Journal of Applied Automation Technologies

Research Paper

Communication Anomaly Behavior Detection Method for Internet of Vehicles Based on Long-Context Mamba

Leon Stasiak[1,*], Urszula Królowa[1] and Irena Patrycja Kotowska[1]

[1] Faculty of Information Technology, University of Silesia in Katowice, Katowice, 40-007, Poland
*Corresponding author: leon.st@us.edu.pl

Abstract. Low-latency anomaly detection models for the Internet of Vehicles need to be developed that can identify malicious communication behaviour in long and noisy traffic sequences. Vehicle messages have various time correlations for identity authentication, packet intervals, neighbor interactions, routing states and channel occupancy; however, these correlations are often reduced due to packet loss, dynamic topologies and bursty traffic. A High-efficiency long-context Mamba detection model for vehicular communication anomaly recognition is proposed in this paper. A behaviour-window construction strategy will be introduced first to align the variables of vehicle-to-vehicle and vehicle-to-infrastructure communication. A long-context Mamba block then selectively updates the state to remember previous abnormal evidence and reduce computational cost. A calibrated detection head has increased the recall rate for minority attacks and reduced false alarms. Experimental results are compared with those of classic machine learning, recurrent neural networks, temporal convolutions and attention-based methods. The model has reached 95.6% anomaly recall, 96.3% macro-F1, and a 5.8ms inference delay in the edge-device simulation. The Framework can perform real-time security monitoring of a dynamic vehicle communication environment.

Keywords: *Long-Context Mamba, Communication Security, Anomaly Behavior Recognition, Selective State Space*

Received on 27 February 2023, Accepted on 04 August 2023, Published on 14 August 2023

Introduction

The Internet of Vehicles is now an essential communication foundation for collaborative perception, autonomous driving assistance, intelligent traffic management, roadside perception, and vehicle-cloud collaborative services. The connections between vehicles, vehicles and infrastructure, and vehicles and the cloud continuously exchange status information, safety beacons, routing information, authentication requests, and service responses. The information can be used by vehicles and roadside units for lane change coordination, collision warnings, congestion avoidance, and emergency response. As vehicle connectivity and software-defined capabilities continue to improve, system security is now directly related to people's lives and the safe operation of traffic [1]. Therefore, due to the rapid spread of malicious communication in dynamic vehicle clusters, intrusion detection methods for the Internet of Vehicles have gradually attracted people's attention [2]. Many studies on multi-layer intrusion detection, optimized convolution detection, and tree-based vehicle safety models have identified that intelligent traffic safety requires communication anomaly detection [3].

However, the technical challenges of anomaly detection in vehicular network communication still persist. The vehicular network has a constantly changing topology, unstable traffic density, various types of information, and strong temporal correlation. Identity spoofing, replay attacks, denial of service, malicious routing responses, CAN bus injection, and hybrid anomalous traffic attacks are usually not limited to the packet level but gradually develop over longer communication cycles [4]. Deep learning methods can enhance detection capabilities, but CNN-based models are often local, recurrent models may forget distant evidence, and attention models similar to Transformers are relatively expensive for long-duration vehicle sequences [5]. Research on in-vehicle

intrusion detection also indicates that due to roadside and in-vehicle edge devices not always being able to provide large amounts of memory or high computational power, lightweight inference is required [6]. Therefore, the issues of detection accuracy for long contexts and real-time deployment costs remain prominent [7].

This paper proposes a method for detecting abnormal behavior in vehicular network communication based on long-context Mamba. The method for constructing the behavior window is Through packet intervals, message frequency, protocol conversion, identity consistency, channel occupancy, routing response, and neighbor interaction variables. Then, a selective state space mechanism is employed to retain long-range anomaly evidence with near-linear sequence processing costs. Improve anomaly recall rate, reduce false positives under dynamic vehicle density, and maintain low inference latency in edge deployment. The new model aims to identify burst attacks and slowly developing anomalous behaviors in real automotive communication data.

Related Work

Communication Anomaly Detection in Internet of Vehicles

Various research directions on communication anomaly detection in the Internet of Vehicles have been explored, including CAN bus intrusion detection, roadside traffic monitoring, wireless message authentication, and roadside anomaly detection. Transfer learning has been used to improve intrusion detection performance under different vehicle traffic distributions in the dataset [8]. CNN-based and multi-layer hybrid intrusion detection systems perform well on known vehicle attack types, but they often rely on short window representations or hierarchical classifiers [9]. Machine learning methods for CAN bus and in-vehicle networks can detect injected frames, anomalous timing, and malicious message IDs; however, their performance may decline when attack behaviors are temporally sparse or deliberately delayed [10].

Recently, some research has focused on lightweight and interpretable detection. Binary neural networks reduce the inference cost of in-vehicle intrusion detection, while graph-based anomaly frameworks can also learn the structural relationships between messages and electronic control units [11]. The interpretable voting mechanism and interpretable lightweight systems also indicate that vehicle safety for deployment requires both accurate outputs and understandable evidence [12]. However, many of the methods still use fixed-length feature vectors to represent communication behavior. The design may not be able to capture long-range dependencies, such as the replay behavior of valid messages after a certain delay, or routing anomalies that only become apparent after multiple interaction cycles.

Vehicle communication anomalies are also classified as network intrusions. According to deep learning research, intrusion detection models need to address issues of representational capacity, data imbalance, and generalization under unknown attacks [13]. Research on anomaly detection in wireless sensors and the Internet of Things has also found that packet loss, sampling noise, and environmental fluctuations can reduce the effectiveness of traditional classifiers [14]. Vehicular networks have a high density of vehicles and fluctuating channel loads, so these issues are more pronounced. Therefore, a useful detection model should have the ability to retain long-term temporal context and maintain a relatively small size on edge devices.

Efficient Long-Sequence Models for Network Security

Many networks have been used for time series research. CNN-LSTM, autoencoder-LSTM, and other hybrid recurrent models can extract temporal dependencies in intrusion traces [15]. Two-stage anomaly detection and Bayesian deep learning schemes improve the robustness of network intrusion detection, but recursive computations are relatively slow in extended communication windows [16]. Informers are long sequence prediction models that can improve the efficiency of extending time-step attention [17]. Predictable sparse attention and relaxed transition mechanisms also indicate that by selecting certain information instead of using full attention, long-range sequence modeling can be performed more efficiently [18]. Autoencoder-LSTM used for intrusion detection also indicates that compressed temporal states can be used to represent the evolution of traffic anomalies [19].

The changes are related to vehicle communication, and abnormal evidence is usually distributed over a longer context. Deceptive attacks may initially manifest as a small identity inconsistency, while replay attacks may require comparing the current message with previous valid patterns. If the model has already stored previous

channel occupancy and packet interval data, DoS behavior may appear as normal congestion. Therefore, long context state modeling can distinguish between malicious behavior and legitimate high-density traffic. Practical research on CAN bus and the Internet of Things also indicates that connected vehicle applications require integrated, interpretable, federated, and lightweight detection designs [20]. The integration of decision-based Internet of Vehicles (IoV) enhances attack separation capabilities but does not explicitly address long-term memory issues [21]. Real-time connected vehicle anomaly detection also indicates the need for interpretable temporal evidence [22]. Research on distributed anomaly detection in federated learning indicates that different vehicles have different traffic sources [23]. However, the memory growth of the full attention mechanism is quadratic with respect to the sequence length, making it unsuitable for handling thousands of message windows on roadside units.

State space and class recursive sequence models provide an alternative approach. Informer is a long-sequence attention model that reduces computational load by using sparse dependencies [24]. Predictable sparse attention and relaxed transition mechanisms have also been proposed to help sequence models retain distant evidence without exhaustive pairwise comparisons [25]. Efficient recursive sequence models also support the feasibility of compact state propagation [26]. Research on explainable artificial intelligence indicates that detection models should provide verifiable evidence, not just category labels [27]. Tree explanation methods and prediction effect visualization provide references for interpreting safe decisions [28]. In this paper, the term "long-context Mamba" refers to a selective state space detection block that updates the communication memory based on input dependency gates. The goal is not to increase the complexity of the architecture, but to retain anomalous evidence in vehicle communication for a longer period with lower inference costs [29]. This design is also consistent with the interpretable feature-effect analysis of black-box predictions [30].

Efficient Long-Context Mamba Detection Framework

Communication Window Construction and Feature Alignment

The proposed model receives communication logs generated by vehicles, roadside units, and edge gateways. Each record contains a timestamp, message identifier, source identity, target identity, packet length, message interval, protocol status, routing response, channel occupancy rate, authentication result, and local neighbor density. To avoid treating each packet as an isolated event, messages are grouped into overlapping behavior windows. Each window contains 256 consecutive communication events, with an overlap of 64 events between adjacent windows to maintain the continuity of the attack transition.

$$X_t = [b_t, p_t, i_t, r_t, c_t, n_t] \quad \text{Eq.(1)}$$

Here, b_t denotes basic packet statistics, p_t denotes protocol-state variables, i_t denotes identity-consistency variables, r_t denotes routing response variables, c_t denotes channel-load variables, and n_t denotes neighbor-interaction variables. This grouping preserves the physical meaning of vehicular communication behavior.

Because different variables have different scales and update frequencies, feature alignment is performed before sequence modeling. Message interval and channel occupancy are continuous variables, while protocol state and identity consistency include categorical states. The aligned feature token is generated through normalization and embedding fusion.

$$z_t = W_x x_t + W_e e_t + b_z \quad \text{Eq.(2)}$$

The vector z_t is the communication behavior token at time t. The term x_t contains normalized numerical variables, and e_t denotes embedded categorical protocol and identity states. In the dataset, each token has 96 dimensions after fusion.

A reliability mask is attached to each token to describe packet loss, delayed reception, and incomplete roadside-unit feedback. This prevents the model from confusing missing evidence with normal communication.

$$m_t = \sigma(W_m q_t + b_m) \quad \text{Eq.(3)}$$

The reliability coefficient m_t is learned from packet delay, missing-field ratio, and channel congestion. During training, windows with $10\%, 20\%$, and 30% packet loss are simulated to improve robustness. Figure 1 illustrates the communication window construction and feature alignment process.

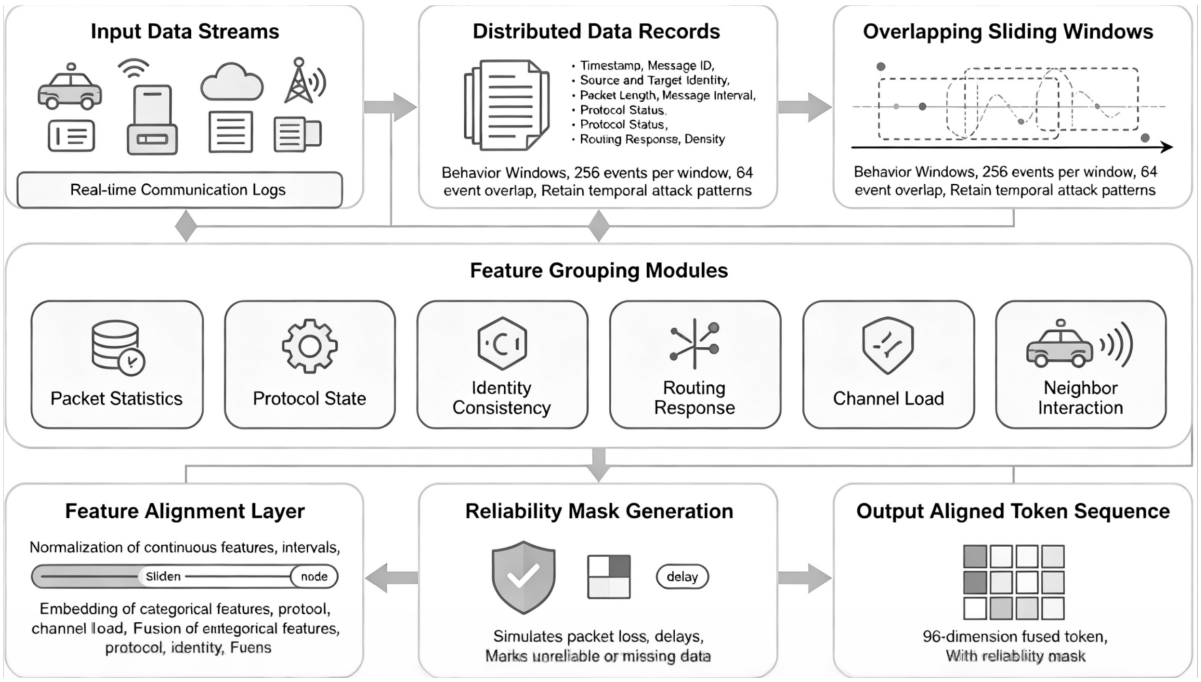

Figure 1. Communication window construction and feature alignment

Selective State Space Anomaly Representation

The core of the proposed framework is a long-context selective state block. Unlike attention mechanisms that compare all token pairs, the selective state block updates a compact state vector according to the current communication token and an input-dependent transition. This makes the model suitable for long vehicular sequences where latency must remain stable.

$$h_t = A_t h_{t-1} + B_t z_t \quad \text{Eq.(4)}$$

The hidden state h_t stores long-context communication evidence. The transition A_t and input projection B_t are not fixed; they are generated from the current token so that abnormal communication states can receive stronger memory updates.

$$A_t = \exp\left(-\text{softplus}\left(W_a z_t\right)\right) \quad \text{Eq.(5)}$$

This transition constrains state decay to a stable range. Normal periodic safety messages are gradually compressed, while unusual identity transitions or routing jumps can be retained longer through smaller decay.

$$B_t = \sigma(W_b z_t) W_v \quad \text{Eq.(6)}$$

The input gate B_t controls how much new evidence enters the state. When message frequency, authentication failure, and routing inconsistency rise together, the gate increases the influence of the current token.

$$y_t = C_t h_t + D z_t \quad \text{Eq.(7)}$$

The output y_t combines long-context state memory and local communication evidence. This design helps separate slow replay behavior from short traffic bursts.

To strengthen abnormal behavior boundaries, an anomaly-sensitive contrast term is added between normal and attack representations. This term increases separation among DoS, spoofing, replay, and routing anomalies.

$$d_{ij} = \frac{\left\| y_i - y_j \right\|_2}{1 + \left| l_i - l_j \right|} \quad \text{Eq.(8)}$$

The denominator uses label distance l_i and l_j so that visually similar attack categories are not forced apart too aggressively when their communication traces overlap. This stabilizes multi-class anomaly learning.

The long-context block uses residual normalization to avoid degradation across stacked layers. In the implementation, four selective state layers are used, and each layer has a hidden size of 128. A dropout rate of 0.15 is applied after residual normalization.

$$g = \frac{\sum_t m_t u_t}{\sum_t m_t + \varepsilon} \quad \text{Eq.(9)}$$

The vector g is the global communication representation. It aggregates both local abnormal spikes and slowly accumulated long-context evidence.

Lightweight Detection Head and Training Strategy

The detection head maps the global representation to attack-category probabilities. The categories include normal communication, DoS, spoofing, replay, routing anomaly, and mixed abnormal traffic. A lightweight two-layer classifier is used because the main temporal modeling burden has already been handled by the selective state block.

$$P(c \mid g) = \mathrm{softmax}\left(W_o GELU\left(W_g g\right)\right) \quad \text{Eq.(10)}$$

The predicted class is the category with maximum posterior probability. The anomaly decision is reported together with confidence so that edge security modules can apply different response levels.

Class imbalance is handled by a calibrated focal objective. Attack samples account for 22.6% of the constructed dataset, and replay samples are less frequent than DoS samples.

$$L_f = -\alpha_c (1 - P_c)^{\gamma} \log(P_c) \quad \text{Eq.(11)}$$

The focusing factor γ is set to 2.0, and minority attack categories are assigned larger α values. This reduces the tendency to classify weak replay traces as normal traffic.

A latency-aware regularization term is used to guide deployment-oriented model selection. It penalizes large hidden states and long inference time while preserving anomaly recall.

$$L = L_f + \lambda_1 \|\Theta\|_2 + \lambda_2 T_{inf} \quad \text{Eq.(12)}$$

The final model has 1.42 million parameters and requires 5.8 milliseconds to run on an edge GPU with a 256-event window. Figure 2 shows the lightweight long-context Mamba anomaly detection framework, which includes behavior token construction, selective state propagation, reliability-aware pooling, and calibration detection.

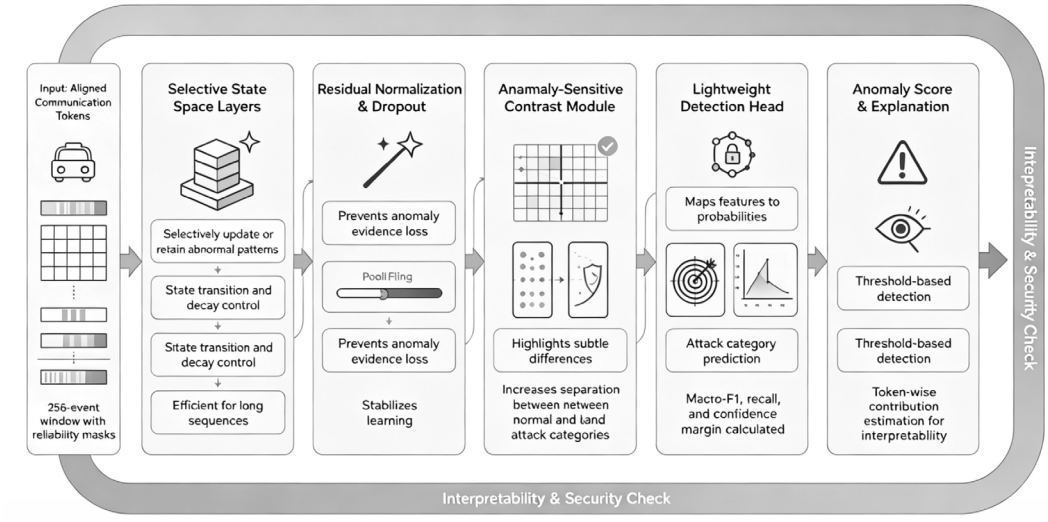

Figure 2. Lightweight long-context Mamba anomaly detection framework

For threshold-based warning, an anomaly score is calculated from the non-normal posterior probability and confidence margin.

$$S_a = 1 - P(\text{ normal } \mid g) + \eta(P_1 - P_2) \quad \text{Eq.(13)}$$

Here, P_1 and P_2 are the largest and second-largest class probabilities. When S_a exceeds 0.62, the system generates an anomaly warning. This threshold gives 95.6% anomaly recall and 4.9% false alarm rate on the validation set.

To support interpretation, the contribution of token t is estimated by masking it and measuring the anomaly-score drop.

$$\phi_t = S_a(X) - S_a(X \setminus z_t) \quad \text{Eq.(14)}$$

High ϕ_t values usually appear near identity changes, abnormal packet bursts, repeated message IDs, or routing-state inconsistency. This provides a practical explanation for security inspection.

Experimental Scheme and Evaluation Protocol

Vehicular Communication Dataset and Attack Labels

The experimental dataset is constructed from simulated and replayed vehicular communication traces containing V2V, V21, and in-vehicle CAN-related message patterns. The dataset contains 1.86 million communication events and 72,640 behavior windows. The normal class accounts for 77.4% of samples, while DoS, spoofing, replay, routing anomaly, and mixed abnormal traffic account for $8.1\%, 4.7\%, 3.6\%, 3.9\%$, and 2.3%, respectively. Each window contains 256 events, and the chronological split ratio is 60:20:20 for training, validation, and testing.

Attack labels are based on communication behavior rather than packet identity. Denial-of-service attacks are characterized by bursts of high-frequency packets and channel occupancy peaks. Spoofing attacks exhibit abnormal neighbor relationships and inconsistent source identities. Replay attacks involve repeating valid messages with a delay. Due to routing anomalies, the response path and the next hop address will change. A hybrid attack is a combination of two or more abnormal behaviors, making it more difficult to classify.

Model Training and Edge Inference Setting

The AdamW optimizer, with an initial learning rate of 0.0008, a batch size of 128, and cosine decay lasting for 80 epochs, will be used for training. If the validation macro F1 does not improve within 8 epochs, early stopping will be executed. The baseline models include Random Forest, XGBoost, CNN, BiLSTM, TCN, Transformer, and Informer. In order to make a fair comparison, all deep baselines use the same train-validation-test splits and the same aligned label inputs.

Edge inference is evaluated on an NVIDIA Jetson-class device and an Intel i7 workstation. The reported latency is averaged over 20,000 windows after warm-up. Memory consumption includes model parameters and intermediate activations. Robustness experiments simulate packet loss from 5% to 30%, communication delay from 20 ms to 120 ms, and vehicle density from 20 to 180 vehicles per square kilometer.

Evaluation Metrics and Ablation Design

Evaluation metrics include accuracy, precision, macro F1 recall, anomaly recall, false positive rate, inference latency, memory consumption, and accuracy-latency trade-off. Macro F1 is used to prevent overestimation of the performance of the majority class. To prevent serious incidents from undetected attacks occurring in a shared driving environment, anomalies must be recalled. Moreover, due to the high false positive rate, people may not trust the safety of these modules.

Through ablation experiments, reliability masks, selective state transitions, anomaly-sensitive contrast items, and delay-aware regularization were all excluded. Add additional tests, including increasing the context length from 64 events to 512 events, and evaluating the scalability of long contexts. The purpose of the above tests is to determine whether the performance improvement is due to the increase in model capacity, better attack representation, or selective memory of long contexts.

https://doi.org/10.64972/jaat.2023v1.303p17e:228-241

Result Analysis and Deployment Discussion

Multi-Attack Detection Performance

Figure 3 shows the results of multiple attack detection. Figure 3(a) compares the accuracy of various baselines, with the proposed model achieving 97.1%, while BiLSTM is at 92.8%, TCN at 94.3%, Transformer at 95.0%, and Informer at 95.5%. Figure 3(b) reports the precision and recall. The proposed model achieved a macro F1 score of 96.3% and an anomaly recall rate of 95.6%, which is a 6.4 percentage point improvement in minority class replay recall compared to the Transformer. Figure 3(c) compares the macro F1 and shows that selective state propagation similar to Mamba improves class balance, not just the accuracy of the normal class [31].

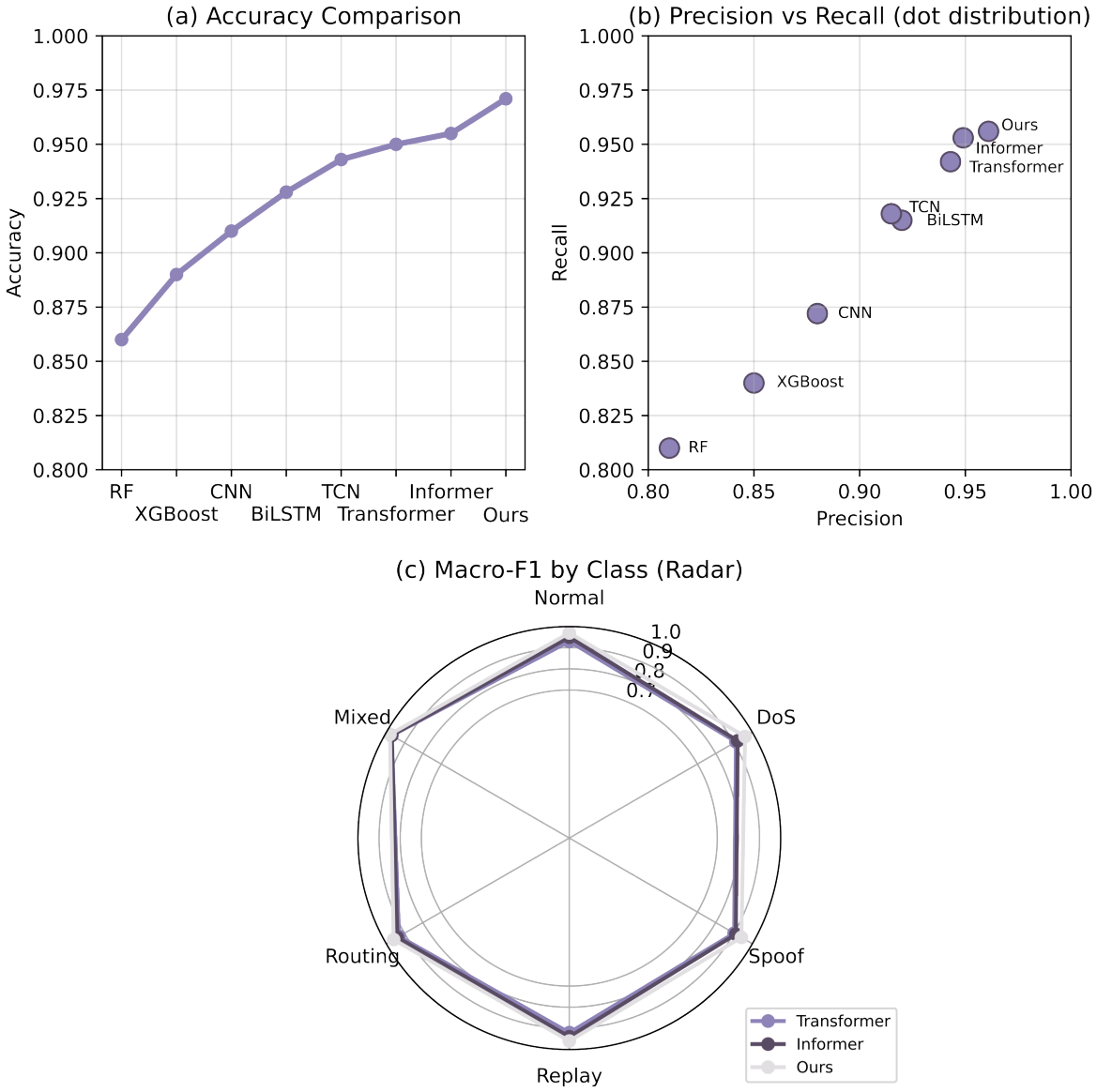

Figure 3. Multi-attack detection performance comparison. (a) Accuracy comparison. (b) Precision and recall comparison. (c) Macro-F1 comparison.

The first two defects are replay and routing errors. Replay traffic usually has a valid message format but lacks extended temporal consistency. The Transformer identified some of this behavior, but its latency increases with the length of the context. BiLSTM can remember sequences, but it loses subtle evidence in longer communication windows. The proposed model has a smaller state and updates this state only when identity consistency, message intervals, and routing responses change simultaneously [32].

https://doi.org/10.64972/jaat.2023v1.303p17e:228-241

Long-Context Modeling Contribution

Figure 4 shows the false positive and false negative rates. As shown in Figure 4(a), there are false positives in the case of normal traffic bursts; the proposed model maintains a false positive rate of 4.9%, while XGBoost and CNN reached 8.2% and 7.6%, respectively. Figure 4(b) shows the missed detections under weak attacks, where low-frequency replay messages are the hardest samples to detect. Figure 4(c) shows threshold sensitivity. When the anomaly threshold changes from 0.55 to 0.70, the anomaly recall rate only decreases by 2.7 percentage points, and the posterior calibration remains stable [33].

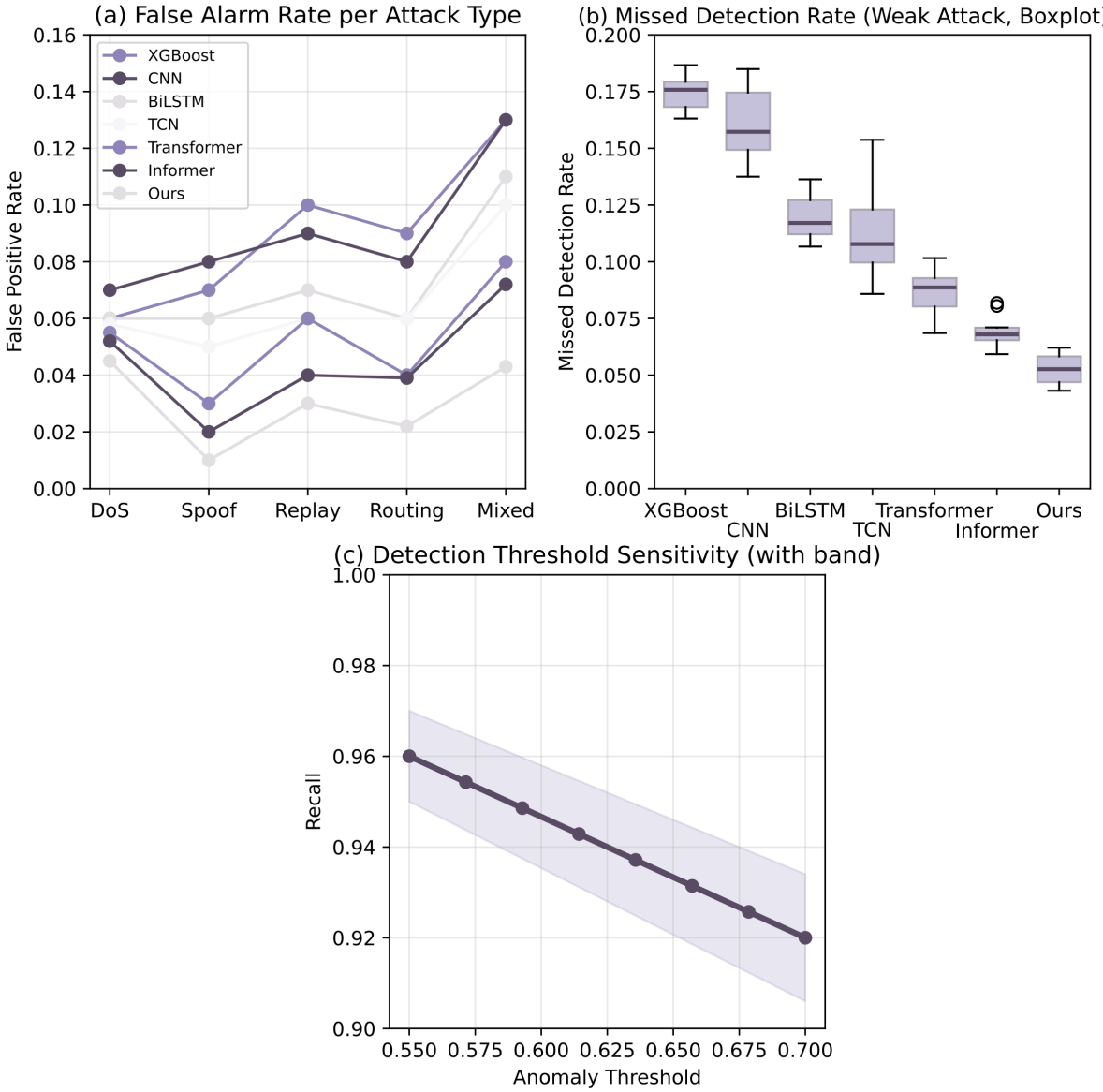

Figure 4. False alarm and missed detection analysis. (a) False alarm under normal traffic. (b) Missed detection under weak attack. (c) Detection threshold sensitivity.

As shown in Figure 5, this is a complete context model. Figure 5(a) shows the event detection results for context lengths of 64, 128, 256, and 512. At 256 events, the model achieved the best macro F1 score, remained stable at 512 events, but the Transformer latency increased. Figure 5(b) shows the state retention capability, which can be used for more than 180 events. Figure 5(c) compares sequence scalability, indicating that selective state propagation offers a better accuracy-cost trade-off than full attention [34].

https://doi.org/10.64972/jaat.2023v1.303p17e:228-241

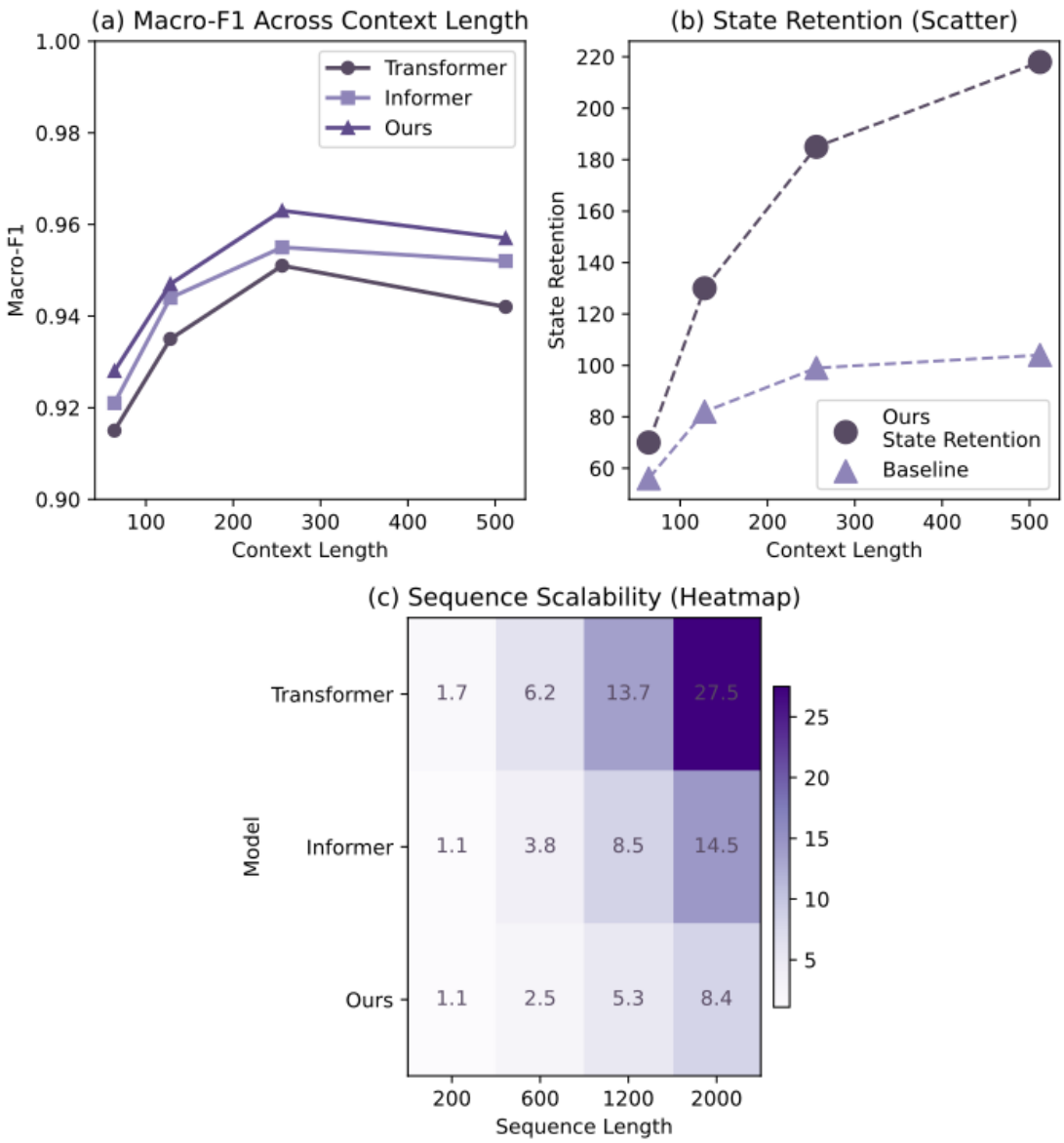

Figure 5. Long-context modeling effect. (a) Performance under different context lengths. (b) State retention capability. (c) Sequence scalability comparison.

The module has been proven to be valuable Through ablation studies. Due to the removal of selective state transitions, the macro F1 dropped from 96.3% to 93.8%. Removing the reliability mask will increase the false positive rate of packet loss by 2.6 percentage points. Removing the anomaly-sensitive contrast will reduce the distinction of replay deception, with the replay recall rate dropping from 93.4% to 89.1%. Therefore, the improved performance of long-context memory and anomaly-oriented representations may stem from a larger number of parameters rather than other factors [35].

Robustness and Edge Efficiency

Under dynamic vehicle communication, the robustness is shown in Figure 6. Figure 6(a) depicts the situation of lost data packets. In the case of 20% packet loss, the proposed model's macro F1 score is 94.5%, while the BiLSTM score is 90.2%. Figure 6(b) shows the communication delay. Due to the reliability mask reducing the impact of the 100-millisecond delay token, the anomaly recall rate remains at 93.8%. Figure 6(c) shows the density of cars. At a density of 180 cars per square kilometer or higher, the false alarm rate of all models increases; however, the proposed method can keep it below 6.1% [36].

https://doi.org/10.64972/jaat.2023v1.303p17e:228-241

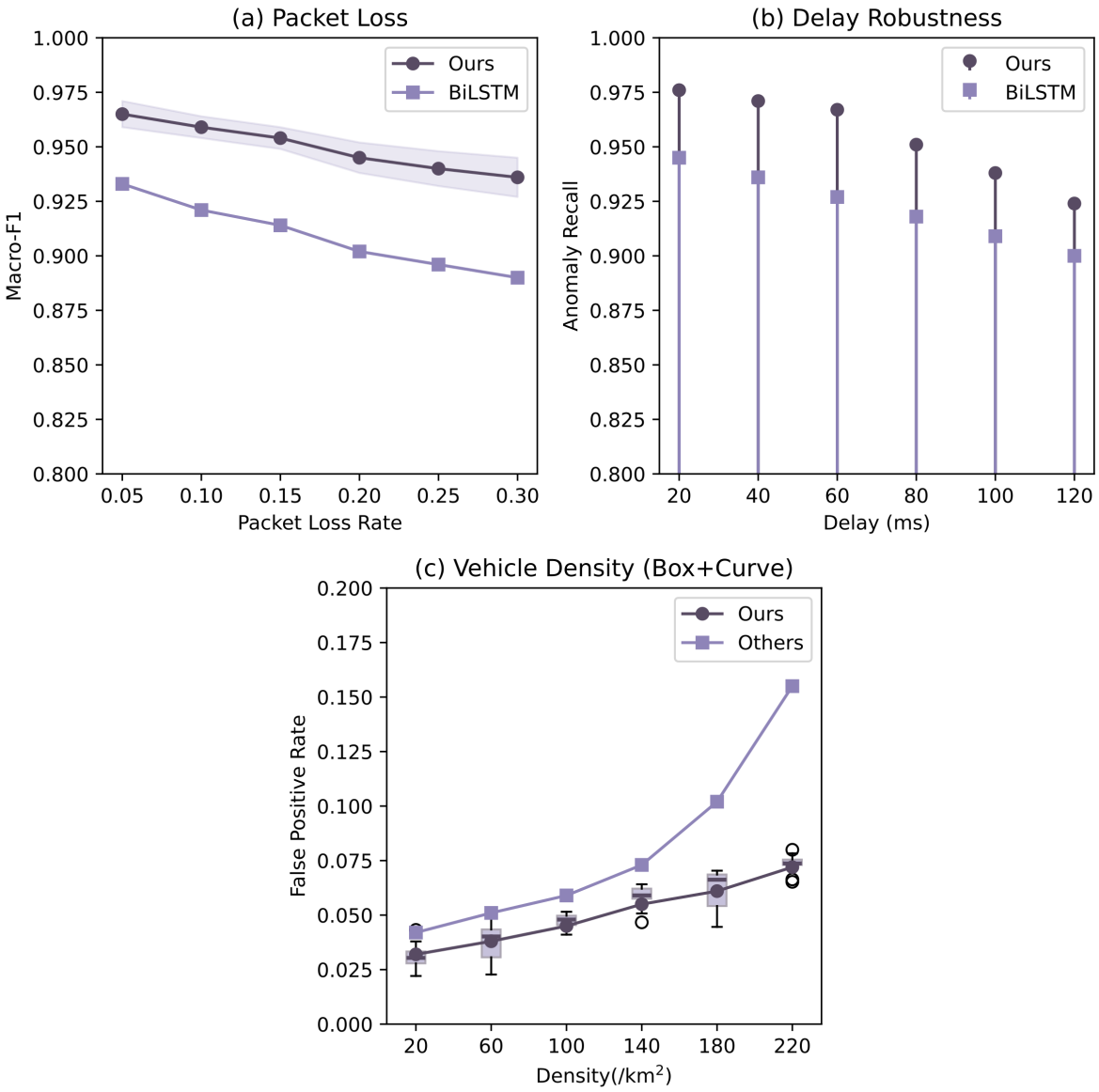

Figure 6. Robustness under dynamic vehicular communication. (a) Packet loss condition. (b) Communication delay condition. (c) Vehicle density condition.

Edge efficiency is shown in Figure 7. Figure 7(a) shows the inference latency. The proposed method has a delay of 5.8 milliseconds per 256-event window, while the delays for Transformer and BiLSTM are 13.7 milliseconds and 10.4 milliseconds, respectively. As shown in Figure 7(b), the proposed model requires 18.6 MB of memory, while the Transformer requires 42.3 MB of memory. Figure 7(c) is the accuracy-latency trade-off curve, representing the most efficient frontier of the model [37].

https://doi.org/10.64972/jaat.2023v1.303p17e:228-241

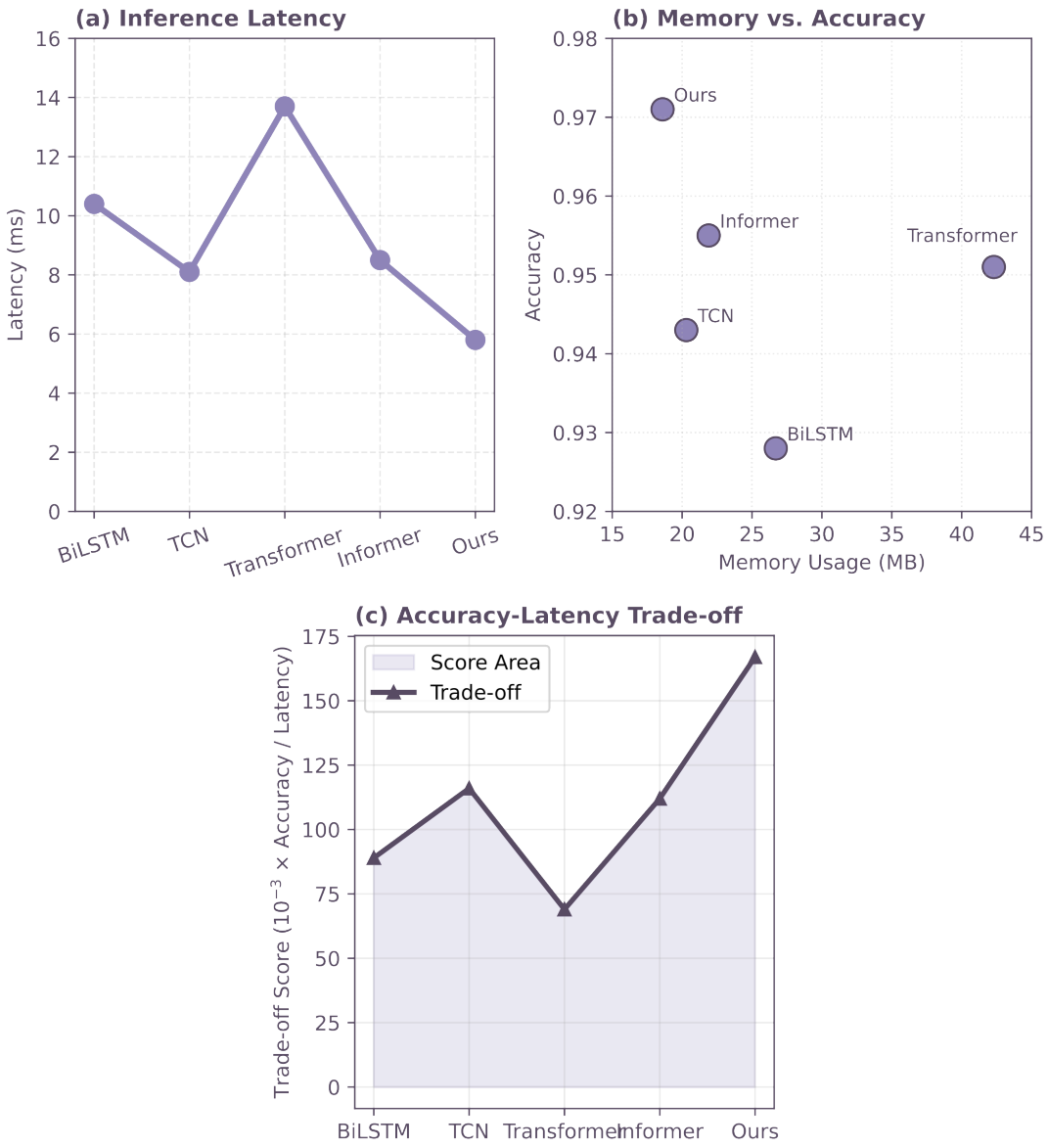

Figure 7. Edge efficiency comparison. (a) Inference latency. (b) Memory usage. (c) Accuracy-latency trade-off.

According to the interpretability analysis, sudden changes in source identity, repeated message IDs, abnormal routing responses, or dense packet bursts are usually associated with high-contribution tokens. This is consistent with research on anomalies in connected vehicles, which requires interpretability of security responses [38]. Token masks are more easily connected with message logs and directly show a reduction in anomaly scores. Furthermore, these findings support the practical value of explainable intrusion detection in vehicular edge systems [39]. During hybrid attacks, the model uses interval bias, identity inconsistency, and routing state memory to make more reliable decisions [40].

Conclusion

This paper proposes a method for identifying abnormal communication behaviors in the Internet of Vehicles based on the extended Mamba. In order to retain long-distance anomaly evidence, heterogeneous vehicle messages are aligned to the communication behavior window and selective state propagation is used. Compared to previous RNN, CNN, and attention-based models, the design in this paper improves the model for capturing replay, spoofing, denial of service, routing anomalies, and hybrid anomaly behaviors in dynamic vehicular communication.

According to the above experiments, the new model improves anomaly recall rate, edge inference efficiency, false positive control, and macro F1 score. A reliability mask uses an anomaly-sensitive contrast mechanism to distinguish visually similar category-based attacks and helps reduce packet loss and communication delays. Since the model provides token-level anomaly score contribution evidence, security checks and operational responses become easier.

Future research will expand this framework by incorporating real roadside unit trajectories, federated learning between vehicle edge nodes, updates to privacy-preserving models, and adaptive thresholds based on different traffic densities. Online incremental training, hardware-aware compression, and quantization can enhance the feasibility of deploying large-scale vehicular communication security systems.

Author Contributions

Leon Stasiak contributes to conceptualization, methodology, software, validation, analysis, investigation, data collection, draft preparation, manuscript editing, visualization, supervision, project administration, and funding acquisition. Urszula Królowa and Irena Patrycja Kotowska contribute to validation and investigation. All authors have read and agreed with the manuscript before its submission and publication.

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

References

[1] Li, X., Hu, Z., Xu, M., Wang, Y., & Ma, J. (2021). Transfer learning-based intrusion detection scheme for Internet of vehicles. Information Sciences, 547, 119-135. https://doi.org/10.1016/j.ins.2020.05.130

[2] Praneeth, V., Kumar, K. R., & Karyemsetty, N. (2021). Security: Intrusion prevention system using deep learning on the Internet of Vehicles. International Journal of Safety and Security Engineering, 11(3), 231-237. https://doi.org/10.18280/ijsse.110303

[3] Yang, L., Moubayed, A., & Shami, A. (2022). MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles. IEEE Internet of Things Journal, 9(1), 616-632. https://doi.org/10.1109/jiot.2021.3084796

[4] Yang, L., & Shami, A. (2022). A transfer learning and optimized CNN based intrusion detection system for Internet of Vehicles. ICC 2022 - IEEE International Conference on Communications, 2774-2779. https://doi.org/10.1109/icc45855.2022.9838780

[5] Yang, L., Moubayed, A., Hamieh, I., & Shami, A. (2019). Tree-based intelligent intrusion detection system in Internet of Vehicles. 2019 IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/globecom38437.2019.9013892

[6] Delwar Hossain, M., Inoue, H., Ochiai, H., Fall, D., & Kadobayashi, Y. (2020). An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/globecom42002.2020.9322395

[7] Alfardus, A., & Rawat, D. B. (2021). Intrusion detection system for CAN bus in-vehicle network based on machine learning algorithms. 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, 944-949. https://doi.org/10.1109/uemcon53757.2021.9666745

[8] Zhang, L., Yan, X., & Ma, D. (2022). A binarized neural network approach to accelerate in-vehicle network intrusion detection. IEEE Access, 10, 123505-123520. https://doi.org/10.1109/access.2022.3208091

[9] Xiao, J., Yang, L., Zhong, F., Chen, H., & Li, X. (2022). Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework. Applied Intelligence, 53(3), 3183-3206. https://doi.org/10.1007/s10489-022-03412-8

[10] Mowla, N. I., Rosell, J., & Vahidi, A. (2022). Dynamic voting based explainable intrusion detection system for in-vehicle network. 2022 24th International Conference on Advanced Communication Technology, 406-411. https://doi.org/10.23919/icact53585.2022.9728968

[11] Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, 169, 102767. https://doi.org/10.1016/j.jnca.2020.102767

[12] Poornima, I. G. A., & Paramasivan, B. (2020). Anomaly detection in wireless sensor network using machine learning algorithm. Computer Communications, 151, 331-337. https://doi.org/10.1016/j.comcom.2020.01.005

[13] Singh, S., & Banerjee, S. (2020). Machine learning mechanisms for network anomaly detection system: A review. 2020 International Conference on Communication and Signal Processing, 976-980. https://doi.org/10.1109/iccsp48568.2020.9182197

[14] Neuschmied, H., Winter, M., Hofer-Schmitz, K., Stojanovic, B., & Kleb, U. (2021). Two stage anomaly detection for network intrusion detection. Proceedings of the 7th International Conference on Information Systems Security and Privacy, 450-457. https://doi.org/10.5220/0010233404500457

[15] Zhang, J., Li, F., & Ye, F. (2020). An ensemble-based network intrusion detection scheme with Bayesian deep learning. ICC 2020 - 2020 IEEE International Conference on Communications, 1-6. https://doi.org/10.1109/icc40277.2020.9149402

[16] Hsu, Y. F., & Matsuoka, M. (2020). A deep reinforcement learning approach for anomaly network intrusion detection system. 2020 IEEE 9th International Conference on Cloud Networking, 1-6. https://doi.org/10.1109/cloudnet51028.2020.9335796

[17] Deore, B., & Bhosale, S. (2022). Hybrid optimization enabled robust CNN-LSTM technique for network intrusion detection. IEEE Access, 10, 65611-65622. https://doi.org/10.1109/access.2022.3183213

[18] Ketepalli, G., & Bulla, P. (2022). Feature extraction using LSTM autoencoder in network intrusion detection system. 2022 7th International Conference on Communication and Electronics Systems, 744-749. https://doi.org/10.1109/icces54183.2022.9835788

[19] Mahmoud, M., Kasem, M., Abdallah, A., & Kang, H. S. (2022). AE-LSTM: Autoencoder with LSTM-based intrusion detection in IoT. 2022 International Telecommunications Conference, 1-6. https://doi.org/10.1109/itc-egypt55520.2022.9855688

[20] Lampe, B., & Meng, W. (2022). IDS for CAN: A practical intrusion detection system for CAN bus security. GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 1782-1787. https://doi.org/10.1109/globecom48099.2022.10001536

[21] Yang, L., Shami, A., Stevens, G., & de Rusett, S. (2022). LCCDE: A decision-based ensemble framework for intrusion detection in the Internet of Vehicles. GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 3545-3550. https://doi.org/10.1109/globecom48099.2022.10001280

[22] Nguyen, D. C., Nguyen, K. D., & Chacko, S. (2022). A real-time explainable anomaly detection system for connected vehicles. Proceedings of the 7th International Conference on Internet of Things, Big Data and Security, 17-25. https://doi.org/10.5220/0010968500003194

[23] Islam, A., Morol, M. K., & Shin, S. Y. (2022). A federated learning-based blockchain-assisted anomaly detection scheme to prevent road accidents in Internet of Vehicles. Proceedings of the 2nd International Conference on Computing Advancements, 516-521. https://doi.org/10.1145/3542954.3543028

[24] Zhou, H., Zhang, S., Peng, J., Zhang, S., Li, J., Xiong, H., et al. (2021). Informer: Beyond efficient Transformer for long sequence time-series forecasting. Proceedings of the AAAI Conference on Artificial Intelligence, 35(12), 11106-11115. https://doi.org/10.1609/aaai.v35i12.17325

[25] Zhuang, Y., Zhang, J., & Tu, M. (2022). Long-range sequence modeling with predictable sparse attention. Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics, 234-243. https://doi.org/10.18653/v1/2022.acl-long.19

[26] Ai, X., & Fang, B. (2022). Leveraging relaxed equilibrium by lazy transition for sequence modeling. Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics, 2904-2924. https://doi.org/10.18653/v1/2022.acl-long.208

[27] Luo, Y., Chen, Z., & Yoshioka, T. (2020). Dual-path RNN: Efficient long sequence modeling for time-domain single-channel speech separation. ICASSP 2020, 46-50. https://doi.org/10.1109/icassp40776.2020.9054266

[28] Barredo Arrieta, A., Diaz-Rodriguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., et al. (2020). Explainable artificial intelligence: Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

[29] Lundberg, S. M., Erion, G., Chen, H., DeGrave, A., Prutkin, J. M., Nair, B., et al. (2020). From local explanations to global understanding with explainable AI for trees. Nature Machine Intelligence, 2(1), 56-67. https://doi.org/10.1038/s42256-019-0138-9

[30] Apley, D. W., & Zhu, J. (2020). Visualizing the effects of predictor variables in black box supervised learning models. Journal of the Royal Statistical Society Series B: Statistical Methodology, 82(4), 1059-1086. https://doi.org/10.1111/rssb.12377

[31] Otoum, Y., Wan, Y., & Nayak, A. (2022). Transfer learning-driven intrusion detection for Internet of Vehicles. 2022 International Wireless Communications and Mobile Computing, 342-347. https://doi.org/10.1109/iwcmc55113.2022.9825115

[32] Luo, A. (2022). Intrusion detection system for Internet of Vehicles based on ensemble learning and CNN. Journal of Physics: Conference Series, 2414(1), 012014. https://doi.org/10.1088/1742-6596/2414/1/012014

[33] Pradhan, M., Mohanty, S., & Seemona, A. O. (2022). Machine learning-based intrusion detection system for the Internet of Vehicles. 2022 5th International Conference on Computational Intelligence and Networks, 1-6. https://doi.org/10.1109/cine56307.2022.10037357

[34] Lihua, L. (2022). Energy-aware intrusion detection model for Internet of Vehicles using machine learning methods. Wireless Communications and Mobile Computing, 2022, 9865549. https://doi.org/10.1155/2022/9865549

[35] Ding, D., Zhu, L., Xie, J., & Lin, J. (2022). In-vehicle network intrusion detection system based on Bi-LSTM. 2022 7th International Conference on Intelligent Computing and Signal Processing, 580-583. https://doi.org/10.1109/icsp54964.2022.9778620

[36] Yang, G., Tang, C., Jiang, Z., & Liu, X. (2022). Towards interpretable and lightweight intrusion detection for in-vehicle network. 2022 4th International Conference on Communications, Information System and Computer Engineering, 179-182. https://doi.org/10.1109/cisce55963.2022.9851006

[37] Mercaldo, F., Casolare, R., Ciaramella, G., Iadarola, G., Martinelli, F., Ranieri, F., et al. (2022). A real-time method for CAN bus intrusion detection by means of supervised machine learning. Proceedings of the 19th International Conference on Security and Cryptography, 534-539. https://doi.org/10.5220/0011267500003283

[38] Jin, S., Chung, J. G., & Xu, Y. (2021). Signature-based intrusion detection system for in-vehicle CAN bus network. 2021 IEEE International Symposium on Circuits and Systems, 1-5. https://doi.org/10.1109/iscas51556.2021.9401087

[39] Matzka, S. (2020). Explainable artificial intelligence for predictive maintenance applications. 2020 Third International Conference on Artificial Intelligence for Industries, 69-74. https://doi.org/10.1109/ai4i49448.2020.00023

[40] Zeng, W., Davoodi, A., & Topaloglu, R. O. (2020). Explainable DRC hotspot prediction with Random Forest and SHAP tree explainer. 2020 Design, Automation & Test in Europe Conference & Exhibition, 1151-1156. https://doi.org/10.23919/date48585.2020.9116488