Securing Wireless Sensor Networks Against DoS attacks in Industrial 4.0

Ossama H. Embarak[1], Raed Abu Zitar[2]
[1]Department of Computer Sciences Higher Colleges of Technology, United Arab Emirate
[2]Sorbonne Center of Artificial Intelligence, Sorbonne University-Abu Dhabi, Abu Dhabi, United Arab Emirates
Emails: oembarak@hct.ac.ae ; raed.zitar@sorbonne.ae

Abstract

Wireless Sensor Networks (WSNs) play a vital role in Industrial 4.0 by facilitating significant data collection for monitoring and control purposes. However, their distributed and resource-constrained nature makes WSNs vulnerable to Denial-of-Service (DoS) attacks, which can impede their normal operation and jeopardize their functionality. To address this issue, we propose a new machine learning (ML) approach that enhances the security of WSNs against DoS attacks in Industrial 4.0. Our approach incorporates a spatial learning unit, which captures the positional information in WSN traffic flows, and a temporal learning unit which captures time interdependency features within periods of traffic flows. To evaluate the proposed approach, we tested it on a publicly available dataset. The results demonstrate that it achieves a high detection rate while maintaining a low false alarm rate. Moreover, our Intrusion Detection System (IDS) exhibits good scalability and robustness against various DoS attacks. Our approach provides a reliable and effective solution to secure WSNs in Industrial 4.0 against DoS attacks and can be further developed and tested in various real-world scenarios.

Keywords: Industry 4.0; Wireless Sensor Networks; Intelligent Models; Machine Learning; Security

1. Introduction:

A wireless sensor network (WSN) comprises small, low-cost, and low-power sensors that wirelessly transmit data about their surrounding environment, such as temperature, humidity, light, sound, or motion. WSNs are commonly employed in settings where running wires is impractical or difficult, such as environmental monitoring, industrial control, and home automation, as well as in applications that require collecting large amounts of data from multiple locations, such as agriculture, healthcare, and smart cities. The sensors are linked to a central gateway, which collects and aggregates data from all sensors in the network, enabling analysis and decision-making. WSNs can be configured to operate in diverse environments, from indoor office spaces to outdoor agricultural fields, using various wireless protocols, such as Zigbee, Bluetooth, or Wi-Fi, based on the application's requirements.

Industry 4.0, or the Fourth Industrial Revolution, denotes integrating advanced digital technologies into manufacturing, leading to intelligent, connected systems that use real-time data to make informed decisions. Integrating the Internet of Things (IoT), Big Data, wireless communications, Artificial Intelligence (AI), and Additive Manufacturing characterizes Industry 4.0. WSNs are a crucial component of Industry 4.0 and can gather real-time data from different stages of the manufacturing process, such as equipment status, production rates, and energy consumption, for analysis and optimization of processes. For instance, in a smart factory, WSNs can monitor the condition of machines and equipment, such as temperature, vibration, and humidity, to predict maintenance needs and prevent costly downtime. WSNs can also track the factory's movement of materials and products, providing real-time visibility into the production process. Quality control is another application of WSNs in Industry 4.0, where sensors located throughout the production line collect data to detect defects and inconsistencies in real-time, reducing waste and enabling immediate corrective action.

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

Despite their potentially transformative role in industry 4.0, WSNs face a number of security threats due to the openness of their networks to cyber-attacks. These assaults can take many forms, including but not limited to denial of service, data breaches, and malware infections. A Denial of Service (DoS) attack is a type of cyber attack that aims to disrupt the normal operation of a network or system by overwhelming it with traffic or other malicious activity. In a WSN, a DoS attack can cause the sensors to stop functioning or produce incorrect data, which can have serious consequences in applications such as industrial control, environmental monitoring, or healthcare. Several types of DoS attacks can be carried out in a WSN in industry 4.0, including but not limited to Jamming attacks, Resource depletion attacks, Selective forwarding attacks, and Spoofing attacks. Preventing and mitigating DoS attacks in industrial WSNs can be challenging due to the sensors' limited resources and the network's distributed nature. However, some strategies that can be used include implementing encryption and authentication mechanisms, using redundancy and backup systems, and monitoring the network for suspicious activity. Additionally, designing the network with security in mind from the beginning can help to reduce the risk of attacks.

The utilization of machine learning (ML) techniques in Industry 4.0 shows great potential for the automated detection and mitigation of Denial of Service (DoS) attacks in Wireless Sensor Networks (WSNs). By learning network traffic patterns and characteristics, ML algorithms can identify anomalies or malicious activity that may indicate a DoS attack. Commonly used ML solutions include supervised algorithms that are trained on labeled data consisting of both normal and malicious traffic and unsupervised algorithms that do not require labeled data. Both categories of ML algorithms can detect DoS attacks in real time and initiate mitigation measures, such as blocking the attacker, rerouting traffic, or deploying additional sensors to monitor the network. However, there are challenges in using ML for DoS detection in WSNs due to the sensors' limited resources and the network's distributed nature. Collecting and processing the data required for ML algorithms can be difficult, and regular updates and retraining of the ML algorithms are necessary to adapt to new types of attacks and changes in the network environment.

This study proposes a novel deep-learning solution to address security vulnerabilities in WSNs in industry 4.0 by detecting DoS attacks in traffic flows. The approach combines residual convolutional layers for spatial representational learning and recurrent gated units (GRUs) for temporal representational learning of WSN traffic flows. The two representations are then merged to create a complementary set representation that is used to identify DoS attacks using a feed-forward network (FFN). This solution offers an efficient and effective method for early detection of DoS attacks in WSNs.

The upcoming sections of this work are structured as follows: Section 2 offers a comprehensive review of the latest research in this field, critically evaluating its findings. Section 3 delves into the methodology for implementing the proposed approach for safeguarding industrial WSNs. Section 4 examines and analyzes the conducted experiments, engaging in a discussion and debate about their outcomes. The outcomes and contributions of the research are succinctly outlined in Section 5.

2. Related Work

The adoption of WSN in industry 4.0 applications is gaining popularity recently as it enables instant monitoring, data analytics, and optimization of industrial procedures. In this regard, the literature contains a bunch of studies that investigated the role of WSN in revolutionalizing industry 4.0. For example, the authors of [1] provided a non-deterministic system portable converge cast and assessed it to learn pathway timeframes. This was accomplished by considering characteristics such as network replicas, the scale of WSN, and agility embellishments of network fundamentals. In [2], the authors developed a software-defined network (SDN)-based power-conscious routing procedure to find optimal energy ingesting of WSNs in Industry 4.0. Instead of relying on the conventional shortest-path criterion, the SDN controller was used to calculate the optimal routing path for the WSN based on the energy usage of its most important nodes.

In [3], a group-based industrial WSN (GIWSNs) was proposed to split the wireless sensors into many groups for manifold monitoring responsibilities. Every set of sensors was deployed compactly in a zone of a big plant or manufacture contour and kept connected. They cooperatively contemplated the arrangement and sleep development of sensors according to the concept of symmetries, which eased the computing anxieties from manifold groups to a single group and an extra middle-size group. In [4], the authors reviewed the research literature regarding WSN in industry 4.0 by articulating the main research challenges and highlighting the promising research patterns. Their work seeks to define the role of WSN in industry 4.0, the relation between WSN and IoT in industry 4.0, the categories of

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

WSN attention zones in industry 4, the chief categories of attacks against WSN and their main initiators, and the relevant research gaps. The authors of [5] developed a hybrid system for the provision of the Quality of Service (QoS) in industry 4.0 applications, in which definite negligible data charges and the greatest delay are of extreme standing for regulatory devices and procedures. The authors of [6] proposed a Q-network for trustworthy routing using a subjective policy, that enable the agent to familiarise themself with the effects of a pioneering graph-routing process. In their model, the agent's states were indicated via a collection of scores, and the actions renovate the scores thru the responsibilities of WSNs. These approaches allocated the rewards to the agent when the dormancy of WSN decreases or the expectable network period increases.

For synchronizing nodes in industrial SSN without resorting to timestamps—which was shown to be problematic due to the constrained bandwidth and energy resources of these networks—the authors of [7] presented a clock skew approximation technique in They came up with a two-stage plan, first using a phase-locked loop to estimate the frequency difference between nodes' clocks, and then using that difference in frequency and the time difference between the clocks to calculate the clock skew. In [8], the authors looked into how eavesdropping attacks affect WSNs in industry 4.0, and they came up with a method for detecting them based on a statistical investigation of intercept behavior. To ascertain the presence of an eavesdropping attack, this technique compared the actual number of packets intercepted with the expected number. With the goal of satisfying both the latency constraint and the objective consistency of each application, the authors of [9] proposed a QoS framework for totally arbitrary hybrid wired/wireless SSN. their system features the first serviceability planning proposal for SSNs that can achieve the desired consistency in spite of dynamic intervention.

In [10], the authors developed a protocol layer trust-based intrusion detection system (LB-IDS) for securing WSNs through the detection of cyber-attackers at diverse layers. A sensor node's trustworthiness is determined by adding up the percentage of each layer's trust metric that deviates from the average percentage as it relates to the threats. Physical layer trust, MAC layer trust, and network layer trust are the primary considerations when thinking about security. Key trust metrics from a given layer are used to determine a sensor node's trustworthiness within that layer. At last, the accumulated trust values from each layer are used to approximate the sensor node's overall trustworthiness. In order to determine whether a sensor node can be secured or is malevolent, the trust threshold is used.

The literature on securing wireless sensor networks against DoS attacks in Industrial 4.0 is an important and timely topic in the field of industrial cybersecurity. The authors of this literature recognize the vulnerabilities that wireless sensor networks can be subjected to, especially in the context of Industrial 4.0, where the interconnectivity of devices and systems is crucial for efficient operation. The literature presents different approaches for securing wireless sensor networks against DoS attacks. Some of the methods involve improving the authentication and encryption protocols used to secure the communication between the sensor nodes and the network, while others focus on detecting and mitigating the effects of DoS attacks by deploying intrusion detection and prevention systems.

The authors highlight the importance of securing wireless sensor networks in the context of Industrial 4.0, where cyber-physical systems (CPSs) are becoming increasingly prevalent. The integration of CPSs with wireless sensor networks can bring numerous benefits, including improved efficiency, reduced downtime, and better decision-making processes. However, the authors also recognize that this integration also increases the attack surface, making the networks more vulnerable to cyber-attacks. Overall, the literature on securing wireless sensor networks against DoS attacks in Industrial 4.0 is an important contribution to the field of industrial cybersecurity. The authors provide valuable insights and recommendations for securing wireless sensor networks, which can help organizations protect their critical assets and ensure the safe and efficient operation of their industrial systems.

3. The proposed Wireless Sensors Model for IIoT Applications

In this subsection, we defend the approach taken by the proposed DL system for cyber-attack detection on WSN in industry 4.0. Figure 1 depicts the overall structural layout of the suggested model. The illustrated architecture of the proposed system includes the spatial learning unit, the temporal learning unit, and the classification unit.

Spatial learning with convolution in intrusion detection involves using convolutional neural kernels to learn spatial features from network traffic data. Convolutional kernels are particularly well-suited for this task because they can automatically extract relevant features from raw data, such as network packet headers and payloads. The basic idea behind spatial learning is to use a series of convolutional layers to extract spatial features from the input data. Each convolutional layer consists of a set of learnable filters that scan across the input data, detecting specific patterns and

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

features. These filters are typically small) and are applied with a stride of one, which means they move across the input data one pixel at a time.

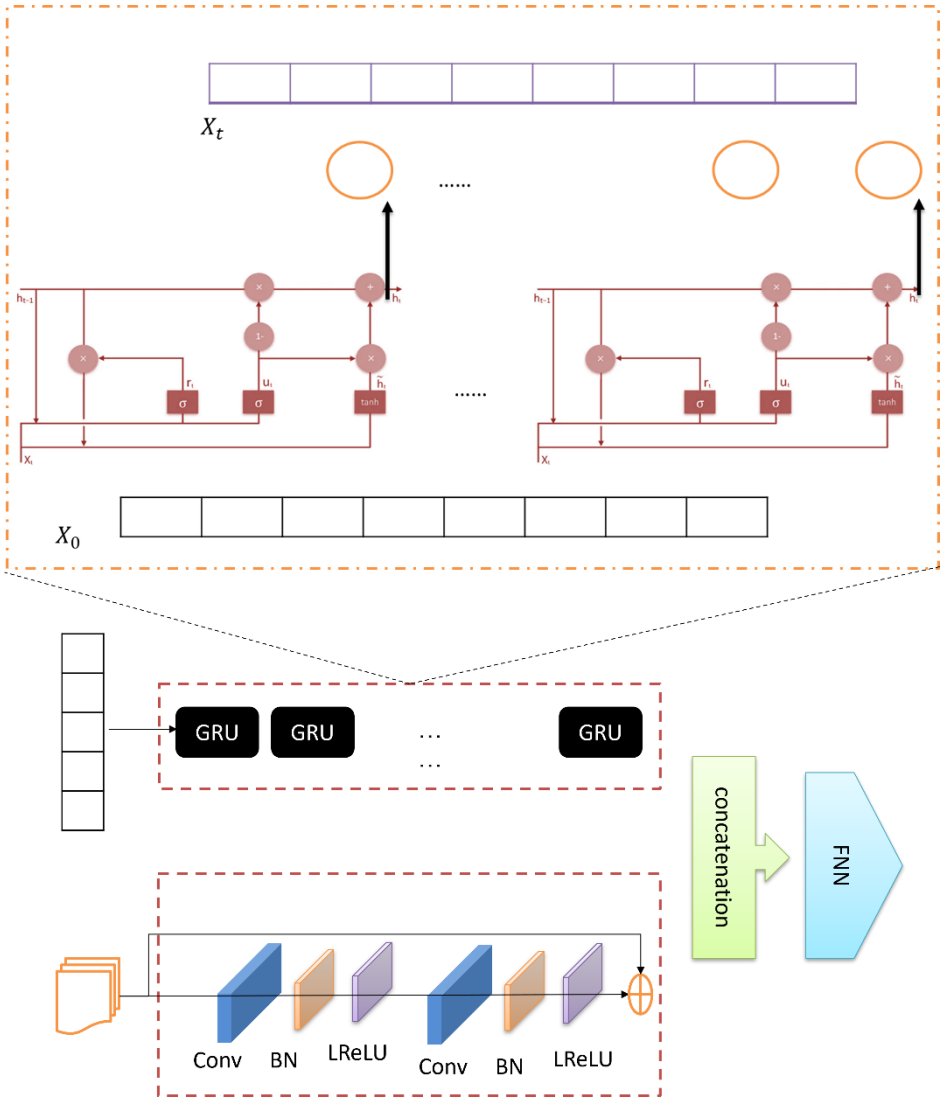

Figure 1: visualization of the architecture of the our model for DoS detection against SN in industry 4.0.

In the context of DoS detection, a convolutional model can be used to identify patterns and anomalies in network traffic data that may indicate the presence of an attack. For example, the kernels may learn to detect patterns in the timing or size of packets, the structure of packet payloads, or the sequence of packets in a session. The implementation of a spatial learning unit uses multiple convolutional layers, followed by batch normalization followed by leakyReLU activation functions. Given the input X_0, the spatial unit can be mathematically expressed as follows:

$$\boldsymbol{X' = LeakyReLU\left(BN\left(Conv1D_3(X_0)\right)\right)} \quad (1)$$

$$\boldsymbol{X'' = LeakyReLU\left(BN\left(Conv1D_3(X')\right)\right)} \quad (2)$$

$$\boldsymbol{X_t = X'' + Conv1D_1(X_0)} \quad (3)$$

Temporal learning is an essential technique for detecting malicious activity in a network by analyzing WSN traffic data. Temporal learning is crucial in DoS detection, as attacks may occur over an extended period of time and may involve complex sequences of events. GRU is a type of recurrent neural network (RNN) that can learn to model temporal dependencies in data. Unlike traditional RNNs, GRUs have gated units that control the flow of information

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

through the model, allowing them to selectively remember or forget past inputs. This makes them well-suited for learning sequences of data with long-term dependencies, such as network traffic data. To effectively integrate the GRU into our system, we feed the WSN traffic data into our model over time, with each input representing a snapshot of the network at a particular moment. The GRU units are then adopted to learn to model the temporal dependencies between these snapshots and detect patterns of behavior that are indicative of malicious activity. The internal calculation of the GRU in our temporal learning units are described as follows.

$$r_t = \sigma\big((w_{xr}x_t + w_{hr}h_{t-1} + b_r)\big) \quad (4)$$

$$u_t = \sigma\big((w_{xu}x_t + w_{ur}h_{t-1} + b_u)\big) \quad (5)$$

$$\tilde{h}_t = tanh(w_{hx}x_t + w_h h(r_t h_{t-1}) + b_u) \quad (6)$$

$$h_t = (1 - u_t)h_{t-1} + u_t\tilde{h}_t \quad (7)$$

The symbol r_t and u_t denote the reset gate and update gate respectively. $\tilde{h}_t$ is the hidden state. The h_t memory state. The output of the GRU model, X_t, is computed as follows:

$$X_t = \sigma(W_t^h \Sigma_{i=1}^{n_h} h_t^i) \quad (8)$$

The temporal representation, X_t, and spatial representation, X_s, form both modules concatenated and finetuned through FFNs composed of three linear layers. This can be defined as follows:

$$Z' = ||(X_t, X_s) \quad (9)$$

$$Z'' = f_a(W' \cdot Z' + b_i') \quad (10)$$

$$Z''' = f_a(W'' \cdot Z'' + b_i'') \quad (11)$$

$$\hat{y}_i = softmax(Z''') \quad (12)$$

The categorical entropy is used as a loss function, and is formulated as follows:

$$J(y, \hat{y}) = \frac{1}{t}\sum_{i}^{t}\sum_{j}^{c} y_{ij} log\,(\hat{y}) \quad (13)$$

4. Results and Discussion

This section provides a detailed analysis of the proposed model for intrusion detection in industrial WSN. The WSN-DS dataset [14] is public security dataset for WSN, which is used in this work for training and evaluation purposes. The number of samples in WSN-DS is 374661, which are unevenly distributed across 5 classes (normal: 340066, Blackhole:14596, Grayhole: 10049, Flooding: 3312, and Scheduling attacks: 6638). Data normalization is performed on the data to lessen the variation between attributes to a particular range, thus decreasing the influence of outliers. In particular, min-max normalization is applied as follows:

$$h_{i,j} = \frac{h_{i,j} - \min(h_{i,j})}{\max(h_{i,j}) - \min(h_{i,j})} \quad (14)$$

As a performance indicator, we choose four classification metrics as our performance indicators, which are mathematically expressed as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (15)$$

$$Precision = \frac{TP}{TP + FP} \quad (16)$$

$$Recall = \frac{TP}{TP + FN} \quad (17)$$

$$F1 - measure = 2 * \frac{Recall \times Precision}{Recall + Precision} \quad (18)$$

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

The above metrics are computed according to a confusion matrix composed of four values: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN), which describe the number of right and improper predictions made by a model for each class**.**

The experimentations of the proposed model involve comparison with the cutting-edge intrusion detection methods, to help understand the competitive advantage of our model. Table 1 shows the numerical results obtained from the proposed model against the competing models. It could be noted that the proposed model can achieve remarkable performance improvements over all the competing methods.

Table 1. comparison of the results of the proposed methods against competing baselines.

MODEL NAME	ACCURACY	PRECISION	RECALL	F1-SCORE	AUC	# PARAMETERS
CNN	98.25	93.47	95.42	94.17	97.62	27,397
LSTM	98.60	94.75	95.16	94.99	97.20	503,141
SIMPLE RNN	98.15	92.17	93.86	92.97	96.12	472,541
GRU	98.32	92.64	92.06	92.15	95.32	493,241
PROPOSED	99.28	95.00	96.00	95.00	98.00	125,341

To further analyze the detection performance for different types of attacks, we display the confusion matrix of the proposed model in Figure 2. Since the dataset suffers from high-class imbalance, we can see high variability in the class precision according to the number of samples per class. However, the general impression of the confusion matrix demonstrates that the proposed model has powerful discriminative capabilities.

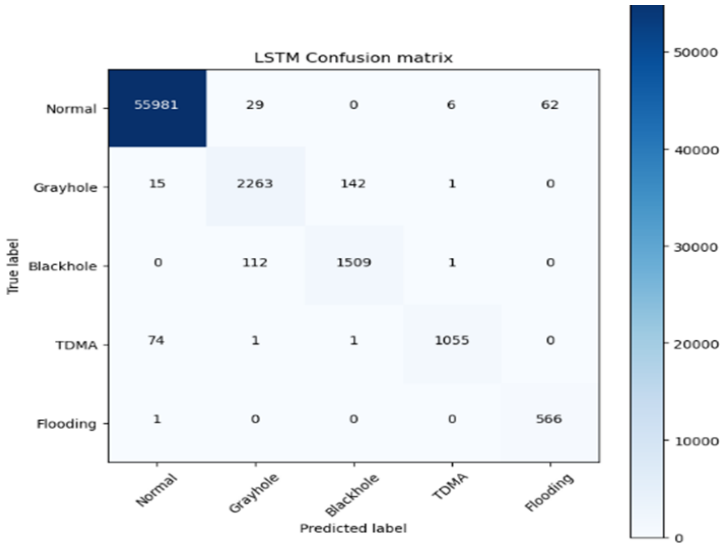

Figure 2: Visualization of the confusion matrix of our model on WSN-DS

Further, the classification capability of our model can also be studied and analyzed by visualizing the receiving operating characteristics (ROC) curves for each class in the test set. This can be achieved by plotting the false positive

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

rate against true positive counterparts. In Figure 3, our model's ROC curves are plotted for each system on different classes, and the corresponding area under the curve is reported. As shown, the detection performance reaches its extreme in case normal and TDMA classes, which obeys the discoveries derived from the confusion matrix.

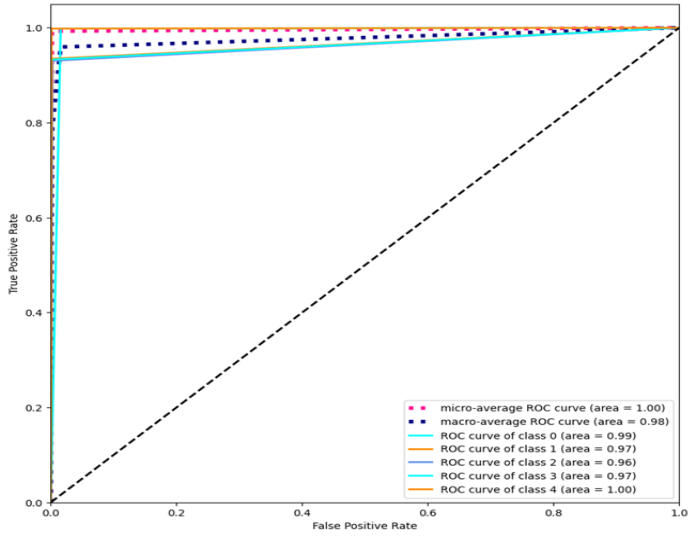

Figure 3: visualization of the ROCAUC curves of the proposed model. Normal=class 0, blackhole=class 1, Grayhole=class 2, Flooding=class 4, Scheduling=class 3.

Furthermore, the diagnosis of training curves is a significant analysis to assure that the deep network consistently learns the patterns of attacks, without falling into randomization problems. In Figure 4, we display the training curves for the proposed model in terms of training accuracy and training loss. The training error measures how well the model fits the training data, while the validation error measures how well the model generalizes to new, unseen data. It could be seen that our model shows some inconsistencies at the first 25 epochs and then the state gets steady after that. This is acceptable as the model weights at the early epochs may not be able to fit the training data well. Another observation is that the proposed model can converge rapidly after 30 epochs, which makes them easy to train in resource-constrained devices dominating the industrial WSN.

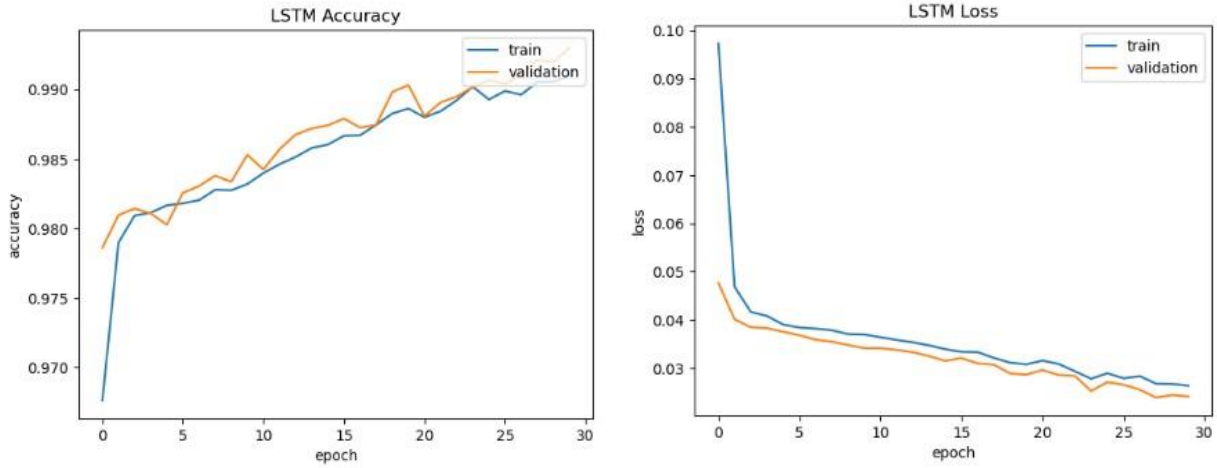

Figure 4: visualization of the training accuracy (left) and training loss curves (right) for the proposed DL system.

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

5. Conclusion

In conclusion, the proposed deep-learning approach provides an effective and efficient solution for protecting SSNs in Industry 4.0 ecosystem settings from cyber-attacks. By leveraging spatial and temporal learning units, the approach can learn complementary representations of DoS attacks without requiring any feature engineering. This structure enables the network to extract spatially relevant features from the input data while preserving the temporal dynamics, leading to precise early detection of DoS attacks. The proof-of-concept simulations performed on the public WSN-DS dataset validate the effectiveness of the proposed approach. The results show that the model achieves a high detection rate while maintaining low false alarm rates, even with limited resources during the training and inferencing stages. Furthermore, the proposed approach exhibits good scalability and robustness against various types of DoS attacks, making it a reliable and practical solution for securing SSNs in Industry 4.0. The research findings suggest that the proposed approach can be further developed and tested in various real-world scenarios to improve the security of SSNs in Industry 4.0 ecosystem settings against cyber-attacks. The successful deployment of this approach could have far-reaching implications for enhancing the security of industrial networks and safeguarding critical infrastructure against cyber threats.

Several future research directions could build upon the existing literature on securing wireless sensor networks against DoS attacks in Industrial 4.0. Some possible future works include:

- Developing new DoS attack detection and mitigation techniques: While the existing literature proposes several approaches for detecting and mitigating DoS attacks, there is still room for developing new and more effective techniques. Future research could explore the use of machine learning and artificial intelligence techniques for detecting and mitigating DoS attacks in wireless sensor networks.

- Investigating the impact of DoS attacks on different types of wireless sensor networks: The existing literature mainly focuses on securing wireless sensor networks in the context of Industrial 4.0. However, different types of wireless sensor networks may have different characteristics and vulnerabilities that could impact their susceptibility to DoS attacks. Future research could investigate the impact of DoS attacks on different types of wireless sensor networks, such as healthcare or environmental monitoring networks.

- Examining the economic and social impacts of DoS attacks: DoS attacks can have significant economic and social impacts, especially in critical infrastructure sectors. Future research could explore the economic and social impacts of DoS attacks on wireless sensor networks in Industrial 4.0 and identify strategies to mitigate these impacts.

- Integrating blockchain technology for securing wireless sensor networks: Blockchain technology has emerged as a promising solution for securing IoT networks. Future research could investigate the potential of integrating blockchain technology for securing wireless sensor networks against DoS attacks.

References

[1]. Z. Qin, D. Wu, Z. Xiao, B. Fu, and Z. Qin, "Modeling and Analysis of Data Aggregation From Convergecast in Mobile Sensor Networks for Industrial IoT," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4457-4467, Oct. 2018, doi: 10.1109/TII.2018.2846687.
[2]. Almuntasheri, S., & Alenazi, M. J. (2022). Software-Defined Network-Based Energy-Aware Routing Method for Wireless Sensor Networks in Industry 4.0. Applied Sciences, 12(19), 10073.
[3]. Lin, C. C., Deng, D. J., Chen, Z. Y., & Chen, K. C. (2016). Key design of driving industry 4.0: Joint energy-efficient deployment and scheduling in group-based industrial wireless sensor networks. *IEEE Communications Magazine*, *54*(10), 46-52.
[4]. Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6), 2087.
[5]. De Beelde, B., Plets, D., & Joseph, W. (2021). Wireless Sensor Networks for Enabling Smart Production Lines in Industry 4.0. Applied Sciences, 11(23), 11248.

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023

[6]. G. Künzel, L. S. Indrusiak and C. E. Pereira, "Latency and Lifetime Enhancements in Industrial Wireless Sensor Networks: A Q-Learning Approach for Graph Routing," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5617-5625, Aug. 2020, doi: 10.1109/TII.2019.2941771.
[7]. H. Wang, F. Yu, M. Li and Y. Zhong, "Clock Skew Estimation for Timestamp-Free Synchronization in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 90-99, Jan. 2021, doi: 10.1109/TII.2020.2975289.
[8]. Y. Zou and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780-787, April 2016, doi: 10.1109/TII.2015.2399691.
[9]. S. Zoppi, A. Van Bemten, H. M. Gürsu, M. Vilgelm, J. Guck and W. Kellerer, "Achieving Hybrid Wired/Wireless Industrial Networks With WDetServ: Reliability-Based Scheduling for Delay Guarantees," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2307-2319, May 2018, doi: 10.1109/TII.2018.2803122.
[10]. Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. International Journal of Communication Systems, 33(4), e4234.
[11]. H. Wang, L. Shao, M. Li, B. Wang and P. Wang, "Estimation of Clock Skew for Time Synchronization Based on Two-Way Message Exchange Mechanism in Industrial Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4755-4765, Nov. 2018, doi: 10.1109/TII.2018.2799595.
[12]. T. M. Chiwewe, C. F. Mbuya and G. P. Hancke, "Using Cognitive Radio for Interference-Resistant Industrial Wireless Sensor Networks: An Overview," in *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1466-1481, Dec. 2015, doi: 10.1109/TII.2015.2491267.
[13]. M. Magno, D. Boyle, D. Brunelli, E. Popovici and L. Benini, "Ensuring Survivability of Resource-Intensive Sensor Networks Through Ultra-Low Power Overlays," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 946-956, May 2014, doi: 10.1109/TII.2013.2295198.
[14]. Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*, 2858-2873.
[15]. Elsayed abou Elwafa, S. A., Aboul Fotouh Saleh, S., Mohamed Abd El-razk, E. E., & Elatawy, S. M. (2022). Securing Management Information Systems Using Blockchain Technology. International Journal of Artificial Intelligence and Education Technology, 1(2), 22-35. https://doi.org/10.54216/IJAIET.010202
[16]. Zaher, M., & El-Khameesy ElGhitany, N. (2021). Blockchain Communication Platform Selection in IoT Healthcare Industry using MARCOS. International Journal of Wireless and Ad Hoc Communication, 2(1), 49-57. https://doi.org/10.54216/IJWAC.020104
[17]. Fattah, S., Gani, A., Ahmedy, I., Idris, M. Y. I., & Targio Hashem, I. A. (2020). A survey on underwater wireless sensor networks: requirements, taxonomy, recent advances, and open research challenges. *Sensors*, *20*(18), 5393.
[18]. Ma, K., Li, Z., Liu, P., Yang, J., Geng, Y., Yang, B., & Guan, X. (2021). Reliability-constrained throughput optimization of industrial wireless sensor networks with energy harvesting relay. *IEEE Internet of Things Journal*, *8*(17), 13343-13354.
[19]. A. Sariga, & J. Uthayakumar. (2020). Type 2 Fuzzy Logic based Unequal Clustering algorithm for multi-hop wireless sensor networks. International Journal of Wireless and Ad Hoc Communication, 1(1), 33-46.
[20]. Almomani, I., Al-Kasasbeh, B. and Al-Akhras, M., 2016. WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. *Journal of Sensors*, *2016*.

DOI: https://doi.org/10.54216/JISIoT.080106
Received: May 12, 2022 Accepted: January 17, 2023