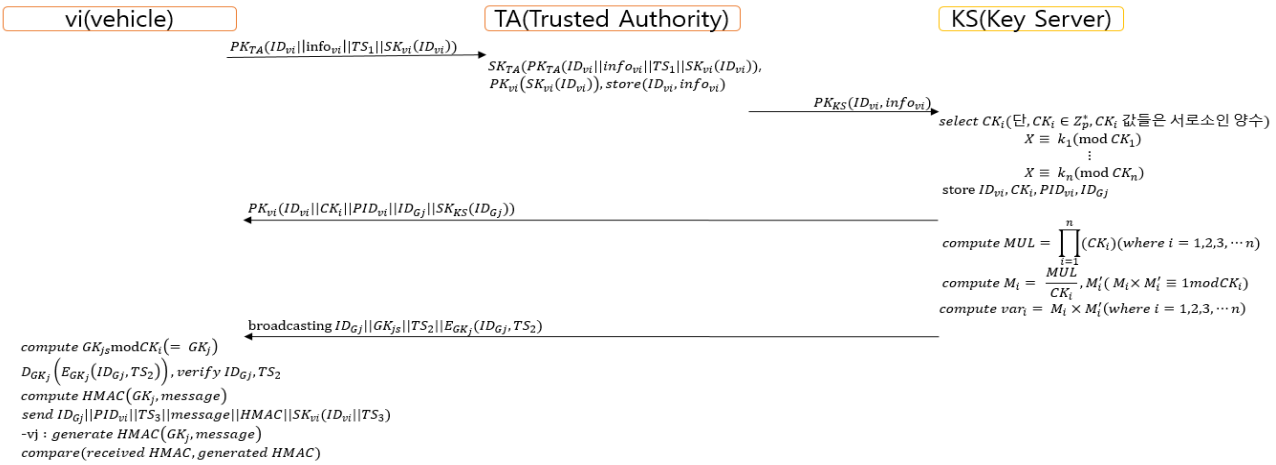

그림 1. Bong 등의 CRT 기반 그룹키를 이용한 메시지 인증기법

된 차량을 전송한다. 3) KS 는 차량(ID_{vi})을 그룹에서 제외시킨 뒤, 새로운 그룹키를 이용하여 새로운 초기값을 계산하여 브로드캐스팅 한다. 4) j 번째 그룹에 속한 다른 차량들은 새로운 초기값을 이용하여 새로운 그룹키를 생성한다.

Ⅲ. Bong 등의 인증 기법에 대한 안정성 분석

Bong 등의 기법에 대한 안전성 분석을 위해 본 장에서는 재전송 공격, 위장공격, 서비스거부 공격의 개요와 이에 따른 안전성을 분석한다. 실제 공격에 앞서 공격자들은 네트워크 트래픽을 수집하여 분석하는 스니핑 등의 기술을 이용해 정보를 획득할 수 있다고 가정한다. 암호, 서명 알고리즘은 안전하다고 가정한다.

3.1 재전송 공격

공격자가 네트워크 참여자들 사이의 통신을 수집한 후 데이터를 복사하고 재전송하여 정당한 사용자로 위장하는 공격이다. 공격자는 네트워크에서 그룹 가입 요청 및 인증 메시지인 2) $\text{TA} \rightarrow \text{KS} : PK_{KS}(ID_{vi}, info_{vi})$를 도청한 것으로 가정한다. 키 분배 요청 메시지는 세션마다 동일한 메시지를 전송하므로 공격자는 이전에 획득한 메시지를 재사용 할 수 있어서 재전송 공격에 취약하다.

3.2 위장 공격

공격자가 정당한 임의의 네트워크 참가자인 것처럼 위장하는 공격이다. 그룹 가입 요청 및 인증 메시지 2) $\text{TA} \rightarrow \text{KS} : PK_{KS}(ID_{vi}, info_{vi})$ 를 도청한 것으로 가정한다. KS 는 메시지의 송신자가 진정한 TA 임을 확인할 수 없고, 공개키의 특성상 누구나 획득할 수 있는 키이므로 임의의 차량(ID_{vi}), 차량정보($info_{vi}$)를 KS 의 공개키로 암호화하고, KS 에게 전송함으로써 공격자는 KS 에게 그룹의 키 분배를 요청할 수 있게 된다. 또한, 신원 확인 및 차량 철회 메시지 4) $\text{TA} \rightarrow \text{KS} : \text{send}\ PK_{KS}(ID_{vi})$를 도청했다고 가정한다. 공격자가 정당한 참가자의 차량을 KS 의 공개키로 암호화하여 전송한다면 KS 는 메시지의 송신자가 정당한 TA TA임을 확인할 수 없으므로 정당한 참가자의 차량을 철회시키는 문제가 발생할 수 있다.

3.3 서비스 거부 공격

네트워크 참가자에게 컴퓨팅 과부하를 제시하여 정당한 참가자에게 서비스를 거부하도록 만드는 공격이다. 공격자는 그룹생성 및 초기화 과정 (2)에서 차량에 전송하는 메시지를 도청한 것으로 가정한다. 차량은 메시지의 송신자가 정당한 KS 가 보냈음을 확인할 수 없고, 세션마다 동일한 메시지를 사용하므로 재전송 공격이 가능함으로서 다량의 접속 시도 등의 방법을 통해 서비스 거부 공격이 가능하다.

Ⅳ. 결론 및 고찰

본 논문에서는 Bong 등의 메시지 인증 기법에 대한 보안 분석을 통해 재전송 공격에 취약함을 분석하였다. 즉, Bong 등의 인증 기법은 메시지 신선성을 제시하지 못하는 문제가 존재한다. 이에 대한 해결책은 네트워크 참가자 간에 동기화된 타임스탬프를 이용한 메시지의 신선성을 제공함으로서 해결할 수 있다. 해결방안은 향후 연구로 제시하고자 한다.

ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

참 고 문 헌

[1] V. Namboodiri, M. Agarwal, and L. Gao, “A study on the feasibility of mobile gateways for vehicular ad-hoc networks,” *Proc. of the First International Workshop on Vehicular Ad Hoc Networks*, pp. 66-75, Oct. 2004.

[2] B. J. Sook, S. Y. Hwa, U. Jin, J. Y. Shin, “RSU-independent Message Authentication Scheme using CRT-based Group Key in VANET,” *Journal of Korean Institute of Information Scientists and Engineers*, vol. 46, pp. 277-284, 2019.

[3] A. Sudarsono, "An Implementation of Efficient Group Signature for Anonymous Authentication System in Vehicular Ad-Hoc Networks," *Proc. of 2020 International Electronics Symposium (IES)*, pp. 108-115, 2020.

[4] D. Manivannan, Shafika Showkat Moni, Sherali Zeadally, “Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs),” *Vehicular Communications*, vol. 25, 100247, 2020.