정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

자율주행자동차 V2V 통신환경에서의 DoS 공격 및 대응기술 동향 연구

이 숭 영*, 김 지 민*, 지 청 민*, 홍 만 표**

요 약

최근 자율주행 자동차의 발전은 자동차제조업체뿐만 아니라 ICT 기업도 참여하면서 매우 빠르게 발전하고 있다. 자율주행기술이 발달함에 따라 외부와의 통신을 통해 더욱 안전한 자율주행이 가능할 것이다. 하지만 외부와의 연결은 외부 IT 시스템의 위협이 차량 내부에 영향을 미치게 될 수 있고 이는 인명피해로 이어질 수 있다. 자율주행자동차의 통신은 실시간으로 다양한 메시지를 처리해야 하기 때문에 가용성이 매우 중요하다. 기존 IT 시스템에 존재하는 가용성을 위협하는 공격은 대표적으로 DoS 공격이 있다. 본 논문에서는 자율주행자동차 V2V 통신을 위해 사용되는 프로토콜을 살펴보고 발생할 수 있는 DoS 공격유형과 현재 연구되고 있는 대응기술에 대한 동향을 소개한다.

Ⅰ. 서 론

최근 국내뿐만 아니라 전 세계적으로 자율주행자동차에 대한 관심이 매우 증가하고 있다. 자율주행자동차가 큰 이슈가 되면서 자율주행과 관련된 기술을 개발하는 곳은 단순 자동차제조업체뿐만 아니라, 여러 ICT 기업도 참여하여 개발하고 있다. 현재 자율주행기술은 매우 빠르게 발전하고 있다. 자율주행자동차의 기술은 미국도로교통안전국(National Highway Traffic Safety Administration, NHTSA)에서 정의한 5단계(0단계~4단계)와 미국자동차기술학회(Society of Automotive Engineers, SAE)에서 정의한 6단계(0단계~5단계)로 구분되며 미국자동차기술학회에서 제시한 단계 별 세부내용은 그림 1과 같다[1]. 각 단계는 운전자의 개입 여부와 개입 정도를 기준으로 나누어진다. 현재 우버나 테슬라 차량에 탑재된 기술 수준은 3단계이다. 국내에서는 2027년까지 4단계 수준의 자율주행을 목표로 하고 있다[2]. 현재 기술 수준으로 자율주행자동차는 카메라와 다양한 센서를 이용하여 차선 및 주변 차량을 인식하고 돌발상황이 발생하지 않으면 운전자 개입 없이 자동으로 목적지까지 운전할 수 있다. 이렇게 각종 센서를 이용하여 자율주행이 가능하지만, 카메라와 센서만을 기반으로 자율주행을 하는 자동차는 카메라와 센서의 시야가 닿지 않는 곳이나 악천후와 같은 기상 악화로 카메라와 센서가 제대로 동작할 수 없는 상황에서는 자율주행에 제약을 받을 수 있다. 이러한 한계는 통신 기술을 통해 보완할 수 있다. 예를 들어 자동차는 외부와의 통신을 통해서 카메라가 제대로 동작하지 않는 상황에서도 자율주행이 가능할 수 있도록 돕는다. 또한, 주행 도중 도로정보, 교통신호 정보, 전방 충돌 및 사고 정보 등과 같은 자율주행에 도움이 되거나 필요한 정보를 받아 더욱 안전한 자율주행을 할 수 있다. 자율주행자동차의 통신에는 다양한 기술이 있는데, 그중 하나로 차량과 인근 차량을 연결하기 위한 V2V(Vehicle to Vehicle) 통신이 있다. V2V 통신을 통해 차량은 인접한 거리에 있는 다수의 차량과 다양한 메시지를 송수신하게 된다. 하지만 자율주행자동차에 통신 기술이 적용되면 폐쇄적인 기존 차량과 달리 외부와 연결되어야 한다. 폐쇄적인 기존 차량에서는 자동차에 발생하는 문제는 그 원인이 자동차 내부만으로 한정되지만, 통신을 통해 외부와 연결되는 경우 외부 IT 시스템에 존재하는 위협이 차량 내부로 침투할 수 있다. 이러한 위협이 차량 내부 네트워크에 영향을 미치게 되는 경우 사고가 발생할 수 있다. 기존 IT 시스템에서 사고가 일어나게

본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(20PQOW-B152473-02)으로 수행된 연구임.
* 아주대학교 컴퓨터공학과 디지털 백신 연구소 (대학원생, lsy1004j@ajou.ac.kr, yoiky12@ajou.ac.kr, ooops222@gmail.com)
** 아주대학교 사이버보안학과 (교수, mphong@ajou.ac.kr)

〔그림 1〕 미국자동차기술학회 자율주행기술 6단계

되면 데이터의 손실과 같은 문제가 발생하지만, 차량 네트워크에서 사고가 일어나게 되면 인명피해까지 발생할 수 있기 때문에 자율주행자동차의 통신에서 보안은 중요하다. 특히 자율주행을 위해서는 수신되는 다양한 메시지에 대해 실시간 처리가 이루어져야 한다. 그렇기 때문에 자율주행자동차는 다수의 메시지를 실시간으로 처리하기 위해서 가용성을 확보하는 것이 중요하다. 기존 IT 시스템에서 가용성을 위협하는 공격은 대표적으로 DoS 공격이 있다. 본 논문에서는 자율주행자동차 V2V 통신환경에서 발생 가능한 DoS 공격과 이에 대한 대응기술 동향에 대해 살펴본다. 본 논문의 구성은 다음과 같다. 2장에서는 자율주행자동차 통신과 관련된 VANET, WAVE, AODV에 대한 이론적 배경을 소개한다. 3장에서는 V2V 통신환경에서 발생할 수 있는 DoS 공격에 대해 살펴본다. 4장에서는 이러한 공격 기법들에 대하여 최근까지 연구되어온 대응기술 동향을 살펴본다. 마지막으로 5장에서는 결론을 맺는다.

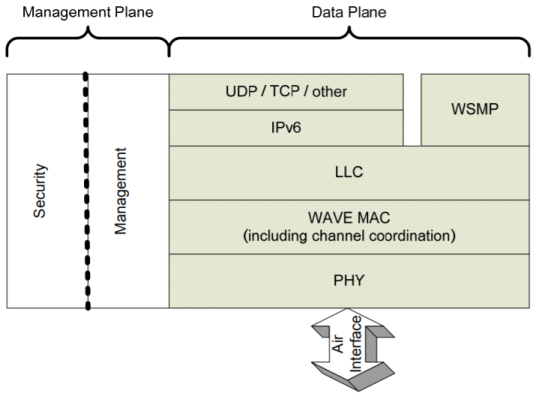
Ⅱ. 이론적 배경

2.1. VANET

VANET(Vehicular Ad-hoc Network)은 이동하는 차량이 노드로 구성되어 차량 간 메시지를 교환하는 애드혹 네트워크 형태이다. 이는 모바일 애드혹 네트워크를 뜻하는 MANET(Mobile Ad-hoc Network)와 구분되는 개념이다[3]. 이 네트워크는 V2V와 V2I(Vehicle to Infrastructure) 통신을 지원하며 무선통신을 위해 DSRC/WAVE를 사용한다. VANET에서 노드 간 경로 설정을 위해 사용되는 라우팅 프로토콜 중 하나로 AODV 라우팅 프로토콜이 있다.

2.2. WAVE

WAVE(Wireless Access in Vehicular Environment)는 ITS(Intelligent Transportation System) 환경에서 원활하고 상호운용 가능한 서비스를 제공하기 위한 무선통신 시스템이다. WAVE와 관련된 표준은 IEEE 1609와 IEEE 802.11p가 있다. WAVE 프로토콜 스택은 그림 2와 같다. IEEE 1609는 WAVE 아키텍처를 설명하는 IEEE 1609.0, WAVE 식별자 할당 기능을 설명하는 IEEE 1609.12, WAVE 애플리케이션과 관리 메시지 보안 서비스를 설명하는 IEEE 1609.2, WAVE 네트워킹 서비스를 위한 IEEE 1609.3, 다중 채널 기능을 설명하는 IEEE 1609.4로 구성되어 있다[4]. IEEE 802.11p는 WAVE를 위한 물리계층과 MAC 계층을 정의한다. 이 중에서 IEEE 1609.3은 무선차량 환경에서 최적화된 작동을 위해 표준 인터넷 프로토콜 버전 6(IPv6)과 WSMP(WAVE Short Message Protocol)로 구성된 표준이다[5]. IPv6에서 전송계층으로 사용되는 프로토콜에는 TCP와 UDP 등이 있다. TCP는 포트 번호 주소 지정과 종단 간 신뢰성, 그리고 선택적 재전송 기능을 제공하고 UDP는 포트 번호 주소 지정과 WSMP에서 제공되지 않는 체크섬 기능을 제공한다.



〔그림 2〕 WAVE 프로토콜 스택[4]

2.3. AODV

AODV(Ad-hoc On Demand Vector)는 Ad-hoc 네트워크에서 사용되는 라우팅 프로토콜이다. AODV는 출발지-목적지 간 경로를 사전에 탐색하는 것이 아니라

On-demand 형식으로 필요할 때 경로를 탐색하므로 라우팅을 위한 부하가 적다[6]. 경로가 이전에 설정된 경우에는 해당 경로를 재사용할 수 있지만 새로운 경로에 대해서는 다시 새롭게 탐색을 해야 한다. 경로를 설정하기 위해서는 RREQ(Route Request) 패킷과 RREP(Route Replay) 패킷이 사용된다.

Ⅲ. V2V DoS 공격 연구 사례

이 장에서는 V2V 통신환경에서 발생할 수 있는 DoS 공격 연구 사례에 대해 살펴본다. 3.1.절과 3.2.절에서는 각각 WAVE에서 사용되는 TCP 프로토콜과 IPv6에서 발생할 수 있는 DoS 공격을 살펴본다. 3.3.절부터 3.6.절까지는 AODV 라우팅 프로토콜에서 발생할 수 있는 DoS 공격을 살펴보고 마지막으로 3.7.절에서 WSMP에서 발생할 수 있는 DoS 공격을 살펴본다. 표 1은 아래 공격유형들을 간략하게 요약한 내용이다.

3.1. TCP SYN Flooding attack

TCP 프로토콜에는 클라이언트와 서버 간 네트워크 연결을 위해 사용되는 Three-way Handshake 절차가 존재한다. TCP SYN Flooding은 이러한 Three-way Handshake 절차를 악용한 공격이다. 먼저 Three-way Handshake 과정은 다음과 같다. 클라이언트에서 서버에 SYN을 전송하여 통신 연결을 요청한다. 서버는 클라이언트에게 SYN-ACK을 사용하여 응답한다. 마지막으로 클라이언트는 다시 서버에게 ACK을 전송하여 연결을 설정한다. 위 과정 중 서버가 클라이언트에게 SYN-ACK을 전송할 때의 상태를 half-open 상태라고 한다[7]. half-open 상태의 연결 정보는 서버의 백로그 큐에 저장된다. 마지막에 클라이언트에게 ACK을 받았을 때, 연결이 설정되면서 서버는 백로그 큐에 남아있던 해당 half-open 연결 정보를 비운다. TCP SYN Flooding은 이 half-open 상태를 악용한다. 악의적인 클라이언트가 마지막 단계인 ACK 패킷을 보내는 대신 SYN 패킷을 전송하게 되면 서버는 새로운 half-open 연결 정보를 저장하게 된다. 악의적인 클라이언트가 계속해서 이런 행동을 반복한다면 서버의 백로그 큐의 저장 공간이 부족해져서 이후에 오는 정상적인 클라이언트의 연결 요청에 대해 응답할 수 없게 된다.

3.2. Duplicate Address Detection(DAD) DoS

IPv6에서는 노드가 서브 네트워크에 참여하기 위해 IP 주소를 설정하는데, 이때 설정된 주소가 다른 노드의 주소와 중복되는지 판단하기 위해 DAD 작업을 진행한다[8]. DAD 과정은 다음과 같다. 먼저 노드에서 임시 주소가 생성되면 노드는 임시 주소가 포함된 NS 패킷을 전송한다. 해당 패킷을 보냄으로써 노드는 생성된 임시 주소가 고유하다는 것을 확인할 수 있다. 전송된 NS 패킷에 대해 응답이 없는 경우 노드는 주소가 고유하다고 가정하고 사용한다. 그런데 이 과정에서 공격자가 자신이 해당 주소를 사용한다고 거짓된 주장을 하여 DoS

〔표 1〕 V2V DoS 공격유형

공격 유형	관련 프로토콜 및 계층	공격 설명
TCP SYN Flooding	TCP / Transport	Three-way handshake를 종료하지 않고 계속해서 SYN 패킷을 전송하여 TCP 연결 장애
DAD DoS	IPv6 / Network	거짓된 DAD 응답으로 주소 설정 불가능
RREQ Flooding	AODV / Network	RREQ 전송 규칙을 위반하여 대량의 패킷 전송으로 경로 설정 불가능
Blackhole	AODV / Network	네트워크 내부 혹은 외부에서 데이터를 삭제하는 등의 행위로 네트워크 통신 방해
Sybil	AODV / Network	다수의 신분을 사용하여 혼란을 발생
Jellyfish	AODV / Network	패킷 전송을 지연시켜 네트워크 지연
BSM DoS	WSMP / Application, MAC	WAVE 채널 간 조정 기능을 악용하여 정상적인 차량의 BSM 전송지연

공격을 수행할 수 있다[9]. 공격자가 거짓된 주장을 하는 방법에는 다음과 같다. 먼저 일반 노드가 DAD를 위한 NS 패킷을 전송하면 공격자가 이미 해당 주소가 사용되고 있다는 거짓된 응답을 전송하는 것이다. 공격자가 위 방법을 통해 거짓된 정보를 전송하면 노드는 다시 주소를 생성하고 DAD를 반복한다. 공격자는 매 반복마다 거짓된 정보를 전송하여 해당 노드가 주소를 얻지 못하게 한다.

3.3. RREQ Flooding attack

AODV 라우팅 프로토콜에서 경로 탐색은 on-demand 방식으로 수행된다. 출발지 노드는 자신으로부터 경로가 설정되지 않은 목적지로 패킷을 전송하기 전에 자신의 이웃에게 RREQ 패킷을 전송한다. RREQ를 받은 이웃은 자신의 라우트 테이블을 확인하고 경로가 있을 경우 RREP 패킷을 통해 경로를 알려주고 없을 경우 다시 RREQ 패킷을 다른 이웃에게 전송한다. 전체 네트워크에서 RREQ 패킷을 계속해서 전송하는 것은 많은 자원을 소비하기 때문에 한 노드가 초당 일정 수 이상의 패킷을 전송할 수 없도록 설계되어 있다. 공격자는 이와 같은 특성을 위반하여 RREQ Flooding 공격을 수행할 수 있다[10]. 공격자는 임의의 IP 주소를 선택하는데, 만약 공격자가 공격 대상의 IP 주소 네트워크 범위를 아는 경우 범위 밖의 IP 주소를 선택한다. 다음으로 공격자는 선택한 IP 주소에 대해 대량의 RREQ 메시지를 연속적으로 발생시킨다. 전체 네트워크에는 공격자가 전송한 RREQ 패킷이 가득 차게 되고 이를 처리하기 위해 많은 자원이 소비된다. RREQ 패킷을 수신한 이웃 노드들은 경로를 저장할 수 있는 라우트 테이블 저장 공간이 가득 차 새로운 RREQ 패킷을 수신할 수 없게 된다.

3.4. Blackhole attack

AODV 라우팅 환경에서는 두 가지 형태의 blackhole 공격이 가능하다[11]. 첫 번째 형태는 출발지와 목적지 경로 내부에 악의적인 노드가 있는 경우에 발생할 수 있는데, 이때 악의적인 노드는 경로 사이에서 출발지와 목적지를 오가는 데이터를 삭제한다. 두 번째 형태는 네트워크 외부에서 발생할 수 있는데, 외부에 있는 악의적인 노드가 내부 네트워크에 접근하여 정상적인 노드의 패킷 교환을 방해하거나 정체를 일으켜 네트워크를 방해할 수 있다. 이를 위해 악의적인 노드는 기존 네트워크에서 설정된 경로를 탐지하여 경로 내에 속한 노드 중 자신과 근접한 노드에게 거짓 경로 설정 응답을 전송한다. 해당 노드에 거짓된 경로가 설정되면 목적지 노드에게 전송되어야 할 데이터를 악의적인 노드가 대신 수신하고 수신한 데이터를 삭제하여 공격을 수행할 수 있다.

3.5. Sybil attack

Sybil 공격은 악의적인 차량이 복수의 신분을 가질 수 있을 때 발생한다[12]. 복수의 신분을 갖는 경우는 두 가지가 있다[13]. 첫 번째는 공격자가 다른 차량의 신분을 도용하여 정상적인 차량처럼 속이는 것이다. 두 번째는 공격자가 존재하지 않는 거짓된 신분을 만들어 내는 것이다. 공격자는 만들어낸 거짓 신분을 통해 위치 정보 등이 조작된 메시지를 전달한다. 이를 수신한 다른 차량은 해당 위치에 존재하지 않는 차량이 마치 실제로 존재하는 것처럼 인식하기 때문에 주행에 혼란을 겪게 된다.

3.6. Jellyfish attack

Jellyfish 공격은 메시지 지연을 통해 네트워크에 영향을 준다[14]. Jellyfish 공격을 수행하는 노드는 다른 노드들로부터 RREQ 패킷을 받았을 때, 이에 대해 거짓 RREP 패킷을 응답함으로써 다른 정상적인 노드에 거짓된 경로가 설정되도록 한다. 그리고 나서 패킷들이 Jellyfish 공격을 수행하는 노드를 통과할 때 해당 노드는 각 패킷에 지연을 추가하여 다른 노드들에게 전송한다.

3.7. BSM DoS

BSM은 차량이 V2V 통신을 수행할 때 인접한 차량에 지속적으로 브로드캐스트하는 메시지이다[15]. 이 메시지에는 송신 차량의 시간, 위치, 속도, 경로 기록 및 기타 관련 정보가 있고 BSM 메시지는 디지털 서명이 되어있다. 수신 차량은 각 메시지에 대한 서명을 확인하

고 평가한 후 운전자에게 경고를 표시할지 결정한다. BSM을 통해 DoS 공격을 발생시킬 수 있는 방법은 크게 두 가지가 있다. 첫 번째 방법은 V2V 통신 환경에서는 공격자가 거짓 메시지가 전송하는 것을 막기 위해서 사용하는 서명 검증을 악용하여 DoS 공격을 수행하는 것이다[16]. 공격 방법은 다음과 같다. 공격자가 잘못된 서명을 붙인 대량의 거짓 메시지를 위조하여 전송하게 되면 이를 수신하는 차량은 잘못된 서명을 검증하기 위해 대부분의 자원을 소모하게 된다. 또 다른 방법은 V2V 통신에서 BSM을 전송하기 위해 사용되는 MAC 계층인 802.11계층의 취약점을 악용하여 공격을 수행하는 것이다[17]. WAVE에는 서비스 채널과 통제 채널이 존재하는데, 차량에서는 WAVE의 다중 채널 조절 기능을 사용하여 전송시간을 두 가지 채널로 나누어 사용한다[18]. 각 채널의 전송시간 앞부분에는 보호 간격이 존재하며 이 동안에는 전송이 불가능하다. 또한, 보호 간격이 끝난 직후 메시지를 전송하기 위해서 유휴상태를 확인해야 하는 절차가 있다. 공격자가 다른 차량들에서 이 절차가 완료되기 전에 BSM을 전송하게 되면 다른 차들의 BSM 전송을 지연시킬 수 있다.

Ⅳ. DoS 공격 대응기술 동향

이 장에서는 V2V 통신환경에서 DoS 공격에 대한 대응기술 연구 동향을 살펴본다. 4.1.절은 VANET에서 Greedy 행동에 기반한 DoS 공격을 탐지하기 위한 연구에 대해 살펴본다. 4.2.절은 차량 간 익명 인증 과정에서 발생할 수 있는 DoS 공격을 완화하는 방안에 대한 연구에 대해 살펴본다. 4.3.절은 IP-chock를 기반으로 DoS 공격을 탐지하는 연구에 대해 살펴본다. 마지막으로 4.4.절에서는 Black hole 공격을 완화하는 방법을 제안하는 연구에 대해 살펴본다. 표 2는 V2V DoS 공격 유형과 그에 대한 대응기술 요약한 것이다.

4.1. Greedy Detection for VANET

VANET에서 greedy 행동에 기반한 공격은 MAC 계층의 취약점을 이용한다. 공격자 노드는 자신의 대기시간을 감소시켜 채널에 더 빠른 접근을 하며, 다른 일반 노드들의 정상적인 동작을 방해한다. 공격자는 백오프 조작을 포함한 여러 가지 기술을 사용하여 Greedy 행동에 기반한 공격을 수행한다. 이러한 공격을 탐지하기 위해 Mejri외 1명은 두 단계로 구성된 GDVAN(Greedy Detection for VANET)이라는 알고리즘을 개발했다[19]. GDVAN 알고리즘의 목적은 VANET을 감시하는 것인데, 알고리즘은 크게 Suspicion 단계와 Decision 단계로 나누어진다. 첫 번째 Suspicion 단계에서는 네트워크의 상태가 정상인지 비정상인지 일차적으로 확인하는 단계이다. 네트워크의 상태가 정상이면 한 노드가 채널에 접근할 때 다른 노드는 접근한 노드의 전송이 끝날 때까지 해당 채널에 접근할 수 없다. 그렇기 때문에 네트워크가 정상적인 상황이라면 노드들의 연결시간은 선형적인 형태를 갖게 된다. 이러한 특성을 사용하여 Suspicion 단계에서는 상관계수와 선형 회귀 분석의 개념을 통해 네트워크의 상태를 관찰한다. 관찰을 통해 Greedy 행동으로 의심되는 경우는 두 가지이다. 하나는 상관계수가 1과 가깝지 않은 경우이고, 다른 하나는 상관계수가 1에 가깝지만, 선형 회귀 직선의 기울기가 1에 가깝지 않은 경우이다. 위와 같은 두 가지 경우에 대해 watchdog을 사용하여 세 가지를 확인한다. 첫 번째는 두 개의 연속된 전송 사이의 지속시간이고, 두 번째는 노드의 패킷 전송시간,

〔표 2〕 V2V DoS 공격유형과 그에 대한 대응기술 요약

공격유형 / 대응기술	TCP SYN Flooding	DAD DoS	RREQ Flooding	Blackhole	Sybil	Jellyfish	BSM DoS
GDVAN	-	-	-	-	-	-	O
Puzzle-based co-authentication	-	-	-	-	-	-	O
IP-chock	O	O	-	-	O	-	-
Black hole mitigation	-	-	O	O	-	O	-

세 번째는 노드의 채널 접근 시도 횟수이다. 세 가지 변수를 확인한 후 알고리즘의 다음 단계인 Decision 단계에서는 퍼지 논리를 사용하여 특정 차량의 상태를 결정한다. 최종적으로 차량은 normal, suspected 또는 greedy로 분류된다.

4.2. Puzzle-based co-authentication

P. Liu외 4명은 차량 환경에서 Puzzle 기반 상호 인증을 통해 익명 인증 시간에 대한 오버헤드를 줄여 DoS 공격을 완화하는 방법을 제안했다[20]. 해당 연구에서는 익명 인증을 최초 검증하는 데 걸리는 시간이 14.7ms 이상 걸리기 때문에 서로 다른 ID를 가진 메시지가 다량으로 수신되는 경우 DoS의 위협이 발생할 수 있다고 설명한다. 이에 대응하기 위해 제안한 알고리즘인 PCA(Puzzle-based co-authentication)는 해시 퍼즐 설계 단계와 상호 신뢰 클러스터 설계 단계로 구성된다. 먼저 해시 퍼즐 설계 단계는 해시의 단방향성을 이용해서 공격자가 무차별적으로 메시지를 보내는 것을 방지하기 위한 퍼즐을 생성한다. 퍼즐은 메시지와 퍼즐에 대한 답으로 구성되며, 퍼즐을 해시한 값에서 마지막으로 나타나는 연속된 0의 개수 k를 퍼즐의 평가 값으로 사용한다. 퍼즐을 사용한 인증 과정은 다음과 같다. 먼저 검증자는 퍼즐을 생성한 뒤, 퍼즐의 답을 제외한 메시지와 k 값을 요청자에게 전송한다. 요청자는 퍼즐의 답을 계산하여 검증자에게 전송하고, 검증자는 메시지와 요청자가 전송한 퍼즐의 답을 이용하여 올바른 k값이 계산되는지 확인한다. 요청자가 퍼즐의 답을 계산할 때 해시의 단방향성으로 인해 $O(2^k)$ 만큼의 시간 복잡도가 필요하므로, 공격자는 무차별적으로 메시지를 전송할 수 없게 된다. 다음으로 상호 신뢰 클러스터 설계는 정상적인 단일 사용자들의 자원을 통합하기 위한 협력 인증 체계이다. 상호 신뢰 클러스터는 이미 서로 신뢰하는 구성원으로 구성되며 같은 클러스터의 구성원끼리는 함께 퍼즐을 생성하거나 인증서를 검증하기 위해 함께 협력할 수 있다.

4.3. IP-CHOCK-based detection

K. verma외 1명은 VANET 환경에서 DoS 공격을 탐지하기 위해 IP-CHOCK에 기반한 방법을 제안했다[21]. 이 방법은 악의적인 노드가 IP 주소를 스푸핑하여 DoS 공격을 수행하는 것을 탐지한다. 이 방법의 크게 두 가지 단계로 구성된다. 하나는 Detection Engine 단계이고 나머지는 Bloom-filter 단계이다. Deteciton Engine 단계는 다시 두 가지로 나뉜다. 첫 번째 Deteciton Engine 단계에서는 들어오는 모든 교통 정보를 확인한다. 교통의 변화는 차량의 센서를 통해 감지된다. 이 단계에서는 두 번째 Deteciton Engine 단계에 필요한 차량 IP 주소를 수집한다. 두 번째 Deteciton Engine 단계에서는 첫 번째 단계에서 센서를 통해 감지된 값을 처리하여 이 값이 네트워크에 영향을 미칠 가능성이 있는지 결정한다. 이 단계에서 네트워크에 악의적인 영향을 미칠 가능성이 있는 차량 IP 주소를 발견하지 못하면 해당 정보를 데이터베이스에 저장하고 발견한다면 이를 Decision Engine에 전달한다. 마지막 단계는 해시 기능을 가진 Bloom-filter 단계이다. 의사결정 엔진에서 수집된 정보에 악의적인 IP 주소가 포함되어 있으면 Bloom-filter 과정을 거치게 된다. 그리고 그 결과로 생성된 참조 링크를 연결된 차량에 전송하여 VANET에서 악의적인 IP 주소가 포함된 메시지가 사용되지 못하도록 막는다.

4.4. Black hole attack mitigation

J. Tobin 외 3명은 무선 차량 네트워크에서 blackhole 공격을 완화하는 방법을 제안했다[22]. 이 방법은 공격 탐지, 고발, 블랙리스트 등록의 세 가지 단계로 나뉜다. 먼저 출발지 혹은 목적지 노드가 서로 연결된 경로를 통해 패킷을 전송하는 도중에 네트워크 문제를 인식했을 때 공격 탐지 절차 단계가 시작된다. 이를 위해 출발지 노드는 경로 내에 포함된 홉들에게 이전 홉에게 받은 패킷 수와 다음 홉에 전송한 패킷 수를 요청한다. 출발지 노드가 특정 홉에게 요청한 정보를 받으면, 경로 내에 포함된 홉들 중 응답하지 않는 홉이 존재할 때까지 같은 정보를 다음 홉에게 요청한다. 홉으로부터 응답을 받지 못하는 경우 출발지 노드는 목적지 노드에게 대체 경로를 통해 해당하는 노드에 대한 경고 메시지를 전송한다. 경고 메시지를 받은 목적지 노드는 출발지 노드가 수행 했던 것과 같은 동일한 과정을 진행한다. 만약 경로 내에 포함된 모든 홉들로부터 응답을 받는 경우 알고리즘을 종료한다. 하지만 목적지 노드에

서 출발지 노드가 응답을 받지 못했던 홉으로부터 동일하게 응답을 받지 못하는 경우 출발지 혹은 목적지 노드는 해당 노드에 대한 고발 단계를 진행한다. 고발 단계에서는 이전 단계에서 출발지 및 목적지 노드가 고발한 노드로부터 수집한 패킷 수를 비교하여 서로 일치하지 않는 경우 해당 노드가 악의적인 행동을 하는 것으로 판단한다. 그리고 악의적인 행동을 하는 것으로 판단된 노드는 블랙리스트에 등록되어 VANET에 참여하지 못하게 된다.

Ⅴ. 결 론

본 논문에서는 자율주행자동차 V2V 통신환경에서 발생 가능한 DoS 공격과 대응기술 동향에 대해 살펴보았다. V2V 통신환경에서 발생 가능한 DoS 공격은 V2V 통신에서 사용되는 특정 메시지를 활용한 공격을 제외하고는 기존 IT 시스템에서 존재했던 DoS 공격과 크게 다르지 않다. BSM DoS 또한 V2V 통신에 사용되는 특정 메시지를 사용한다는 사실만 다르고 공격하는 원리나 방법은 비슷하다. 대응기술도 마찬가지로 기존에 존재하던 대응기술을 대부분 차량에 맞게 간소화하여 적용한다. 현재는 차량의 이동성과 한정적인 자원을 고려해서 간소화한 대응기술을 사용하고 있지만, 향후 통신성능과 자율주행기술이 더욱 발전하게 되면 더욱 높은 수준의 대응기술이 적용되어 강력한 보안성을 갖춘 안전한 자율주행이 가능할 것으로 기대된다.

참 고 문 헌

[1] SAE, “Level of Driving Automation”, *SAE J3061,* 2018

[2] 관계부처 합동, “미래자동차 산업 발전 전략”, 2019

[3] Anwer, M. Shahid, Chris GuyA, “Survey of VANET Technologies”, Journal of Emerging Trends in Computing and Information Sciences 5(9) pp. 661-674, 2014

[4] “IEEE Guide for Wireless Access in Vehicular Environments (WAVE)-Architecture,” *IEEE Standard 1609.0-2013,* 2013.

[5] “IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services,” *IEEE Standard 1609.3-2016,* 2016

[6] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” *Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999

[7] K. Geetha, N. Sreenath, “Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol”, *RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE,* pp. 1161-1172, 2015

[8] Carlos E. Caicedo, James B.D. Joshi, Summit R. Tuladhar, “IPv6 Security Challenge”, *Computer, vol. 42, no. 2,* pp.36-42, Feb 2009

[9] A. S. A. Mohamed Sid Ahmed, R. Hassan and N. E. Othman, “IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey.”, *IEEE Access, vol. 5,* pp. 18187-18210, 2017.

[10] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang, “Resisting flooding attacks in ad hoc networks.” *International Conference on Information Technology: Coding and Computing Volume II,* pp. 657-662, 2005,

[11] V. Bibhu, K. Roshan, K. Balwant, D. Kumar, “Performance Analysis of Black Hole Attack in Vanet”, *I. J. Computer Network and Information Security,* pp. 47-54, Nov 2012

[12] Karn, Chaitanya, Gupta, C.P., “A survey on VANETs security attacks and Sybil Attack detection.” *International Journal of Sensors Wireless Communications and Control. 6.* pp. 45-62. 2016

[13] P. Kafil, M. Fathy, M. Z. Lighvan, “Modeling Sybil attacker behavior in VANETs.” *2012 9th International ISC Conference on Information Security and Cryptology*, pp. 162-168. 2012,

[14] Elsa Mustikawati, Doan Perdana, Ridha Muldina Negara, “Network Security Analysis in Vanet Against Black Hole and Jellyfish Attack with Intrusion Detection System Algorithm”, *CommIT (Communication & Information Technology)*

Journal 11(2), pp. 77 - 83, 2017

[15] B. Brecht et al., "A Security Credential Management System for V2X Communications.", *IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 12,* pp. 3850-3871, Dec. 2018.

[16] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs." *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, pp. 261-265. 2012

[17] M. Kaur, J. Martin and H. Hu, "Comprehensive view of security practices in vehicular networks." *International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 19-26. 2016

[18] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Multi-Channel Operation," *IEEE Standard 1609.4-2016,* 2016

[19] M. N. Mejri, J. Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs.", *IEEE Transactions on Mobile Computing, vol. 16, no. 3,* pp. 759-771, March 2017.

[20] P. Liu, B. Liu, Y. Sun, B. Zhao, I. You, "Mitigating DoS Attacks Against Pseudonymous Authentication Through Puzzle-Based Co-Authentication in 5G-VANET," *IEEE Access, vol. 6,* pp. 20795-20806, 2018.

[21] K. Verma, H. Hasbullah, "IP-CHOCK (filter)-Based detection scheme for Denial of Service (DoS) attacks in VANET," *International Conference on Computer and Information Sciences (ICCOINS)*, pp. 1-6. 2014

[22] J. Tobin, C. Thorpe, L. Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks," *IEEE 85th Vehicular Technology* Conference, pp. 1-7, 2017

〈저자소개〉

이 승 영 (Sung-young Lee)

학생회원

2019년 2월 : 아주대학교 사이버보안학과 학사

2019년 3월~현재 : 아주대학교 컴퓨터공학과 석사과정

<관심분야> 정보보호, 자율주행, 차량보안

김 지 민 (Ji-min Kim)

학생회원

2015년 2월 : 아주대학교 정보컴퓨터공학과 학사

2015년 3월~현재 : 아주대학교 컴퓨터공학과 석·박사 통합과정

<관심분야> 정보보호, 임베디드/IoT 보안

지 청 민 (Cheong-min Ji)

학생회원

2012년 2월 : 아주대학교 정보컴퓨터공학과 학사

2012년 3월~현재 : 아주대학교 컴퓨터공학과 석·박사 통합과정

<관심분야> 차량보안, 임베디드/IoT 보안, 블록체인 보안, 영상데이터 보안

홍 만 표 (Man-pyo Hong)

종신회원

1981년 2월 : 서울대학교 계산통계학과 학사

1983년 8월 : 서울대학교 계산통계학과 석사

1991년 2월 : 서울대학교 전산과학과 박사

1985년 3월~2016년 2월 : 아주대학교 정보컴퓨터공학부(과) 교수

2016년 3월~현재 : 아주대학교 사이버보안학과 교수

<관심분야> 정보보호, 기반시설보안, 임베디드/IoT 보안, 금융보안, 차량보안, 병렬처리