CNN–LSTM–Based Intrusion Detection System with Robust Zero-Day Defense in Vehicular Network

Minsu Kim[1], Taeyang Lee[1], Hanyoung Park[2], and Ji-Woong Choi[2]
[1]*School of Undergraduate Studies, DGIST, Daegu, South Korea*
[2]*Department of Electrical Engineering and Computer Science, DGIST, Daegu, South Korea*
Email: {excel2001, sunny626, prkhnyng, jwchoi}@dgist.ac.kr

***Abstract*—With the rapid growth of Vehicle-to-Everything (V2X) communications, ensuring secure and reliable data exchange has become a critical challenge in intelligent transportation systems (ITS). In particular, conventional intrusion detection systems (IDS) often struggle to detect zero-day attacks or maintain effectiveness under ultra-low false positive rate (FPR) conditions. This paper proposes a hybrid Intrusion Detection System (IDS) based on Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) that integrates spatial and temporal modeling to detect complex anomalies in dynamic V2X traffic. The proposed model is evaluated on both known and previously unseen attack scenarios using the CICIDS-2017 dataset, demonstrating robust detection performance under low-FPR constraints. These results highlight the model's practical applicability to safety-critical V2X environments requiring high reliability and real-time responsiveness.**

***Index Terms*—V2X communication, intrusion detection system, deep learning, CNN–LSTM, zero-day attack, false positive rate**

I. Introduction

With the advancement of intelligent transportation systems (ITS), vehicle-to-everything (V2X) communication has become a core infrastructure supporting autonomous driving. V2X enables not only simple information exchange but also supports a wide range of real-time automotive applications such as platooning [1], [2], vehicle-edge computing (VEC) for task offloading [3], [4], remote driving [5], [6], and intersection management [7]. As these applications continue to evolve, the importance of V2X communication is becoming increasingly prominent. However, V2X systems have vulnerability to a wide range of security threats since they rely on the wireless connectivity. Moreover, issues such as incomplete authentication procedures, inadequate key management, and insufficient integrity verification mechanisms may compromise the overall reliability of the system by enabling adversaries to inject forged messages or disrupt communication flows [8]. Given that V2X is a real-time system demanding ultra-low latency (on the order of milliseconds) and reliability exceeding 99.99% [9], these security threats may lead not only to performance degradation but also to immediate system malfunctions or decision-making errors [10]. For instance, Denial-of-Service (DoS) attacks may prevent specific vehicles or infrastructure nodes from participating in communication [10], [11], while replay attacks can mislead the system by injecting outdated but seemingly valid information [8].

To counter these security threats, rule-based intrusion detection systems (IDS) were among the earliest approaches employed [12]. While these systems are effective in detecting predefined attack types through explicit signatures or fixed rules, they face substantial limitations in identifying zero-day attacks that mimic normal traffic behavior [13], [14]. These limitations are particularly pronounced in V2X environments, where highly dynamic traffic patterns resulting from diverse driving scenarios and communication context render static rule-based methods insufficient for detecting real-world anomalies. Specifically, supervised learning models have been employed to distinguish benign communication flows from various types of malicious behavior [13]–[17]. Ali et al. compared the detection performance and training efficiency of various machine learning models, Convolutional Neural Network (CNN), Support Vector Machine (SVM), and Random Forest as suitable candidates for V2X security applications [14]. Sommer and Paxson analyzed the feasibility of ML-based IDS, highlighting the challenges of managing the false positive rate (FPR) and ensuring generalization performance in real-world network environments [13]. Shone et al. devised an anomaly detection model based on a stacked autoencoder architecture and validated its capability in isolating malicious behaviors within complex traffic flows [15]. Kim et al. implemented a hybrid Convolutional Neural Network–Bidirectional Long Short-Term Memory (CNN–BiLSTM) architecture for real-time detection through V2X simulation experiments, achieving a consistently high true positive rate (TPR) [16]. Additionally, Zhang and Yan introduced a Random Forest-based IDS designed for online analysis of large-scale traffic in Vehicular Ad-hoc Network (VANET) environments, achieving superior detection performance and processing efficiency compared to traditional rule-based methods [17]. These studies reinforce the feasibility of real-time V2X security systems by offering improved detection flexibility and automated feature learning capabilities, in contrast to conventional signature-based approaches.

However, previous works predominantly have considered static training and testing environments with predefined attack types. As a result, their detection performance against previously unseen threats, such as zero-day attacks, has not been thoroughly validated. This suggests that existing detection

models exhibit limited generalization capabilities, particularly considering that previously unseen attack types may arise in real-world V2X deployments without prior exposure during training. Korba et al. pointed out the limited capability in detecting zero-day attacks of supervised learning-based models and proposed a federated learning-based architecture that enables model training without sharing raw data [18]. Similarly, Xu et al. employed data augmentation techniques for detecting zero-day attacks in IoV scenarios [19]. However, both approaches do not explicitly consider FPR control and were evaluated under constrained settings that do not adequately reflect the operational requirements of V2X environments, including ultra-low latency, high reliability, and scalability under dynamic vehicular traffic conditions.

Additionally, in V2X systems, one of the most critical considerations for practical deployment is minimizing the FPR. In real-world operations, a high FPR not only undermines operator trust and delays timely responses but also leads to alert fatigue in automated systems, ultimately reducing both alert reliability and operational efficiency [20]. Nevertheless, many prior studies have focused primarily on performance metrics such as average F1-score or the area under the receiver operating characteristic curve (ROC-AUC), with limited attention to performance in low-FPR regions—particularly, how the TPR varies when the FPR is constrained to 0.01 or below [13], [18]. To overcome these limitations, this study proposes a ML-based IDS designed to maintain high TPR under low-FPR conditions and enhance robustness against zero-day attacks. The main contributions of this study are as follows:

- We propose a CNN–LSTM-based IDS, where the CNN layers extract local spatial patterns from V2X packet flows and the LSTM layers capture temporal dependencies and inter-packet correlations to effectively detect complex anomalies.
- To validate the effectiveness of the proposed approach, we evaluate its performance against both known and zero-day attacks in V2X communication scenarios. Additionally, we compare it with representative supervised learning-based models, including Decision Tree, Random Forest, XGBoost, LightGBM, and LSTM. Simulation results demonstrate that the proposed method outperforms baseline models in both known and zero-day attack scenarios, particularly under low-FPR conditions, highlighting its robustness and generalization capability in dynamic V2X environments.
- We analyze TPR behavior under an ultra-low-risk region of FPR < 0.01, which is not deeply scrutinized in previous works. The simulation results show that the proposed method markedly outperforms baseline approaches in terms of effectiveness and stability under the low-FPR constraint.

The remainder of this paper has the following structure. Section II describes the proposed CNN–LSTM-based IDS model. Section III explains the simulation configuration, and performance analysis under both known and zero-day attack scenarios, with a particular focus on low-FPR conditions. Finally, Section IV summarizes the paper.

II. Proposed Method

A. CNN+LSTM Architecture

This paper presents a hybrid deep learning framework that combines CNN and LSTM architectures to capture both local and sequential characteristics of V2X traffic. The CNN component extracts localized spatial dependencies among packet flow features, whereas the LSTM component learns long-range temporal dynamics across sequential traffic patterns. The overall architecture of the proposed CNN+LSTM model is shown in Fig. 1. The input consists of a sequence of network flows, where each flow is represented as a fixed-length vector of normalized numerical features. The CNN layers apply one-dimensional convolution to extract spatial dependencies across adjacent flows and detect abrupt deviations or structural anomalies. Subsequently, the extracted spatial features are passed to stacked LSTM layers, which capture long-range temporal dependencies and recurring traffic patterns. A final dense layer with a sigmoid activation function produces a binary classification output, indicating whether the input sequence is benign or malicious. By jointly learning spatial correlations and temporal evolution of traffic patterns, the framework effectively identifies complex attack signatures, which enhances detection robustness in dynamic V2X environments.

B. Attack Scenarios and Dataset

Connected vehicular systems are vulnerable to a wide range of cyber threats since they rely on real-time communication among vehicles, Roadside Units (RSUs), and cloud infrastructure. This study focuses on representative attack types that reflect practical security threats in V2X environments.

- **DoS/DDoS:** These attacks overwhelm centralized components in Vehicle-to-Infrastructure (V2I) or Vehicle-to-Network (V2N) communication, such as RSUs and traffic management servers, by generating excessive traffic. As a result, they can disrupt congestion control, signal timing, and emergency vehicle coordination.
- **PortScan:** Attackers use PortScan techniques to probe RSUs or On-Board Units (OBUs) for open ports and vulnerable services. This activity typically serves as a reconnaissance phase prior to executing more targeted intrusions.
- **Infiltration:** These attacks exploit security flaws in V2X interfaces to gain unauthorized access to internal Electronic Control Units (ECUs). Once compromised, attackers may manipulate sensor data or interfere with vehicle control logic.
- **Heartbleed:** These attacks target known vulnerabilities in the Transport Layer Security (TLS) protocol to extract sensitive information, such as GPS coordinates or cryptographic keys, especially in Vehicle-to-Cloud (V2C) communications.

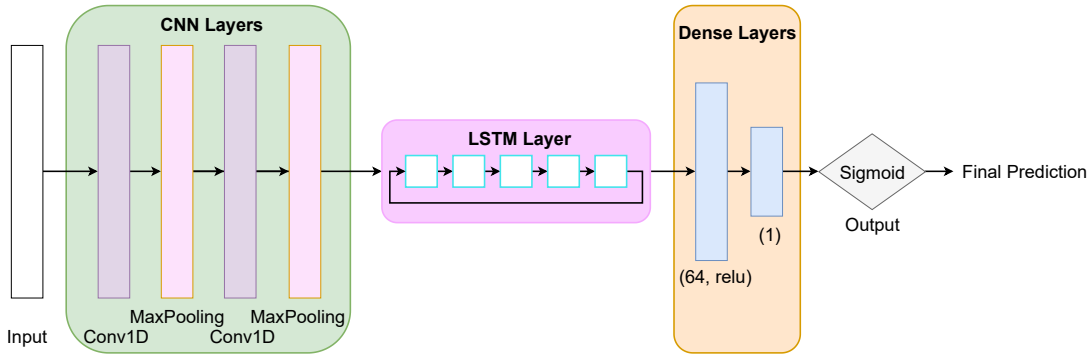

Fig. 1. CNN+LSTM architecture.

The CIC-IDS2017 dataset is utilized for empirical evaluation, as it provides labeled instances of both benign and malicious network flows. All attack categories are relabeled into binary labels: `BENIGN` or `ATTACK`. To evaluate generalization and zero-day performance, the dataset is divided as follows.

- **Training Set:** It consists of benign flows and DDoS attack traffic collected on Friday. It is augmented with additional benign flows from Monday to improve diversity.
- **Known Attack Test Set:** The known attack test set includes DoS attacks such as Slowloris, Slowhttptest, and Hulk. These attacks are similar in nature to the training data but are excluded from training to evaluate generalization.
- **Zero-Day Attack Test Set:** The zero-day attack test set contains previously unseen threats such as Heartbleed, PortScan, and Infiltration. These are used to assess the model's robustness against novel or mutated attacks.

C. Data Preprocessing and Sequence Construction

To support temporal modeling, the system organizes network flows into fixed-length sequences using a sliding window of size 30. Each sequence contains 30 consecutive flows and is labeled based on the class of the last flow, simulating real-time inference conditions where only past and current observations are available.

For deep learning models, only numerical features are used as input. String-based attributes, including IP addresses, are converted into integer representations to ensure compatibility with neural network architectures. All input features are normalized using Min-Max scaling. Flow records containing missing or corrupted values are excluded from training and evaluation. In contrast, tree-based models operate on individual flow instances without sequence construction, serving as non-temporal baselines for comparative evaluation. This preprocessing strategy enables the proposed deep learning models to exploit temporal dependencies across flows while providing a consistent input format across all model types.

III. Simulation Results

A. Simulation Environments

All experiments are conducted on a PC equipped with two NVIDIA RTX 3080 GPUs and an Intel i9-10900X CPU running at 3.7 GHz. Deep learning models are implemented using TensorFlow, while tree-based models are implemented using Scikit-learn, XGBoost, and LightGBM libraries.

B. Baseline Models and Evaluation Strategy

To evaluate the effectiveness of the proposed CNN+LSTM model, we conduct comparative experiments with several baseline models. As deep learning-based baselines, we consider a CNN-only model that extracts local spatial patterns using stacked one-dimensional convolution and pooling layers, and an LSTM-only model that captures temporal dependencies through stacked LSTM layers. These models are designed to isolate the individual contributions of spatial and temporal modeling, respectively, and serve as ablation baselines for the proposed hybrid architecture. The structures of the CNN-only and LSTM-only models are illustrated in Fig. 2 and Fig. 3, respectively. In addition to the deep learning baselines, we evaluate four representative tree-based classifiers: Decision Tree, Random Forest, XGBoost, and LightGBM [14]. Unlike neural network-based models, these algorithms treat each flow as an independent sample without modeling temporal dependencies, thereby serving as non-sequential learning baselines. All models are trained and tested using the same dataset partitions described in Section II-B. Hyperparameters for the deep learning and tree-based models are summarized in Table I and Table II, respectively. Deep learning models are trained using a unified configuration, while tree-based models are individually tuned according to commonly adopted best practices for each algorithm.

Model performance is assessed using standard binary classification metrics, including accuracy, precision, recall, F1-score, and AUC. In addition, we specifically evaluate the TPR under a low FPR (< 0.01), which is critical for latency-sensitive and safety-critical applications such as V2X.

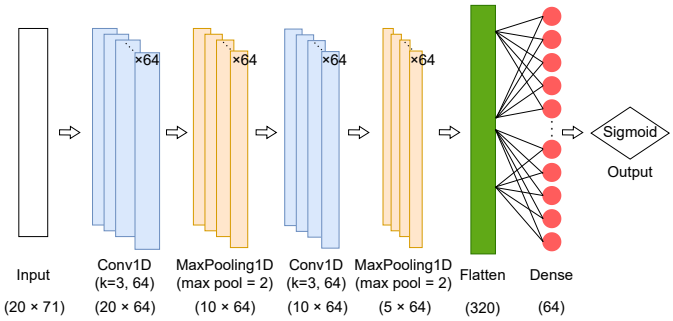

Fig. 2. Baseline CNN model architecture.

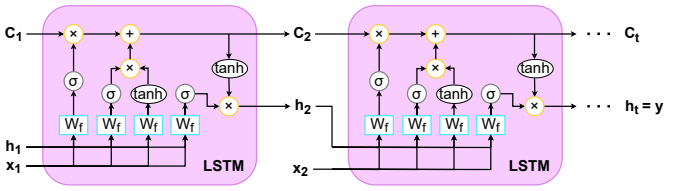

Fig. 3. Baseline LSTM model architecture.

C. Performance on DoS/DDoS Attacks

To evaluate the generalization capability of the proposed model on previously excluded but similar attack categories, we test it on DoS and DDoS samples excluded during training. Table III presents the performance of each model. The proposed CNN+LSTM architecture achieves the best overall results, with a recall of 0.97 and an F1-score of 0.98. While the CNN model also demonstrates strong recall (0.96), its relatively lower precision results in more false positives. On the other hand, the LSTM model maintains more balanced precision but exhibits a slightly lower recall (0.94), indicating that relying solely on temporal dependencies may limit detection of short-duration anomalies. These outcomes highlight the complementary nature of spatial and temporal modeling, which the hybrid architecture successfully integrates. Among the tree-based models, XGBoost and LightGBM exhibit competitive F1-scores of 0.97, comparable to those of the deep learning models. Decision Tree and Random Forest perform significantly worse, achieving F1-scores of only 0.89 and 0.77, respectively. Their performance is constrained by their inability to learn from sequential flow structures, leading to overfitting on simple patterns and failure to handle dynamic traffic behaviors.

TABLE I
HYPERPARAMETERS FOR DEEP LEARNING MODELS

Parameter	**Value**
Batch Size	256
Epochs	50
Optimizer	SGD
Loss Function	Binary Cross-Entropy
Early Stopping	Patience = 5 (monitoring validation loss)

TABLE II
HYPERPARAMETERS FOR TREE-BASED MODELS

Model	Max Depth	N_estimators	Learning Rate	Early Stop
Decision Tree	10	–	–	–
Random Forest	10	100	–	–
XGBoost	10	1000	0.2	75 (logloss)
LightGBM	10	500	0.1	50 (logloss)

TABLE III
PERFORMANCE ON KNOWN DOS/DDOS ATTACKS

Model	Accuracy (%)	Precision	Recall	F1-score
CNN+LSTM	98.43	0.98	0.97	0.98
LSTM	97.11	0.97	0.94	0.95
CNN	95.90	0.92	0.96	0.94
Decision Tree	91.41	0.83	0.96	0.89
Random Forest	88.71	1.00	0.62	0.77
XGBoost	97.17	1.00	0.95	0.97
LightGBM	98.29	0.98	0.96	0.97

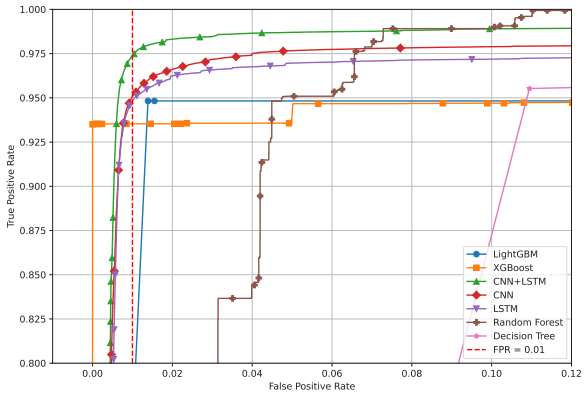

Fig. 4. ROC curves for known DoS/DDoS attacks

To further investigate performance under stringent operational conditions in V2X environments, we analyze ROC curves in the low-FPR region, as illustrated in Fig. 4. The proposed architecture maintains a TPR of 0.98 under this constraint, outperforming CNN (0.94), LSTM (0.91), XGBoost (0.96), and LightGBM (0.81). In contrast, Decision Tree and Random Forest yield TPRs below 0.1, indicating their limited applicability under low-risk and high-reliability conditions. This implies that the proposed architecture achieves superior detection of DoS and DDoS attacks, especially under low false positive constraints, by capturing both bursty and repetitive patterns in network traffic. These results highlight the operational benefits of spatio-temporal modeling in enhancing detection reliability in latency-sensitive settings.

D. Performance on Zero-Day Attacks

In the zero-day detection scenario, where attack types are not seen during training, the proposed architecture demonstrates the highest performance. As shown in Table IV, the CNN+LSTM model achieves an F1-score of 0.98 and a recall of 0.99, outperforming all baseline models. The CNN model

TABLE IV
PERFORMANCE ON ZERO-DAY ATTACKS

Model	Accuracy (%)	Precision	Recall	F1-score
CNN+LSTM	97.42	0.96	0.99	0.98
LSTM	93.22	0.97	0.91	0.94
CNN	96.61	0.95	0.98	0.97
Decision Tree	47.94	1.00	0.06	0.12
Random Forest	44.31	0.16	0.00	0.00
XGBoost	55.48	0.89	0.03	0.07
LightGBM	44.52	0.00	0.00	0.00

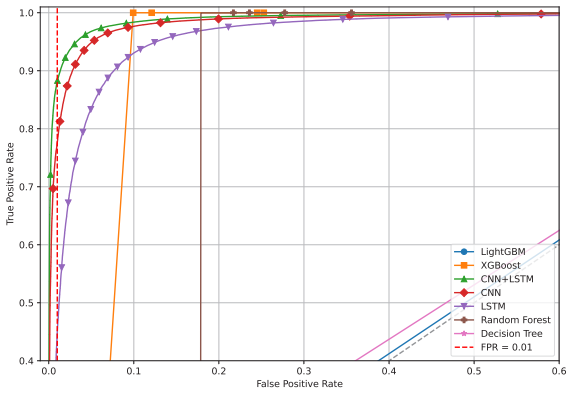

Fig. 5. ROC curves for zero-day attack detection

also delivers strong results with an F1-score of 0.97 and a recall of 0.98, indicating its effectiveness in capturing short-term, localized anomalies. The LSTM model attains a recall of 0.91 and an F1-score of 0.94, reflecting its strength in modeling long-term dependencies but limited capability in detecting abrupt or short-lived attacks. In contrast, all tree-based models—including Decision Tree, Random Forest, XGBoost, and LightGBM—exhibit recall values below 0.1, indicating poor generalization to previously unseen threats.

As shown in Fig. 5, the CNN+LSTM model maintains a TPR of 0.98 under a strict FPR constraint of 0.01, which is critical for reliable intrusion detection in V2X systems. The CNN model maintains a TPR of 0.96 under the same condition, ranking second among all models. This result demonstrates that CNN is highly effective in detecting localized anomalies, even without explicitly modeling temporal information. The LSTM model achieves a TPR of approximately 0.85, suggesting that relying solely on temporal modeling may limit the detection of sudden or irregular patterns. Tree-based models fail to achieve meaningful TPR values under low-FPR constraints, further confirming their limitations under distribution shifts. These findings confirm that the integration of spatial and temporal modeling is essential for resilient zero-day attack detection. The proposed CNN+LSTM architecture exhibits strong generalization capabilities against previously unobserved and evolving traffic behaviors, maintaining high detection reliability even under distribution shifts.

IV. CONCLUSION

In this paper, we proposed an IDS based on the hybrid architecture of CNN–LSTM to address the security challenges of V2X communications. By combining spatial and temporal modeling, the proposed CNN+LSTM architecture effectively detects both localized and sequential anomalies in network traffic. Experimental result demonstrated that the proposed method consistently outperforms conventional machine learning and single-stream deep learning baselines under both known and zero-day attack scenarios. In particular, the model maintained a high TPR under an ultra-low FPR threshold of 0.01, which is critical for deployment in safety-critical and latency-sensitive V2X environments. Such robustness is particularly important in dynamic V2X settings, where traffic characteristics and threat vectors change rapidly and timely intrusion response is essential for maintaining operational safety.

ACKNOWLEDGMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) under the projects No. RS-2024-00442085, “Development of Core Technologies for Securing V2X Wireless Communication Infrastructure for Autonomous Vehicle Services,” and No. RS-2024-00398157, “Development of 6G System Technologies Supporting AI-Native Application Services.”

REFERENCES

[1] J. Wang, X. Li, J. Guo, and K. Li, “Self learning-based platooning control strategy for connected autonomous vehicles with switching topologies,” *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 12, pp. 19 842–19 851, Dec. 2024.
[2] H. Park, Y. Jang, and J.-W. Choi, “Channel charting-based vehicle position estimation in real-world coordinates of lanes,” in *Proc. 16th Int. Conf. Ubiquitous Future Netw.*, 2025.
[3] A. K. Sinthia, N. I. Mahbub, and E.-N. Huh, “Optimizing proactive content caching with mobility aware deep reinforcement and asynchronous federate learning in vec,” *ICT Express*, vol. 11, no. 2, pp. 293–298, 2025.
[4] J. Kwak and et al., “An integrated network-computing load balancing simulator for vec-assisted autonomous vehicles,” *IEEE Commun. Mag.*, vol. 63, no. 6, pp. 146–153, 2025.
[5] H. Park, Y. Jang, K. Ko, and J.-W. Choi, “Energy consumption analysis of 5g c-v2x sensor sharing for tele-operated driving,” *IEEE Access*, vol. 13, pp. 42 547–42 588, 2025.
[6] H. Park, Y. Jang, and J.-W. Choi, “Latency analysis of 5g c-v2x real-time video transmission over different channel states,” in *Proc. IEEE 101st Veh. Technol. Conf. (VTC)*, 2025, pp. 1–6.
[7] C. Zhang and et al., “Evaluation of an infrastructure-based warning system: A case study on roundabout driving behaviors,” *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 5, pp. 6056–6069, May 2025.
[8] J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
[9] 5GAA, “Evaluation methodology for new radio v2x use cases,” Technical Report, Munich, Germany, Jul. 2024.
[10] N. Trkulja, D. Starobinski, and R. A. Berry, “Denial-of-service attacks on c-v2x networks,” pp. 1–8, 2021.
[11] K. Kim, D. Kwon, W.-C. Jin, S. Choi, J. Kim, and J.-W. Choi, “Fatal c-v2x denial-of-service attack degrading quality of service in a highway scenario,” *J. Commun. Netw.*, vol. 26, no. 2, pp. 182–192, Apr. 2024.
[12] T. Venkatasamy, M. J. Hossen, G. Ramasamy, and et al., “Intrusion detection system for v2x communication in vanet networks using machine learning-based cryptographic protocols,” *Sci. Rep.*, vol. 14, p. 31780, 2024.

[13] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Secur. Privacy*, 2010, pp. 305–316.
[14] M. Ali, S. Khan, M. S. Hossain, and M. Alhamid, "A comprehensive survey and tutorial on smart vehicles: Emerging technologies, security issues, and solutions using machine learning," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2371–2415, 2022.
[15] S. Shone and V. N. Ngoc, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.
[16] H. Kim, J. Park, and H. Kim, "An intrusion detection system for v2x communication using hybrid deep learning architecture," *Sensors*, vol. 21, no. 21, p. 7340, 2021.
[17] M. Zang and Y. Yan, "Machine learning-based intrusion detection system for big data analytics in vanet," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, Apr. 2021, pp. 1–5.
[18] A. A. Korba, A. Boualouache, B. Brik, R. Rahal, Y. Ghamri-Doudane, and S. M. Senouci, "Federated learning for zero-day attack detection in 5g and beyond v2x networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Rome, Italy, 2023, pp. 1137–1142.
[19] Y. Xu, Z. Zhang, Y. Liu, H. Liu, and M. Zhang, "Detection of zero-day attacks via sample augmentation for the internet of vehicles," *Veh. Commun.*, vol. 43, p. 100887, 2025.
[20] C. M. Layman and D. M. Roden, "The impact of false positive rates on operator performance in security systems," *Comput. Secur.*, vol. 126, p. 102970, 2023.