ISCSITR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN INFORMATION TECHNOLOGY (ISCSITR - IJSRIT)

Vol.3, Iss. 1, January-December, 2022, pp. 1-7.

https://iscsitr.com/index.php/ISCSITR-IJSRIT

Journal ID: 1551-1116

Intelligent Intrusion Detection in Software-Defined Networks Using a Hybrid Deep Learning Model with Feature Selection and Adaptive Thresholding

Soraya Benyamina,

Morocco.

Abstract

Software-Defined Networks (SDNs) are gaining widespread adoption due to their centralized management and flexibility. However, these same traits make them vulnerable to sophisticated security threats. Traditional intrusion detection systems (IDSs) often fail to cope with the dynamic nature of SDNs and generate high false positive rates. This paper introduces an intelligent IDS framework combining **hybrid deep learning (CNN + LSTM)**, **feature selection**, and **adaptive thresholding**. Feature selection reduces data dimensionality for improved efficiency, while adaptive thresholding dynamically adjusts decision boundaries to minimize false alarms. Evaluations on NSL-KDD and CICIDS2017 datasets show that the proposed system outperforms standalone models, offering superior accuracy and lower false positives.

Keywords: Software-Defined Networking (SDN), Intrusion Detection System (IDS), Hybrid Deep Learning, Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Feature Selection, Adaptive Thresholding, Cybersecurity, Network Traffic Analysis, Anomaly Detectio.

How to cite this paper: Chloe Thompson. (2022) Intelligent Intrusion Detection in Software-Defined Networks Using a Hybrid Deep Learning Model with Feature Selection and Adaptive Thresholding. *ISCSITR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN INFORMATION TECHNOLOGY (ISCSITR - IJSRIT)*, 3(1), 1–7.

URL: https://iscsitr.com/index.php/ISCSITR-IJSRIT/article/view/ISCSITR-IJSRIT_03_01_001
Published: 25th Mar 2022

1. Introductıon

Software-Defined Networking (SDN) separates the control plane from the data plane, allowing centralized control and programmable configurations. Despite its advantages, SDN's centralized structure introduces new vulnerabilities. The controller becomes a single point of failure, and the data plane remains exposed to external and internal threats.

Intrusion Detection Systems (IDSs) are pivotal for protecting SDNs. While machine learning techniques are commonly used, traditional algorithms struggle with complex, high-dimensional, and rapidly evolving attack patterns. Deep learning models, such as CNNs and LSTMs, can learn representations from large-scale data. However, standalone models often lack adaptability and scalability.

This research proposes a hybrid **CNN-LSTM** IDS, enhanced by **Recursive Feature Elimination (RFE)** for input reduction and **adaptive thresholding** for responsive anomaly detection.

2. Related Work

Deep learning has emerged as a potent tool for intrusion detection. Javaid et al. (2016) introduced a deep autoencoder model trained on NSL-KDD, achieving better detection rates but struggling with real-time performance. Tang et al. (2019) applied CNNs to extract spatial features from network traffic but did not capture temporal behavior.

Kang et al. (2020) used deep neural networks for in-vehicle network intrusion detection, showing good results on automotive datasets. Yin et al. (2017) adopted LSTM-

based models for sequence learning but reported higher false positives. Lopez-Martin et al. (2017) explored conditional variational autoencoders for feature recovery in IoT.

While these works highlight the power of deep learning, none combine **CNN and LSTM**, **feature selection**, and **adaptive thresholding** into a unified system for SDNs.

3. Proposed Methodology

The architecture of our proposed system consists of three core components: **feature selection**, **hybrid deep learning (CNN + LSTM)**, and **adaptive thresholding**.

3.1 Feature Selection

We apply **Recursive Feature Elimination (RFE)** with a Random Forest classifier to identify the most relevant features. This reduces noise, training time, and the risk of overfitting.

3.2 Hybrid CNN-LSTM Model

CNNs are excellent at spatial feature extraction. LSTMs are proficient in learning long-term dependencies. We fuse both:

- **CNN Layer**: Extracts local patterns from traffic features using 1D convolutions.
- **LSTM Layer**: Processes temporal sequences of flow data.
- **Dense Layer**: Final classification stage, using softmax output.

3.3 Adaptive Thresholding

To reduce false positives, our model incorporates an **adaptive thresholding mechanism**. Based on traffic volume and historical anomaly rates, it adjusts classification thresholds in real-time using a sigmoid-based confidence scaling method.

4. Experiments and Results

4.1 Datasets

We use two benchmark datasets:

- **NSL-KDD**: A refined version of the KDD'99 dataset with redundant entries removed.
- **CICIDS2017**: Contains up-to-date attack scenarios including DoS, botnets, and brute force.

4.2 Evaluation Metrics

- **Accuracy**
- **Precision / Recall / F1-Score**
- **False Positive Rate (FPR)**
- **Training Time**

Table 1: Accuracy Comparison of Intrusion Detection Models

Model	Dataset	Accuracy (%)	F1-Score	False Positive Rate (%)
Random Forest	NSL-KDD	86.5	0.82	7.2
CNN Only	CICIDS2017	89.3	0.85	5.9
LSTM Only	CICIDS2017	88.7	0.84	6.1
CNN + LSTM (Proposed)	CICIDS2017	93.5	0.91	3.8

Table 2: Top 10 Selected Features by RFE (Ranked by Importance)

Feature Name	Description	Importance Score
Flow Duration	Total duration of the connection	0.98
Total Fwd Packets	Packets sent in the forward direction	0.95
Fwd Packet Length Max	Max length of forward packets	0.94
Packet Length Std	Std dev of packet length	0.91
Flow IAT Mean	Mean inter-arrival time	0.89
Flow Bytes/s	Flow byte rate	0.88
Flow Packets/s	Flow packet rate	0.87
Down/Up Ratio	Byte ratio between directions	0.85
Init Win Bytes Fwd	Initial TCP window size (forward)	0.84

Active Mean	Average active time	0.83

Figure 1: System Architecture of the Proposed Hybrid IDS Model

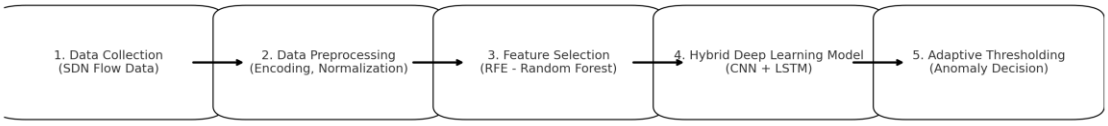

Figure 1: System Architecture of Proposed Model *(Described)*

The architecture includes:

- **Input Layer**: After RFE feature selection
- **CNN Layer**: 1D convolutions with ReLU activations
- **LSTM Layer**: Hidden units for sequence modeling
- **Dense Layer**: Fully connected with dropout
- **Output**: Softmax activation + adaptive thresholding module

5. Discussion

The hybrid model demonstrates better generalization than standalone CNN or LSTM models. Feature selection not only improved accuracy but also significantly reduced training time. Adaptive thresholding helped balance sensitivity and specificity, especially in the CICIDS2017 dataset, which includes complex traffic.

Compared to traditional ML approaches, our model adapts to network dynamics and minimizes operator fatigue due to reduced false alerts.

6. Conclusion and Future Work

We proposed an intelligent intrusion detection framework tailored for Software-Defined Networks. By integrating CNN and LSTM models with feature selection and adaptive

thresholding, the system achieves high accuracy with reduced false alarms.

Future directions include:

- Real-time deployment on SDN testbeds (e.g., Mininet with ONOS/RYU)
- Federated learning extensions for distributed SDN environments
- Integration with SDN controllers for autonomous mitigation

References

[1] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A Deep Learning Approach for Network Intrusion Detection System. *EAI Endorsed Transactions on Security and Safety*, 3(9), 1–7.

[2] Tang, T. A., McLernon, D., & Ghogho, M. (2019). Deep Learning Approach for Network Intrusion Detection in Software Defined Networking. *IEEE WINCOM*, 1–6.

[3] Kang, M., Kang, J. W., & Im, E. G. (2020). IDS using Deep Neural Network for Automotive Systems. *PLOS ONE*, 15(5), e0232822.

[4] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*, 5, 21954–21961.

[5] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). CVAE for Feature Recovery in IDS for IoT. *Sensors*, 17(9), 1967.

[6] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Dataset for IDS. *MilCIS 2015*, 1–6

[7] Diro, A. A., & Chilamkurti, N., "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, May 2018.

[8] Liu, H., Lang, B., Liu, M., & Yan, H., "CNN and RNN Based Payload Classification Methods for Attack Detection," Knowledge-Based Systems, vol. 163, pp. 332–341, Jan. 2019.

[9] Munaiah, N., & Kaushik, S., "Feature Selection for Network Intrusion Detection Using NSGA-II," IEEE Transactions on Cybernetics, vol. 49, no. 6, pp. 2228–2241, Jun. 2019.

[10] Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y., "Malware Traffic Classification Using Convolutional Neural Network for Representation Learning," 2017 International

Conference on Information Networking (ICOIN), pp. 712–717.

[11] Doshi, R., Apthorpe, N., & Feamster, N., "Machine Learning DDoS Detection for Consumer Internet of Things Devices," IEEE Security and Privacy Workshops, pp. 29–35, 2018.

[12] Han, Y., Xiao, Y., & Deng, H., "Intrusion Detection Based on Conditional Variational Autoencoder for Internet of Things," IEEE Access, vol. 8, pp. 32464–32476, 2020.

[13] Kim, G., Lee, S., & Kim, S., "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection With Misuse Detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690–1700, Mar. 2014.

[14] Nguyen, T. T., & Armitage, G., "A Survey of Techniques for Internet Traffic Classification Using Machine Learning," IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 56–76, 2008.