Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.6, Dec. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.6.1171

SOME/IP 에서의 시퀀셜 모델 기반 침입탐지 시스템

강 연 재,[1†] 피 대 권,[1] 김 해 린,[1] 이 상 호,[1] 김 휘 강[2‡]
[1,2]고려대학교 (대학원생, 교수)

Intrusion Detection System Based on Sequential Model in SOME/IP

Yeonjae Kang,[1†] Daekwon Pi,[1] Haerin Kim,[1] Sangho Lee,[1] Huy Kang Kim[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

전방충돌 방지 보조 또는 지능형 주행 제어 기능 등이 현대의 자동차에 탑재됨에 따라 차에서 교환되는 데이터 양이 급증하고 있다. 따라서, 기존의 CAN 통신으로는 전송속도의 한계가 있어 넓은 대역폭과 양방향 통신을 지원하는 오토모티브 이더넷, 특히 SOME/IP가 널리 채택되고 있다. SOME/IP는 다양한 자동차 운영체제와 호환되는 표준 프로토콜로 차내 구성 요소간의 연결성을 높여준다. 하지만 SOME/IP 자체에는 암호화나 인증이 구현되어 있지 않아 악의적인 패킷 주입, 프로토콜 위반과 같은 공격에 취약한 문제가 있다. 본 논문에서는, 이러한 공격들을 효과적으로 탐지하기 위해 SOME/IP에서 딥러닝 기반의 침입탐지 시스템을 제안하였다. 제안된 침입탐지시스템의 성능을 6가지 공격 패턴을 활용하여 테스트 하였고 정확도 94%, 6가지 공격의 평균 F1-score은 0.94로 높은 성능을 달성할 수 있었다.

ABSTRACT

Front Collision-Avoidance Assist (FCA) or Smart Cruise Control (SCC) is installed in a modern vehicle, and the amount of data exchange between ECUs increases rapidly. Therefore, Automotive Ethernet, especially SOME/IP, which supports wide bandwidth and two-way communication, is widely adopted to overcome the bandwidth limitation of traditional CAN communication. SOME/IP is a standard protocol compatible with various automobile operating systems, and improves connectivity between components in the vehicle. However, no encryption or authentication process is defined in the SOME/IP protocol itself. Therefore, there is a need for a security study on the SOME/IP protocol. This paper proposes a deep learning-based intrusion detection system in SOME/IP and performs six attacks to confirm the performance of the intrusion detection system.

Keywords: Vehicle, SOME/IP, Automotive Ethernet, Intrusion Detection System (IDS)

I. 서 론

현재 미국의 신차 92.7%는 안전 및 운전 편의를 위한 보조 시스템인 ADAS (Advanced Driver Assistance System)를 최소 한 개 이상 탑재하고 있다 [1]. 또, 2043년까지 미국에 등록된 차량의 95%에 대부분의 ADAS 기능을 장착할 것으로 예측된다 [2]. ADAS의 대표적인 예로, 전방에 예상치 못한 장애물이 탐지될 경우, 경고 및 제동을 해주는 전방충돌방지보조(FCA; Forward Collision-Avoidance Assist) 시스템과 차량이 차선에서 벗어난 경우 알림과 함께 차선에 맞게 주행방향을 조정해주는 차로유지보조(LKA; Lane Keeping Assist) 시스템 등이 있다.

Received(11. 04. 2022), Modified(12. 06. 2022), Accepted(12. 06. 2022)
† 주저자, kangyj1995@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

이와 같이 차량 내 다양한 센서 및 ECU의 기능이 다양해짐에 따라 데이터 전송량이 증가하여 네트워크 전송 대역폭 요구도 늘어났다 [3]. 반면, 기존의 대표적인 차량내부통신 표준인 CAN (Controller Area Network)은 최대 1Mbit/s 전송 대역폭을 지원하기 때문에 ADAS와 같은 주행 보조 및 안전 기능 구현을 위한 대용량 트래픽을 처리할 수 없는 문제가 있다. 또 자동차 내 전기, 전자 부품들이 차지하는 비중이 2019년 16%에서 2025년 35%로 증가할 것으로 전망되어 결과적으로 차량에서 전장품의 원가 및 유지 보수에 할당되는 비용이 더 많이 필요할 것이다 [4].

자동차 산업에 이더넷을 도입하는 것은 가용 대역폭을 증가시키고 차량 도메인에서의 IP 기반 통신 체계 확립에 도움을 주었다. 특히, 2013년 차량을 위해 특별히 설계된 프로토콜인 SOME/IP [19]는 서비스 제공자인 서버와 소비자인 클라이언트가 직접 연결되어 통신하는 방식으로 되어 있어 기존의 신호 기반 차량 내부 네트워크인 CAN, LIN, FlexRay와는 전송 방식이 다르다. 특정 ECU 클라이언트는 SOME/IP를 통해 ECU 서버에 정보를 요청할 수 있고 해당 ECU 에 특정 서비스가 실행되고 있는지 확인할 수도 있으며 차량 내부에서 발생한 이벤트를 알릴 수 있다. 이러한 장점을 통해 SOME/IP는 차량 내 이더넷 기술로 자리 잡았다.

하지만, SOME/IP는 보안을 위해 정의된 암호화나 인증 과정이 없어 통신 시, 기밀성 (confidentiality) 및 무결성 (integrity)를 유지할 수 없다. 더불어, 상용화되어 있는 패킷 모니터링 및 이상징후탐지 장치, 방화벽 등에서 SOME/IP를 아직 지원하고 있지 않는 경우가 대부분이어서 SOME/IP 기반 통신은 현재 많은 위협에 노출되어 있는 상태이다.

본 논문에서는 SOME/IP를 기반으로 구성된 자동차 내부 네트워크에 수행할 수 있는 6가지 공격을 제시하고, 해당 공격을 탐지하는 딥러닝 기반의 침입탐지 시스템을 제안한다. 제시되는 6가지 공격은 SOME/IP 내 보안 및 인증 메커니즘의 결여를 이용한 것으로, SOME/IP 프로토콜을 적용한 다른 장치에 시도할 수 있다. 따라서 본 연구는 앞으로 서비스 지향 아키텍처 기반의 SOME/IP를 채택할 모든 도메인에서의 침입탐지 연구에 도움이 될 것으로 판단된다.

본 논문의 구성은 다음과 같다. 본 논문의 2장과 3장에서는 관련 연구와 SOME/IP 프로토콜에 대한 배경 지식을 기술하였다. 4장에서는 데이터셋, 전처리 방식, 공격 유형과 같은 실험 설계의 전반적인 내용에 관해 서술했다. 5장에서는 본 논문에서 SOME/IP 도메인에서 제안하는 침입탐지 모델에 관해 설명하였다. 6장에서는 실험 결과를 판단할 평가 지표와 실험 결과를 설명하고, 마지막으로 본 논문의 결론 및 한계점을 기술하였다.

II. 관련 연구

차량 내부 네트워크 중 오토모티브 이더넷 (Automotive Ethernet)은 2010년대 후반부터 상용 차량에 적용되고 있어서, CAN 기반의 차량용 침입탐지시스템에 비해 상대적으로 많은 연구가 진행되지 않은 상태이다. CAN에서는 잘 알려진 침입탐지 학습용 데이터셋 [5]-[8]이 존재하고, UNR 155 (CSMS) 규정의 발효로 인해 대다수의 상용차량들이 차량용 침입탐지시스템을 탑재하고 있다. 반면에, 오토모티브 이더넷의 경우에는 침입탐지 용 데이터셋이 CAN 데이터셋에 비해 희소하며, AVTP(Audio and Video Transport Protocol)에 대한 침입탐지용 데이터셋 [7] 과 gPTP, AVB까지 다루어진 데이터셋 [20] 이 공개되어 있는 수준이다.

기존에 출시되어 있는 상용차량의 경우에도 최상위 트림의 최신 차량 중 일부에만 오토모티브 이더넷이 들어가 있는 상황이고, 주로 LiDAR(Light Detection And Ranging) 센서 입력을 처리하는 용도로 제한적으로 사용되고 있어, 오토모티브 이더넷 용 침입탐지시스템 및 SOME/IP 에 특화된 침입탐지시스템은 아직 산업계 및 학계 모두 개발 초기 단계라 할 수 있다.

Du 등은 정형기법을 사용해 SOME/IP의 보안을 분석하고, 정형 모델링 도구인 CPN을 사용해 보안 취약점을 식별했다 [10]. Gehrmann와 Duplys은 SOME/IP의 세부사항을 활용하는 SOME/IP 네이티브 침입탐지 아키텍처를 제안했다 [12]. 이 아키텍처는 SOME/IP에 통합되는 모듈의 형태로, 서비스 및 클라이언트 ID를 포함하고 있어 어떤 서비스가 제공되고 가입되는지를 모니터링하는 특징이 있다. 또 M. Iorio 등이 진행한 연구에서도 2단계 보안 프로토콜로 구성된 보안 프레임워크를 제시하고, 트래픽 매트릭스를 사용해 프레임워크의 효용성을 검증하였다 [13][14].

더불어, 오토모티브 이더넷을 대상으로 하는 위협을 탐지하는 연구도 점차 진행되고 있다. Rumez 등은 서비스 지향 아키텍처를 기반으로 하는 차량 프로토콜에 대한 보안 조치 방식에 대해 설명했다 [15]. 저자들은 일반적인 시스템에서 사용하는 방화벽, 침입탐지 시스템 및 액세스 관리와 같은 방식들이 차량에 적용가능한지에 대해 분석했다. Li 등은 그레이박스(grey box) 퍼저를 개발하여 SOME/IP 응용 프로그램의 취약성을 효율적으로 찾아내는 방법을 제시하였다 [16]. Herold 등은 이벤트 처리 엔진인 에스퍼(Esper)에서 룰 기반의 이상탐지 방법을 제안했다 [17]. 해당 연구에서는 SQL과 유사한 언어인 EPL을 사용해 네트워크 패킷을 검사했다. 하지만 이러한 시그니처 기반의 침입탐지시스템을 만들기 위해서는 차량 내부 통신에 대한 도메인 지식 및 차량 공격에 대한 전문 지식이 필요하여 충분한 공격 시그너처 데이터베이스를 구축하기 어려운 단점이 있다. 또한, 패턴이 변형되거나 알려지지 않은 공격이 발생할 경우 사람이 각각 대응해야 한다는 어려움이 존재한다. Alkhatib 등은 SOME/IP 에서의 딥러닝 기반의 침입탐지 시스템을 제안했다 [18]. 하지만 해당 연구에서는 4가지의 공격만을 탐지했고, 사용한 데이터셋의 공격 클래스의 수 역시 100개 이하로 매우 적다는 한계가 있다.

III. SOME/IP

SOME/IP는 자동차 및 임베디드 시스템에서 제어 메시지에 사용할 수 있는 미들웨어 솔루션으로 확장성에 중심을 두고 설계되었다. SOME/IP는 차량 내의 AUTOSAR를 기반으로 구현된 마이크로 컨트롤러부터 고성능 CPU 기반의 시스템까지 호환된다. 차량의 여러 ECU는 SOME/IP를 이용해 서로에 대한 사전 지식 없이도 통신이 가능하다. 또, 이 통신 표준은 OSI 통신 계층의 5~7 계층에 위치하며, TCP 또는 UDP를 기반으로 통신한다.

Fig.1 은 SOME/IP 패킷의 구조를 시각적으로 나타내고 있다. SOME/IP는 고유의 헤더가 있으며 페이로드는 데이터 직렬화(serialization)가 적용되어있다. 직렬화는 사전에 정의된 매개 변수 목록을 기반으로 최소한의 RAM 및 CPU 리소스를 사용해 복잡한 데이터 유형을 변환하는 기능이다. 또, 메서드의 원격 호출을 통해 메시지를 주고 받는 원격 프로시저 호출 (RPC; Remote Procedure Call)

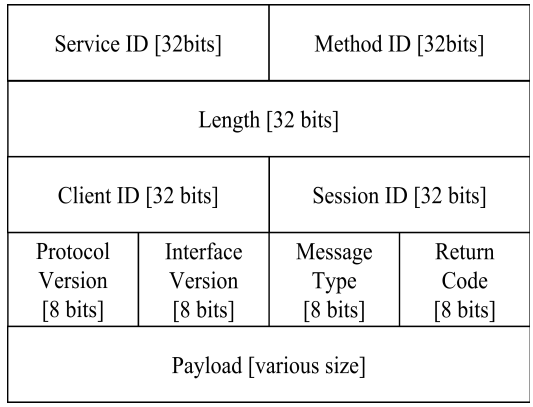


Fig. 1. Format of SOME/IP packet

과 동적으로 서비스를 검색하고 액세스 할 수 있는 서비스 검색 기능도 지원한다. 또한, 패킷 분할 없이 대용량의 SOME/IP 메시지를 UDP를 통해 보낼 수 있다.

더불어, SOME/IP 내에서 통신을 위해 사용할 수 있는 방법은 Request/Response, Fire and Forget, Events, Field 로 총 4가지 방식이 있다. 각 방식에 대한 설명은 Table 1에 정리하였다. 또, SOME/IP에서 에러를 처리하는 방법은 총 2가지이다. 첫 번째는 response 메시지의 return code에 에러 코드를 담는 방법이고 두 번째는 페이로드의 에러 섹션에 담아 보내는 방법이다.

SOME/IP는 자체적인 보안수단이 없어 네트워크 상으로 전송될 때 악의적인 공격에 취약한 상태이다. 예를 들어, 공격자가 두 개의 개별 ECU에 있는 두

Table 1. Specification of SOME/IP

Method	Description
Request/ Response	Common communication patterns between the client and the server. The client sens a request message and the server replies with a response message.
Fire and Forget	A Request message with no response.
Notification Event	Publish/subscribe-Concept communication method. The server forwards updated values or events from the client in a notification event message.
Field	A valid value indicating the status.

애플리케이션 간의 연결에 하이재킹하여 이들 간의 통신을 도청하고 전송하는 데이터를 조작할 수 있다 [11]. 다시 말해, SOME/IP를 이용해 MITM(Man in the Middle Attack) 공격을 수행할 수 있다. 또한 현존하는 대부분의 침입탐지시스템 및 방화벽에서 SOME/IP를 지원하지 않고 있어 문제점이 심각하다고 할 수 있다 [12].

IV. 실험 설계

4.1 데이터 셋

실험에서 사용할 SOME/IP 패킷은 [17]에서 개발한 SOME/IP 패킷 생성기를 이용하여 생성하였다. 패킷 생성기는 우분투(Ubuntu) 리눅스 상에서 Python3를 사용하여 제작하였다. 제작한 패킷 생성기를 이용하여 여러 클라이언트와 서버가 통신하는 상황에서 공격자가 다양한 공격을 시뮬레이션 할 수 있도록 실험을 설계하였다. 수행할 공격은 잘못된 형식의 패킷을 보내거나 프로토콜 및 시스템 내 규칙을 위반하거나 패킷 내 타이밍을 어긋나게 하는 특성을 가진 패킷을 전송하는 시나리오를 상정하였다. 각 공격 별 상세설명은 4.3 절에 기술하였다.

본 논문에서는 패킷 생성기를 이용해 3개의 서비스를 제공하는 환경을 만들며 15개의 클라이언트, 8개의 서버, 1개의 공격자가 통신하는 상황을 재현하였다. 또 데이터셋에는 총 6가지의 공격 클래스(Interval disturbing, ClientId spoofing, Interface spoofing, Fake error, ErrorOnError, ErrorOnEvent)가 포함되며 공격 클래스별 공격 수는 Table 2 에 정리하였으며, 패킷 생성기로 데이터셋을 생성할 때 사용한 파라미터는 Table 3에 정리하였다.

Table 2. Dataset classes

Class	Dataset
Interval disturbing	465
ClientId spoofing	482
Interface spoofing	479
Response drop	453
ErrorOnError	364
ErrorOnEvent	322

Table 3. Packet generator setting parameters

Parameters	Our value
Services	3
Devices	- 15 clients, 8 servers - 1 attacker
Number of the packets to generate per service, client, and method	800
Min, response time of the attacker	1 s
Max. response time of the attacker	3 s

4.2 데이터 전처리

Fig.2에서 보듯이, SOME/IP 패킷 생성기를 통해 6가지 종류의 공격을 생성해 내고, 이때 생성된 패킷을 전처리하여 CSV 포맷으로 저장한 뒤 One hot Encoding 방식을 통해 딥러닝 모델의 입력으로 사용될 수 있도록 하였다.

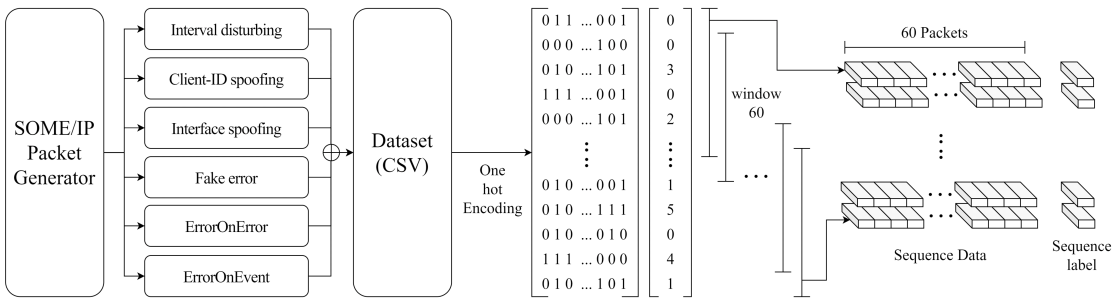


Fig. 2. Data generation and pre-processing

4.2.1 패킷 생성 후 레이블링

우선, 본 연구에서 제작한 SOME/IP 패킷 생성기는 레이블이 없는 pcap 파일을 생성한다. 본 논문에서 제안하는 딥러닝 기반의 침입탐지 모델은 지도학습 방법을 따르기 때문에 추가적인 레이블링 작업이 필요하다. 따라서, 정상 상태는 0으로 레이블링 했고, 공격들은 ClientId spoofing = 1, Fake error = 2, Interval disturbing = 3, ErrorOnError = 4, ErrorOnEvent = 5, Interface spoofing = 6 으로 공격 유형에 따라 1에서 5 사이의 값으로 레이블링 하였다.

4.2.2 피처 탐색 및 One-hot Encoding

레이블링이 완료된 데이터에서 14개의 범주형 데이터를 추출하여 피처로 활용하였다. 관련하여, Table 4에서 사용할 데이터 컬럼 및 해당 데이터에 대한 사항을 정리하였다. 피처로 선택한 데이터 중 MAC 주소, IP 주소 등은 컴퓨터가 이해할 수 있도록 One-hot Encoding 방식을 사용해 이진 벡터로 변환하였다. 최종적으로 14개의 피처는 One-hot Encoding 을 통해 1,702개의 피처로 확장 되었다.

4.3 SOME/IP 공격 유형

본 논문에서 정의하는 SOME/IP 내 공격자는 유효한 MAC 주소, IP 주소, Service ID를 가지며 네트워크 내 모든 패킷을 도청할 수 있다. 따라서, 공격자는 시스템 내 알려진 장치를 손상시킬 수 있으며 다른 장치나 서비스로 가장하여 패킷을 보낼 수 있다 [17].

또, 본 논문에서는 정상적인 방식의 SOME/IP 통신인지 여부를 판단하는데 초점을 두어, 규약을 위반한 통신 시도가 감지되거나 이로 인해 통신 과정에서 발생할 수 있는 이상징후가 발생하는지를 고려했다: 즉, (1) 공격자가 SOME/IP 패킷의 헤더나 페이로드를 변조하여 오작동을 일으키거나 (2) ECU 간의 통신 과정에서 프로토콜 규약 및 해당 시스템 규약을 벗어나거나 (3) 패킷 간의 적절한 시간 간격

Table 5. Description of six attacks in SOME/IP

Attack type	Description
Interval disturbing	Attacker sends packet to deviate from normal time interval.
ClientId spoofing	Send a message disguised as ClientId.
Interface spoofing	Send a message with an invalid interface version.
Fake error	Send a fake response message.
ErrorOnError	Send error message to error message.
ErrorOnEvent	Send error message to event message.

Table 4. Dataset features

Feature	Description	Feature	Description
Source MAC	MAC address of the sending device.	method ID	The identifier for the method.
Destination MAC	MAC address of the receiving device.	Client ID	The identifier for the client.
Source IP	IP address of the sending device.	Session ID	The identifier for the client inside the ECU.
Destination IP	IP address of the receiving device.	Message type	The field used to differentiate types of messages.
Source port	Port number of the sending device.	Return code	The signal whether a request was successfully processed.
Destination port	Port number of the receiving device.	Protocol version	The version of SOME/IP protocol.
service ID	The identifier for the service.	Interface version	The major version of the service interface.

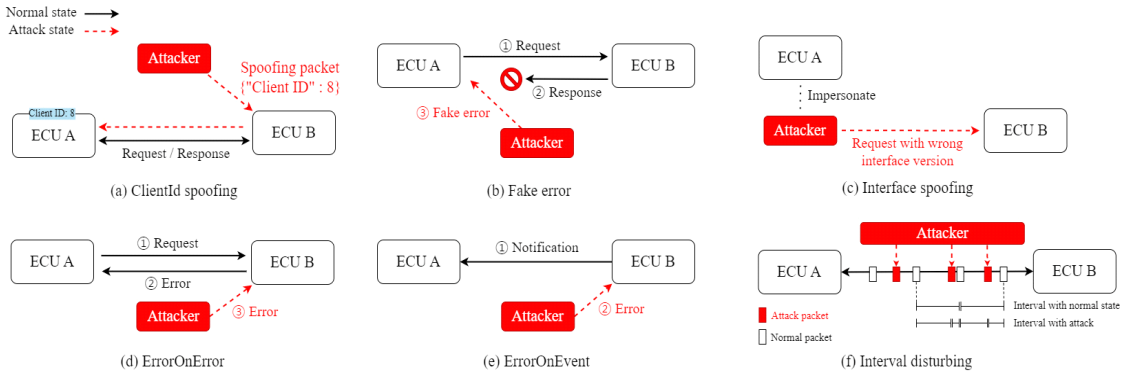


Fig. 3. Process of six attacks in SOME/IP

을 망가뜨리는 것이다. 본 논문에서는 이러한 이상징후를 기반으로 6가지 공격 유형을 다뤘다. 각 공격 유형에 대한 설명은 Table 5와 Fig.3에 요약하였다.

V. SOME/IP 침입 탐지 시퀀셜 모델

네트워크 도메인의 침입 탐지를 위해 다양한 시퀀셜 모델이 사용되고 있다. 시퀀셜 모델은 시간에 대한 값을 기억해두는 특성을 가진다. 시퀀셜 모델은 크게 RNN, GRU, LSTM 종류가 있다. 본 논문에서는 LSTM 시퀀셜 모델에 CNN이라는 합성곱 신경망 모델을 결합한 CNN-LSTM 시퀀셜 모델을 SOME/IP에 대한 침입 탐지를 위해 사용할 것을 제안한다.

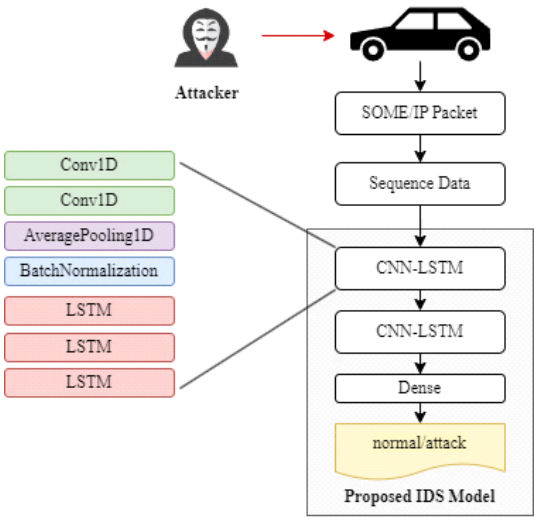


Fig. 4. CNN-LSTM based model structure

CNN-LSTM 모델은 시공간의 연관성을 효과적으로 보존하는 특징이 있다. 특히, CNN-LSTM 모델의 CNN 부분은 SOME/IP 패킷의 추상적인 특징을 추출하며, LSTM 부분은 추출한 특징을 입력으로 받아 시간에 대한 값을 기억하게 하며 이를 통해 순차적인 예측을 가능하게 한다. 즉, SOME/IP 패킷의 순서 정보를 반영함과 동시에 로컬 피처를 잘 반영할 수 있는 장점을 가진다.

본 논문에서 제시한 CNN-LSTM 모델의 구조는 Fig.4에서 볼 수 있다. 본 모델은 ReLU 활성화 함수를 가지는 1차원의 합성곱 층 2개와 각 합성곱 연산으로부터 얻은 결과 벡터에서 평균값을 가진 스칼라 값을 추출하는 풀링층을 추가했다. 그리고 학습 안정화와 빠른 학습 속도를 위한 배치 정규화 층이 있고, 이후 시계열 특징을 학습하는 LSTM 층을 두었다. CNN-LSTM 구조에서 배치 정규화 층과 마지막 LSTM 층 이후에 Drop out 층을 삽입하여 과적합을 방지하고자 하였다. 또한, 입력과 출력층을 제외하고 총 18개의 층으로 구성하였으며, 학습에 사용된 모델의 하이퍼파라미터는 Table 6에 정리하여 두었다. 모델의 CNN-LSTM 구조를 모두 통과하고 나면 Dense 층을 시그모이드 함수를 통해 해

Table 6. Hyper parameters

Hyperparameters	Values
Number of layers	18
Activation function	ReLU, Sigmoid
Optimizer	RMSprop
Loss	Categorical Cross Entropy
Learning rate	0.001

당 결과 값을 7개의 클래스로 분류하도록 하였다.

VI. 실험 결과 및 평가 방법

성능평가를 위해 6.1절에 침입탐지 모델의 성능평가 지표들을 기술했으며, 본 연구의 실험 결과를 6.2절에 정리하였다.

6.1 평가 방법

본 논문에서는 탐지 모델이 추측한 레이블과 정답 레이블을 비교해 confusion matrix를 만든다. 우리는 정상과 6개의 공격, 총 7개의 클래스가 있기 때문에 7x7의 confusion matrix를 얻는다. confusion matrix를 통해 X축에 위치하는 모델의 예측값과 Y축에 위치하는 실제값을 비교할 수 있다. 이상적인 다중 분류 모델의 confusion matrix는 대각선의 항목이 모두 1이어야 하며, 이외의 값은 0이어야 한다.

평가지표로는 정확도(Accuracy), 정밀도(Precision), 재현율(Recall) 및 F1-score를 사용하였다. 각 평가지표들은 아래의 수식을 통해 계산할 수 있다.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\mathrm{Precision} = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1-score = 2 \times \frac{\mathrm{Precision} \times Recall}{\mathrm{Precision} + Recall} \quad (4)$$

마지막으로 AUC-ROC 곡선을 통해 다양한 임계값에서의 모델 분류 성능을 측정하였다. ROC 곡선은 모든 임계값에서의 모델 성능을 나타내며, AUC는 ROC 곡선 아래의 영역을 의미한다. 따라서, 이상적인 ROC 곡선은 X, Y축에 가까이 그려지며 이상적인 AUC는 1에 가깝다.

6.2 탐지 결과

Table 7에 본 연구에서 제안한 모델의 성능과 RNN 및 LSTM 모델의 성능을 비교하여 정리하였다.

Table 7과 Fig.5를 통해 나타난 결과를 살펴보면, CNN-LSTM 모델의 성능이 RNN과 LSTM 모델에 비해 전반적으로 우수함을 확인할 수 있다.

CNN-LSTM 모델은 Fake error, ErrorOnError, Interface spoofing 에 대해 F1-score가 각각 1.00 , 0.99의 높은 성능을 달성하였다. 특히 ErrorOnError 공격의 경우, RNN 모델은 F1-score 0.08, LSTM 모델은 F1-score 0.15에 비해 CNN-LSTM 모델이 높은 탐지율을 보였다. 더불어 ErrorOnEvent 공격의 경우, RNN 모델은 F1-score 0.18, LSTM 모델은 F1-score 0.19에 비해

Table 7. Detection results using existing and proposed methods

Model	class	precision	recall	F1 score
RNN	Normal	0.67	0.74	0.70
	ClientId spoofing	0.33	0.23	0.27
	Fake error	0.87	0.96	0.91
	Interval disturbing	0.96	0.64	0.77
	ErrorOnError	0.14	0.06	0.08
	ErrorOnEvent	0.14	0.24	0.18
	Interface spoofing	0.99	0.99	0.99
LSTM	Normal	0.75	0.77	0.76
	ClientId spoofing	0.54	0.54	0.54
	Fake error	1.00	0.98	0.99
	Interval disturbing	0.83	0.84	0.84
	ErrorOnError	0.30	0.10	0.15
	ErrorOnEvent	0.16	0.24	0.19
	Interface spoofing	1.00	0.99	1.00
CNN-LSTM	Normal	0.92	0.97	0.95
	ClientId spoofing	0.87	0.74	0.80
	Fake error	0.99	1.00	1.00
	Interval disturbing	0.91	0.82	0.86
	ErrorOnError	1.00	1.00	1.00
	ErrorOnEvent	0.99	0.95	0.97
	Interface spoofing	1.00	0.98	0.99

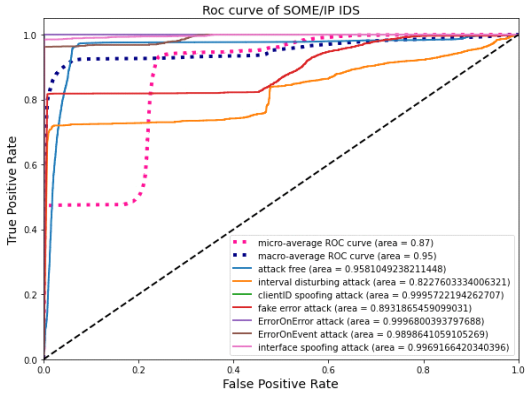


Fig. 5. ROC Curves and AUC values of each class

CNN-LSTM 모델은 F1-score 0.97로 우수한 성능을 달성하였다.

다만, 6가지 공격 중 ClientId spoofing 공격에 대한 F1-score는 다른 공격들에 비해 다소 낮은데, ClientId spoofing은 공격자가 실재 존재하는 디바이스의 ClientId를 가장해 메시지를 보내는 공격으로, 패킷 포맷 및 전송방식은 SOME/IP 사양을 모두 충족시키고 있어 미탐이 발생하기 쉬운 유형이어서 정확도가 다소 낮았을 것으로 판단된다.

VII. Discussion and Limitation

본 연구에서 사용한 데이터셋은 패킷 생성기를 이용하여 최대한 공격 환경을 실제와 유사하도록 시뮬레이션하여 제작되었지만, 실제 차량에서 추출한 게 아니라는 한계점이 있다. 향후에는 오토모티브 이더넷이 구현되어 출고된 실제 차량에 공격을 주입하여 데이터셋을 추출하고, 그 데이터셋을 기반으로 한 침입탐지 실험 결과를 추가할 예정이다. 또한, 이미 다룬 6가지 공격 유형에 머무르지 않고 알려지지 않은 공격을 발견해낼 것이며, 해당 공격을 탐지하는 연구로 확장할 것이다.

본 연구에서 제시된 SOME/IP 용 공격 유형들 및 이에 대한 탐지 알고리즘을 구현하는 시도는 본 연구가 최초라 할 수 있다. 이에, SOME/IP 용 침입탐지 시스템에서 주로 활용해야 하는 피처가 어떤 것인지에 대한 선행 연구들은 아직 부족한 상태여서, 본 연구에서는 피처 선정 (Feature Selection) 과정을 엄격하게 하기 보다는 14개의 범주형 피처를 선택하여 One-hot Encoding하여 총 1,702개의 피처를 사용하는 방식을 택했다. 향후에는 피처 선택에 있어서 유의미한 변수를 선택하는 방법론인 REFCV와 같은 방식을 적용하여 최적화 시킬 예정이다.

본 연구에서 제시한 모델이 다소 낮은 정확도를 보였던 Client spoofing 계열의 공격에 대해서도 탐지율을 높일 수 있도록 모델을 고도화하는 작업이 필요하다고 판단된다.

VIII. 결 론

본 논문에서는 최근 각광받고 있는 SOME/IP 에 향후 발생할 수 있는 잠재적인 침입을 탐지하기 위해, CNN-LSTM 모델의 침입탐지 시스템을 제안하였다.

Fake error, ClientId spoofing, Interval disturbing, Interface spoofing 유형의 SOME/IP 상의 공격을 시퀀셜 모델을 사용하여 탐지를 한 첫 연구이며, 제안한 모델은 각 클래스에 대해 94%의 정확도를 내었고, 평균적으로 0.94의 F1-score, 0.95의 정밀도를 보였다.

본 연구를 통해 향후 오토모티브 이더넷을 탑재하고 출시될 상용 차량들의 내부 네트워크 보안 향상에 기여할 수 있을 것으로 판단된다.

References

[1] NewsRoom, "Advanced driver assistance technology names", https://newsroom.aaa.com/2019/01/common-naming-for-adas-technology/, Accessed: Oct. 2022

[2] HLDI Bulletin, "Predicted availability and prevalence of safety features on registered vehicles - a 2020 update", Vol.39, No.2, pp. 1-16, Apr. 2022

[3] "Automotive ethernet and measurement technology, the link between the past and the future", Techworld, Jun. 2021, 10

[4] Kotra, "Future automotive, global value chain trends and overseas expansion strategies", http://dl.kotra.or.kr/pyxis-api/1/digital-files/c16960f0-1211-018a-e053-b46464899664, Accessed: Oct.

2022
[5] P. Tumas, A. Nowosielski and A. Serackis, "Pedestrian detection in severe weather conditions," IEEE Access, vol. 8, pp. 62775-62784, Jan. 2020
[6] H. Kang, B.I. Kwak, Y.H. Lee, H. Lee, H. Lee, and H.K. Kim, "Car hacking and defense competition on in-vehicle network," Third International Workshop on Automotive and Autonomous Vehicle Security, vol. 2021, pp. 25-30, Feb. 2021
[7] K.H. Park, and H.K. Kim, "This Car is Mine!: Automobile Theft Countermeasure Leveraging Driver Identification with Generative Adversarial Networks," ESCAR ASIA 2019, pp. 1-6, Nov. 2019
[8] IEEE Dataport, "Intrusion detection in CAN bus", https://ieee-dataport.org/documents/intrusion-detection-can-bus#files, Accessed: Dec. 2022
[9] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive ethernet-based networks," Vehicular Communications, Vol. 29, pp. 1-11, Jun. 2021
[10] J. Du, R. Tang, and T. Feng, "Security analysis and improvement of vehicle ethernet SOME/IP protocol," Sensors, vol. 22, no. 18, pp. 1-26, Sep. 2022
[11] Argus, "Hijacking SOME/IP protocol with man in the middle attack", https://argus-sec.com/some-ip-protocol-man-in-the-middle-attack/, Accessed: Oct. 2022
[12] T. Gehrmann and P. Duplys, "Intrusion detection for SOME/IP: challenges and opportunities," 2020 23rd Euromicro Conference on Digital System Design (DSD), pp. 583-587, Aug. 2020
[13] M. Iorio, M. Reineri, F. Risso, R. Sisto and F. Valenza, "Securing SOME/IP for in-vehicle service protection," IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13450-13466, Nov. 2020
[14] M. Iorio, A. Buttiglieri, M. Reineri, F. Risso, R. Sisto and F. Valenza, "Protecting in-vehicle services: security-enabled SOME/IP middleware," IEEE Vehicular Technology Magazine, vol. 15, no. 3, pp. 77-85, Sep. 2020
[15] M. Rumez, D. Grimm, R. Kriesten and E. Sax, "An overview of automotive service-oriented architectures and implications for security countermeasures," IEEE Access, vol. 8, pp. 221852-221870, Dec. 2020
[16] Y. Li, H. Chen, C. Zhang, S. Xiong, C. Liu and Y. Wang, "Ori: a greybox fuzzer for SOME/IP protocols in automotive ethernet," 2020 27th Asia-Pacific Software Engineering Conference (APSEC), pp. 495-499, Dec. 2020
[17] N. Herold, S.A. Posselt, O. Hanka and G. Carle, "Anomaly detection for SOME/IP using complex event processing," 2016 IEEE/IFIP Network Operations and Management Symposium(NOMS), pp. 1221-1226, Apr. 2016
[18] N. Alkhatib, H. Ghauch and J.L. Danger, "SOME/IP intrusion detection using deep learning-based sequential models in automotive ethernet networks," 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 0954-0962, Oct. 2021
[19] Autosar, "SOME/IP protocol specification", https://www.autosar.org/fileadmin/user_upload/standards/foundation/21-11/AUTOSAR_PRS_SOMEIPProtocol.pdf, Accessed: Nov. 2021
[20] A.H. Mirza and S. Cosan, "Computer network intrusion detection using seq

uential LSTM Neural Networks autoencoders," 2018 26th Signal Processing and Communications Applications Conference (SIU), pp. 1-4, May. 2018

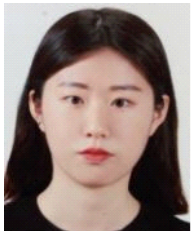
[21] S.A. Althubiti, E.M. Jones and K. Roy, "LSTM for anomaly-based network intrusion detection," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-3, Nov. 2018

[22] A.R. Javed, S.U. Rehman, M.U. Khan, M. Alazab and T.R. G, "CANintelliIDS: detecting in-vehicle intrusion attacks on a controller area network Using CNN and attention-based GRU," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1456-1466, Feb. 2021

〈저자소개〉

강 연 재 (Yeonjae Kang) 학생회원
2020년 8월: 서울여자대학교 수학과 학사
2021년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 자동차 보안, 정보보호, 침입탐지시스템, 네트워크 보안

피 대 권 (Daekwon Pi) 학생회원
2020년 2월: 극동대학교 산업보안학 학사
2021년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 자동차 보안, 위협 인텔리전스



김 해 린 (Haerin Kim) 학생회원
2021년 2월: 세종대학교 지능기전공학부 학사
2021년 3월~현재: 고려대학교 대학원 정보보안학과 석사과정
〈관심분야〉 data-driven security, 이상징후탐지시스템

이 상 호 (Sangho Lee) 학생회원
2018년 2월: 숭실대학교 정보통신전자공학부 학사
2021년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 data-driven security, 개인정보보호

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업 및 시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장. Technical Director
2010년 3월~2014년 12월: 고려대학교 정보보호대학원 조교수
2015년 1월~2020년 2월: 고려대학교 정보보호대학원 부교수
2020년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 온라인게임 보안, 자동차 보안, 침입탐지시스템, 네트워크 보안