ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 22-04-14
j.inst.Korean.electr.electron.eng.Vol.26,No.4,622~627,December 2022
https://doi.org/10.7471/ikeee.2022.26.4.622
99

공격 횟수와 공격 유형을 고려하여 탐지 성능을 개선한 차량 내 네트워크의 침입 탐지 시스템

Intrusion Detection System for In-Vehicle Network to Improve Detection Performance Considering Attack Counts and Attack Types

임 형 철*, 이 동 현*, 이 성 수*★

Hyunchul Im*, Donghyeon Lee*, and Seongsoo Lee*★

Abstract

This paper proposes an intrusion detection system for in-vehicle network to improve detection performance considering attack counts and attack types. In intrusion detection system, both FNR (False Negative Rate), where intrusion frame is misjudged as normal frame, and FPR (False Positive Rate), where normal frame is misjudged as intrusion frame, seriously affect vechicle safety. This paper proposes a novel intrusion detection algorithm to improve both FNR and FPR, where data frame previously detected as intrusion above certain attack counts is automatically detected as intrusion and the automatic intrusion detection method is adaptively applied according to attack types. From the simulation results, the propsoed method effectively improve both FNR and FPR in DoS (Denial of Service) attack and spoofing attack.

요 약

본 논문에서는 공격 횟수와 공격 유형을 모두 고려하여 차량 내 네트워크에서 해킹을 탐지하는 침입 탐지 시스템의 성능을 개선하는 기법을 제안한다. 침입 탐지 시스템에서 침입을 정상으로 잘못 인식하는 FNR(False Negative Rate)과 정상을 침입으로 잘못 인식하는 FPR(False Positive Rate)은 모두 차량의 안전에 큰 영향을 미친다. 본 논문에서는 일정 횟수 이상 공격으로 탐지된 데이터 프레임을 자동적으로 공격으로 처리하며, 자동 공격으로 판단하는 방법도 공격 유형에 따라 다르게 적용함으로서 FNR과 FPR을 모두 개선하는 침입 탐지 기법을 제안하였다. 시뮬레이션 결과 제안하는 기법은 DoS(Denial of Service) 공격과 Spoofing 공격에서 FNR과 FPR을 효과적으로 개선할 수 있었다.

Key words : Controller Area Network, Intrusion Detection System, Random Forest, Machine Learning, In-Vehicle Network, Attack Count, Attack Type

---

* Soongsil University (Master Student, Professor)
★ Corresponding author
E-mail : sslee@ssu.ac.kr, Tel : +82-2-820-0692

※ Acknowledgment
This work was supported by Industrial Technology Challenge Track of the Ministry of Trade, Industry and Energy (MOTIE) / Korea Evaluation Institute of Industrial Technology (KEIT). (20012624) It was supported by the R&D Program of the Ministry of Trade, Industry, and Energy (MOTIE) and Korea Evaluation Institute of Industrial Technology (KEIT). (20008417, RS-2022-00155731)
Manuscript received Dec. 13, 2022; revised Dec. 16, 2022; accepted Dec. 19, 2022.

Ⅰ. 서론

차량 내에 사용되는 ECU(Electronic Control Unit)는 차량 시스템을 제어하는 전자 제어 장치이다. CAN(Controller Area Network) 버스는 ECU 간에 효율적이고 안정적인 통신 채널을 제공하며, 오늘날 대부분의 자동차에 사용되고 있다. 그러나 CAN 버스에는 통신을 보호하기 위한 인증이나 암호화와 같은 보안 기능이 없어 공격자가 쉽게 CAN 버스에 접근할 수 있다. 즉 공격자는 CAN 버스의 취약점을 이용하여 조작된 메시지를 주입하고 차량 시스템을 제어할 수 있다[1]. 이는 차량의 오동작을 일으켜 운전자의 안전을 위협할 수 있다. 따라서 CAN 버스를 외부 위협으로부터 보호하기 위해서는 차량 내 네트워크(IVN: In-Vehicle Network)를 위한 침입 감지 시스템(IDS: Instrusion Detection System)이 필요하다.

IDS를 사용하여 악의적인 공격을 탐지하는 것은 차량 내부에서 구현되는 방법이다. 특히 머신러닝 기반 IDS는 CAN 버스 상의 정상적인 프레임과 비정상적인 프레임을 추출하고 학습한 다음 비정상적인 프레임을 탐지함으로써 공격을 예측할 수 있다[2]. 머신러닝 기반 IDS로는 다양한 모델이 연구되었는데, 서포트 벡터 머신(SVM)을 사용하여 정상 동작을 학습하고 편차를 기반으로 이상 동작을 탐지하는 방법[3]이 제안되었다. 또한 최근접 이웃 알고리즘(Nearest Neighbour)을 이용하여 공격 탐지 정확도를 개선하는 기법[4]이 제안되었다. [5]에서는 정상 및 비정상 프레임으로 분류하기 위해 GBDT(Gradient Boosting)을 사용한 의사 결정 트리(Decision Tree) 기법을 제안했다. GBDT는 최적의 의사 결정 트리 모델을 얻기 위해 여러 트리를 사용하고 훈련시키는 기술이다. 이 밖에도 신경망을 이용하는 딥러닝을 통해 공격을 탐지하는 방안들이 제시되었다[6]-[8].

IDS는 공격을 탐지할 뿐만 아니라 방어 동작까지 수행할 수 있다. IDS에서 공격을 탐지하면 CAN 버스의 에러 프레임을 활용하여 해킹된 노드를 버스 오프 상태로 만드는 기법인 NES(Node Expulsion System)가 제안되었다[9].

그러나 IDS에서 잘못된 판단, 즉 공격을 정상으로 탐지하거나 정상을 공격으로 탐지하는 경우는 오히려 차량 안전에 심각한 영향을 미친다. 이를 해결하기 위해서는 IDS에서 침입을 정상으로 잘못 탐지하는 FNR(False Negative Rate)과 정상을 침입으로 잘못 탐지하는 FPR(False Positive Rate)을 크게 낮추어야 한다.

본 논문에서는 IDS에서 FNR과 FPR을 개선하는 알고리즘을 제안한다. 제안된 알고리즘은 일정 횟수 이상 공격으로 탐지된 데이터 프레임을 자동적으로 공격으로 처리함으로서 FNR을 감소시킬 수 있다. 또한 단순히 공격의 유무를 판단하는 방식이 아니라 공격의 유형까지 분류해주는 방식을 사용하여 FPR도 감소시킬 수 있다.

Ⅱ. CAN 버스 공격 및 탐지

1. CAN 버스의 공격 유형

CAN 버스에 메시지를 주입하기 위해서는 원격으로 접근하는 방법과 물리적으로 접근하는 방법이 있다. 본 논문에서는 그림 1과 같이 OBD-II 포트를 통해 CAN 버스에 악의적인 메시지를 물리적으로 주입하는 세 가지 공격들을 다룬다. 해당 공격들은 실제 현대자동차의 YF 소나타를 테스트 차량으로 주입된 데이터 세트이다[7]. 먼저 DoS(Denial of Service) 공격은 짧은 주기로 '0×000'과 같이 높은 우선 순위를 갖는 CAN 메시지 ID를 주입하여 통신을 방해할 수 있다. 두 번째는 스푸핑(Spoofing) 공격으로 정상적인 식별자를 공격자가 위장하여 악의적인 데이터 프레임을 송신하게 된다. 마지막으로 퍼징(Fuzzing) 공격은 CAN 버스 상에 무작위의 식별자와 데이터를 주입하는 방식이다.

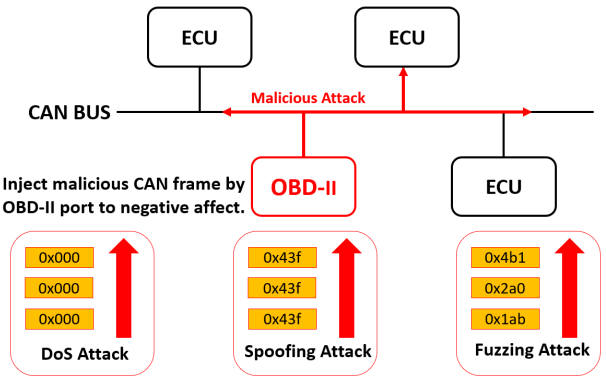

Fig. 1. Types of attack in CAN bus through OBD-II port.
그림 1. OBD-II 포트를 통한 CAN 버스 상의 공격 유형

2. 공격 탐지 방안

CAN 버스에서 공격을 탐지하는 IDS에는 여러 모델이 존재하지만, 본 논문에서는 의사 결정 트리를 이용하는 랜덤 포레스트(Random Forest) 방식을 사용하였다. 랜덤 포레스트 모델에 제공하는 입력 변수(Feature)로는 동일한 메시지 식별자가 버스 상에 나타나는 시간 간격으로 하였다[10]. 또한 데이터 간의 페이로드(Payload)

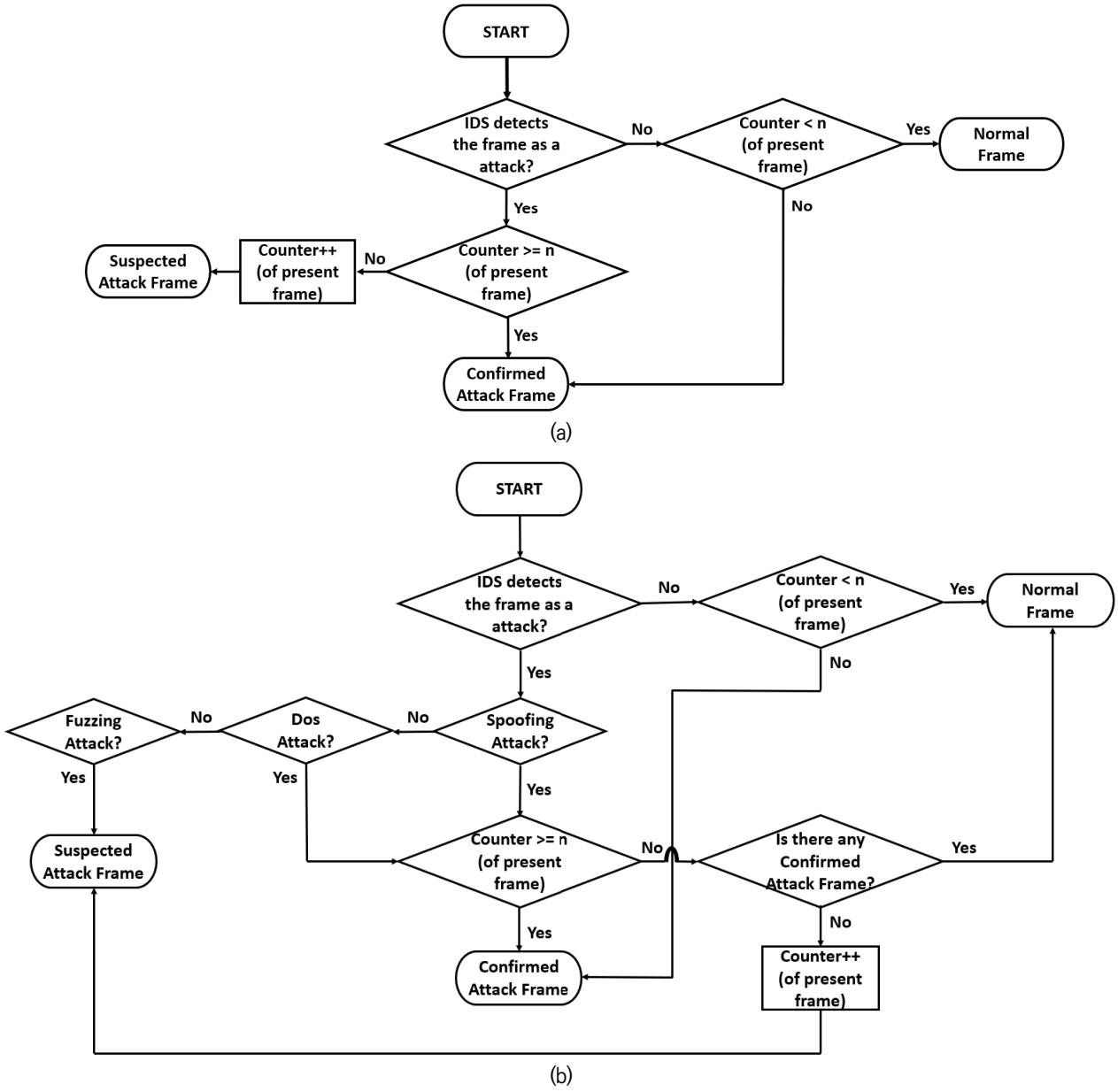

Fig. 2. Proposed algorithm (a) Algorithm based on presence of attack (b) Algorithm based on attack type.
그림 2. 제안하는 알고리즘 (a) 공격 유무에 따른 알고리즘 (b) 공격 유형에 따른 알고리즘

의 변화량을 계산하는 해밍 거리(Hamming Distance)를 입력 변수로 설정하였다[11]. 두 가지 입력 변수로 학습시킨 랜덤 포레스트 IDS의 성능 지표를 표 1에 나타내었다. 정확도와 정밀도를 보면 IDS의 기능을 수행하기에 적합하다고 할 수 있지만 공격을 정상으로 판단한 비율인 FNR이 상당히 높게 나타났음을 알 수 있는데 이는 주행 중인 차량에서 심각한 위험을 초래할 수 있다.

Table 1. Performance of intrusion detection system.
표 1. 침입 탐지 시스템의 성능 지표

Attack Type	FNR	FPR	Accuracy	Precision
DoS Attack	8.52%	0.15%	98.26%	99.33%
Spoofing Attack	6.19%	0.36%	98.54%	98.41%
Fuzzing Attack	1.37%	0.29%	99.51%	98.67%

Ⅲ. 제안하는 알고리즘

1. 공격 유무를 반영한 알고리즘

CAN 버스에서 머신러닝 기반 IDS는 학습된 데이터 세트를 바탕으로 정상적인 프레임과 비정상적인 프레임을 구별하여 공격을 예측한다. IDS의 정확도는 비교적 우수하지만 공격을 정상으로 잘못 탐지하는 확률인 FNR은 더 개선해야 한다. 이를 해결하기 위해 본 논문에서는

그림 2(a)와 같은 알고리즘을 제안한다. 그림 2(a)의 알고리즘에서는 먼저 IDS에서 공격으로 탐지한 프레임은 계속 공격으로 의심하고, 해당 프레임에 대한 공격 탐지 횟수를 증가시킨다. 일정 횟수 이상으로 해당 프레임이 공격으로 탐지된다면 IDS에서 공격으로 탐지하지 않아도 자동적으로 공격으로 처리된다. 이와 같은 방법은 똑같은 프레임을 계속 주입하는 DoS 공격과 스푸핑 공격 방식에서 큰 효과를 볼 수 있다. 표 2를 보면 그림 2(a)의 알고리즘을 적용한 이후 DoS 공격과 스푸핑 공격의 FNR이 급격하게 감소한 것을 확인할 수 있다.

Table 2. Performance applying Fig. 2(a) algorithm.
표 2. 그림 2(a) 알고리즘 적용 이후의 성능 지표

Attack Type	FNR	FPR	Accuracy	Precision
DoS Attack	0%	0.15%	99.88%	99.39%
Spoofing Attack	0%	0.36%	99.71%	98.50%

2. 공격 유형을 반영한 알고리즘

그림 2(a)의 알고리즘을 통해 FNR은 감소했으나 FPR은 변화가 없음을 알 수 있다. FPR은 정상 동작을 공격으로 탐지하는 비율로 FNR에 비해 심각하고 위험한 상태를 초래하지는 않는다. 하지만 0.0001%의 FPR이라고 하더라도 초당 1500 프레임을 브로드캐스팅 하는 CAN 통신에서 1시간마다 5개의 FP(False Positive)가 발생할 수 있다[12]. 따라서 IDS는 더욱 신중하게 공격을 판단할 수 있어야한다. 본 논문에서는 FNR뿐만 아니라 FPR까지 낮추기 위해 단순히 공격의 유무가 아니라 공격의 유형까지 파악하도록 IDS를 학습시키고 그림 2(b)와 같은 알고리즘을 제안한다. 공격의 유형을 파악할 수 있다면, 공격의 특성을 알 수 있어 정상 동작을 공격으로 잘못된 예측을 할 경우에도 적절하게 대처할 수 있다.

그림 2(b)의 알고리즘은 IDS에서 공격 유형을 파악하고 그림 2(a) 방법과 동일하게 공격 프레임을 확정짓는다. DoS 공격과 스푸핑 공격은 동일한 공격 프레임을 주입하기 때문에 공격 프레임이 확정된다면, IDS에서 정상 프레임을 공격 프레임으로 잘못된 판단을 할 경우에도 제안하는 알고리즘을 통해 정상으로 처리될 수 있다. 즉 동일한 프레임을 주입하는 공격 특성을 이용하여 공격 유형을 파악하고 해당 유형에 대한 공격 프레임을 확정짓는다면 IDS의 오탐지를 적절하게 대응할 수 있다. 이는 표 3을 보면 그림 2(b)의 알고리즘을 적용한 이후 DoS 공격과 스푸핑 공격의 FPR도 급격하게 감소한 것을 확인할 수 있다.

Table 3. Performance applying Fig. 2(b) algorithm.
표 3. 그림 2(b) 알고리즘 적용 이후의 성능 지표

Attack Type	FNR	FPR	Accuracy	Precision
DoS Attack	0%	0%	100%	100%
Spoofing Attack	0%	0%	100%	100%

3. 알고리즘 적용 전후 비교

본 논문에서 제안하는 알고리즘의 효과를 검증하기 위해 DoS 공격, 스푸핑 공격, 퍼징 공격에 대한 데이터 세트를 함께 랜덤 포레스트 기반 IDS에 학습시켰다. 또한 훈련에 포함된 데이터 세트가 아닌, 각 공격에 대한 데이터를 규합하여 IDS에 입력하고 예측을 진행하였다. 알고리즘이적용 되기 전의 성능 지표와 적용 이후의 성능 지표를 표 4에 나타내었다. 이를 통해 그림 2(b) 알고리즘을 적용한 이후 FNR은 99.2% 감소하였고, FPR은 62.9% 감소했음을 알 수 있다. 또한 정확도와 정밀도도 상승했음을 알 수 있다.

Table 4. Comparison of performance applying different algorithms.
표 4. 다양한 알고리즘 적용 전후의 성능 지표 비교

Algorithm	FNR	FPR	Accuracy	Precision
Conventioal IDS	5.44%	0.26%	98.77%	98.80%
IDS with Fig. 2 (a) algorithm	0.44%	0.26%	99.70%	98.86%
IDS with Fig. 2 (b) algorithm	0.44%	0.10%	99.84%	99.57%

퍼징 공격에 따른 성능 지표의 차이는 표 2~4의 비교를 통해 알 수 있다. 즉 본 논문에서 제안하는 알고리즘이 퍼징 공격에서는 효과가 미미하다. 이는 퍼징 공격 방식이 무작위의 식별자와 데이터를 주입하는 방식이므로 공격 프레임을 확정지을 수 없기 때문이다. 하지만 제안하는 알고리즘은 DoS 공격 및 스푸핑 공격에 대해서는 [8]에서 비교하는 모든 머신러닝 기반 IDS와 신경망을 이용하는 딥러닝 기반 IDS에도 적용이 가능하다는 장점이 있다.

Ⅳ. 결론

본 논문에서는 IDS에서 발생할 수 있는 오탐지를 해결하기 위한 알고리즘을 제안하였다. 단순히 공격의 유무가 아니라 공격의 유형까지 분류하여 IDS의 잘못된 예측을 보완할 수 있음을 보였다. 이는 차량용 네트워크에서

의 공격 패턴이 잘 알려져 있지 않고 부족한 현재 상황에서 매우 유효한 기법이다. 하지만 제안하는 알고리즘이 DoS 공격과 스푸핑 공격에서는 우수한 결과를 나타내었지만, 퍼징 공격이 발생할 때에는 효과가 떨어짐을 알 수 있다. 따라서 추후에는 퍼징 공격 탐지에 대한 정확도를 높이는 IDS 방안과 오탐지에 대한 해결 방안을 추가로 연구할 필요가 있다.

References

[1] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks - Practical examples and selected short-term countermeasures," *Reliability Engineering & System Safety,* vol.96, no.1, pp.11-25, 2011.
DOI: 10.1016/j.ress.2010.06.026

[2] E. Aliwa, C. Perera, and O. Rana, "Cyberattacks and Countermeasures For In-Vehicle Networks," *ACM Computing Surveys*, vol.54, no.1, pp.1-37, 2020. DOI: 10.1145/3431233

[3] A. Theissler, "Anomaly detection in recordings from in-vehicle networks," *Proceedings of International Workshop on Big Data Applications and Principles,* pp.1-10, 2014.

[4] A. Tomlinson, J. Bryans, and S. Shaikh, "Using a one-class compound classifier to detect in-vehicle network attacks," *Proceedings of Genetic and Evolutionary Computation Conference*, pp.1926-1929, 2018. DOI: 10.1145/3205651.3208223

[5] D. Tian, Y. Li, Y. Wang, X. Duan, C. Wang, W. Wang, R. Hui, and P. Guo, "An intrusion detection system based on machine learning for CAN-Bus," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering,* vol.221, pp.285-294, 2018.
DOI: 10.1007/978-3-319-74176-5_25

[6] M. Kang and J. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol.11, no.6, pp.1-17, 2016. DOI: 10.1371/journal.pone.0155781

[7] E. Seo, H. Song, and H. Kim, "GIDS: GAN-Based Intrusion Detection System for In-Vehicle Network," *Proceedings of Annual Conference on Privacy, Security and Trust,* pp.1-6, 2018.
DOI: 10.1109/PST.2018.8514157

[8] H. Song, J. Woo, and H. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications,* vol.21, pp.100198, 2020.
DOI: 10.1016/j.vehcom.2019.100198

[9] T. Kang, J. Lee, and S. Lee, "Counterattack Method against Hacked Node in CAN Bus Physical Layer," *j.inst.Korean.electr.electron.eng.,* vol.23, no.4, pp.1469-1472, 2019.
DOI: 10.7471/ikeee.2019.23.4.1469

[10] H. Song, H. Kim, and H. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," *Proceedings of International Conference on Information Networking,* pp.63-68, 2016.
DOI: 10.1109/ICOIN.2016.7427089

[11] D. Stabil, M. Marchetti, and M. Colajanni, "Detecting Attacks to Internal Vehicle Networks through Hamming Distance," *Proceedings of AEIT International Annual Conference*, pp.1-6, 2017. DOI: 10.23919/AEIT.2017.8240550

[12] A. Tomlinson, J. Bryans, and S. Shaikh, "Towards Viable Intrusion Detection Methods for The Automotive Controller Area Network," *Proceedings of Computer Science in Cars Symposium,* pp.1-9, 2018. DOI: 10.1145/3273946.3273950

BIOGRAPHY

Hyungchul Im (Member)

2021 : BS degree in Mechanical Engineering, Soongsil University.
2021~ : Candidate for Ph.D degree in Electronic Engineering, Soongsil University.
〈Main Interest〉 Automotive Electronics, Automotive SoC, Sensor Signal Processing

Donghyeon Lee (Member)

2022 : BS degree in Electronic Engineering, Soongsil University.
2022~: Candidate for MS degree in Electronic Engineering, Soongsil University.
〈Main Interest〉 Automotive Electronics, Automotive SoC, Sensor Signal Processing

Seongsoo Lee (Life Member)

1991 : BS degree in Electronic Engineering, Seoul National University.
1993 : MS degree in Electronic Engineering, Seoul National University.
1998 : PhD degree in Electrical Engineering, Seoul National University.
1998~2000 : Research Associate, University of Tokyo
2000~2002 : Research Professor, Ewha Womans University
2002~Now : Professor in School of Electronic Engineering, Soongsil University