Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station

Manoj Basnet
Department of Electrical and Computer Engineering
University of Memphis
Memphis, TN, USA
mbasnet1@memphis.edu

Dr. Mohd. Hasan Ali
Department of Electrical and Computer Engineering
University of Memphis
Memphis, TN, USA
mhali@memphis.edu

Abstract— **The integration of the open communication layer to the physical layer of the power grids facilitates bidirectional communication, automation, remote control, distributed, and embedded intelligence, and smart resource management, in the grids. However, cybersecurity threats are inherent with the open communication layer, which can violate the confidentiality, integrity, and availability (CIA) of the grid resources. The soaring usage and popularity of electric vehicles (EVs) demand the robust deployment of trustworthy electric vehicle charging station (EVCS). We propose the novel deep learning-based intrusion detection systems (IDS) to detect the denial of service (DoS) attacks in the EVCS. The deep neural network (DNN) and long-short term memory (LSTM) algorithms are implemented (in python 3.7.8) to detect and classify DoS attacks in the EVCS. Results show that both the DNN and LSTM based IDS achieved more than 99% detection accuracy. On top, the LSTM method is superior to the DNN method in terms of accuracy, precision, recall, and measure.**

Keywords— cybersecurity, deep learning, DoS, electric vehicle charging station (EVCS), intrusion detection system (IDS), smart grid

I. Introduction

Electric vehicle charging station (EVCS) consists of three essential components, namely sensing, communication and networking, and the computational components [1]. The sensing components deal with the array of wired/wireless sensors to assess the health and safety check of the various electrical components in the EVCS. Communication and networking components interact with the local grid, supervisory control, and data acquisition (SCADA) system, internal sensors, and electric vehicles (EVs) through the internet to ensure energy efficiency and availability. Enabling wireless technology might be Wi-Fi, cellular, Bluetooth, and so on. The computational components help to perform logical, arithmetic as well as control functions. An EV owner has to schedule the charging through an app or internet so that the maximum number of EVs could be integrated into the grids [2]. An EVCS might ask for authentication before charging so that the personal and financial information has to be shared through some media such as radio frequency identification (RFID), Bluetooth, near field communication (NFC). These wireless communications pose extreme vulnerabilities in EVCS.

There are several motivations behind the cyberattack in EVCS, ranging from prank, electricity theft, identity theft, to severe advanced persistent threats (APT) such as ransomware and malware where EVCS might work as an entry point [3]. The denial of service (DoS) attack has been one of the most widely seen attacks. The DoS attack causes congestion in the network with fake requests so that all the network components are busy with processing the fake requests and unable to respond to the genuine requests [4]. Therefore, DoS attacks have to be taken carefully; otherwise, it is costly in terms of the availability of the resources.

Timely detection of the attacks and its most accurate classification helps the EVCS operator to take the appropriate prevention strategy against the attacks, which is known as intrusion detection system (IDS). Host-based (HIDS), network-based (NIDS), and hybrid IDS are mostly used IDS and classified accordingly in terms of their implementation location. Three basic intrusion detection techniques have been widely deployed in state-of-the-art applications, namely: Signature-based detection (SD), Anomaly-based detection (AD), and Stateful protocol analysis (SPA) [5]. SD-based IDS has to know the fingerprint (pattern) of the attacks beforehand to match the pattern of incoming attack to the stored fingerprint. Therefore, they cannot learn a new kind of attacks. Also, the system admin has to update the fingerprint of the new attacks manually. AD-based IDS detects the anomaly by analyzing whether the incoming attack deviates from the network behavior or not. The mostly used IDS is AD- NIDS, which includes all the machine learning-based IDS.

Despite the capability to learn and detect new network attacks, it suffers from a high false alarm rate (FAR) and goes offline to rebuild the network behavior as it discovers the new attack type. Stateful protocol analysis (SPA), a.k.a. specification-based detection, on the other hand, extracts and crafts the correct behaviors of critical objects as security specifications, and compares them against the actual behavior of the network [6]. The difference in SPA and AD is that the former compares the specification against standard security protocols, while the latter compares the behavior against the observed network behavior. SPA is resource consuming since it has to trace and examine the protocol states. Moreover, it fails to inspect benign protocols behaviors and might not be compatible with the dedicated operating system (OS) and applications.

As far as author's knowledge, very limited works have been done in EVCS cybersecurity [1] [7] [8] , and not enough modelling and strategies have been proposed to deal with the cyberattacks. In other words, there is a technical gap in the cybersecurity studies for the EVCS.

Based on the above background, we propose the novel deep learning-based IDS to deal with the DoS attacks in the EVCS. The proposed methods implement two mostly successful deep learning algorithms, namely: the deep neural network (DNN) and long short term memory (LSTM) for the binary (DoS attack or not attack (benign)) and multiclass (four different classes of DoS attacks as well as benign class) classification of the DoS attacks in the CICIDS 2018 [9] dataset for EVCS scenario. The proposed DNN- based and

978-1-7281-6611-7/20/$31.00 ©2020 IEEE

LSTM-based IDS in the EVCS network have proved to be at least 99% accurate for detecting the DoS attacks with better performance metrics, latter being the more efficient in terms of precision, recall and F1-score.

II. Cybersecurity Issues in EVCS

EVCS has to communicate with the incoming EVs for scheduling, charging EVs for authentication and authorization, and grids for efficiently utilizing the available energy through wired/wireless media. Therefore, EVCS is always vulnerable to cyber-attacks. Moreover, the future charging station has to handle the bidirectional flow of energy from EVCS to EV and vice-versa [8], which in turn enforce the energy prodigy to design the complex and secure cyber-physical infrastructure of EVCS. There might be various instances that the attackers can attack the wireless link between vehicle to EVCS, vehicle to grid (V2G), or vehicle to vehicle (V2V), which is illustrated in Fig. 1. [7].

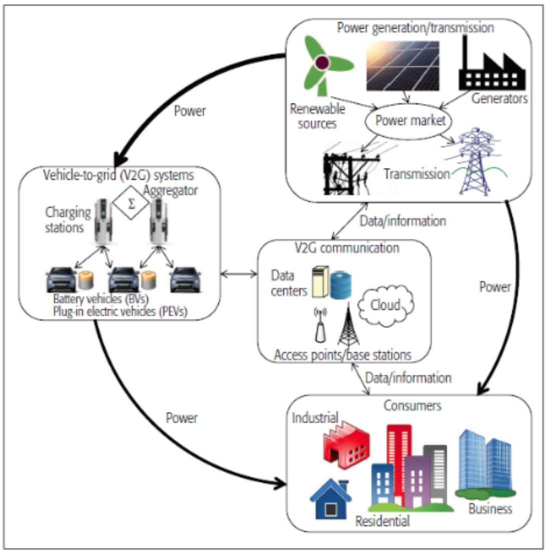

Fig. 1. EVCS Architecture [3]

An intruder can impersonate the credentials of other legitimate users or advertise itself as a legitimate node to broadcast the myriads of requests to the EVCS server. The intruder could exploit any of the weak communication link aforementioned to initiate the DoS attacks in EVCS.

III. Attack Modeling in EVCS

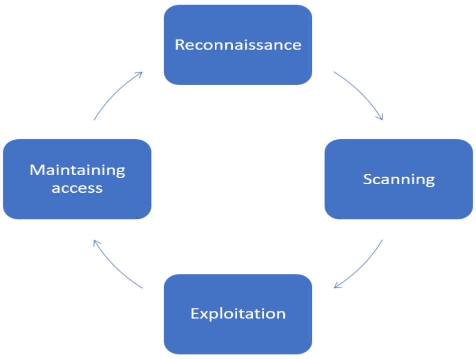

Fig. 2. Attacking cycle of the hacker to take over the system.

As shown in Fig. 2, All the hackers (ethical hackers, black hat hackers, and brown hat hackers) follow the same sequence of events, namely: reconnaissance, scanning, exploitation, and maintaining access to break into the system, whether it is an EVCS or an IT system [10]-[11]. In the reconnaissance phase, hackers either use social engineering (SE) or traffic analysis tools to collect information about the target. In SE, hacker generally wins the trust of the legitimate user to get confidential credentials such as passwords, pins to log into the system by using communication and persuasive skills. In contrast, traffic analysis listens to the network devices to analyze the devices connected to the network [10]. The scanning phase identifies the system vulnerabilities by scanning the IP address, open ports and services running on each open port [10], [12]. In the exploitation phase, hacker attempts to exploit the EVCS component vulnerabilities to get control over it. Various kinds of attacks can be launched in this phase, such as a jamming attack, DoS attack, replay attack, man in the middle attack, malware attacks, ransomware attacks. The mostly launched DoS attacks are SYN attacks, buffer overflow, teardrop attack, puppet, smurf, time delay, time synchronization attacks [10], [13]–[15]. In the last step, hackers launch various attacks such as viruses, trojan horses, and backdoor (mainly) to get permanent access to the EVCS system. Backdoor attacks can cause severe damage as it facilitates multiple attacks to the EVCS server because of its undetectable and stealthy installation on the target server to get back easily and quickly [16].

The DoS attacks are capable of shutting down the entire EVCS infrastructure-- making it unavailable to the customers --which lead to the severe economic and reputation loss as well as sheer customer dissatisfaction. The severity becomes even critical, while multiple instances of DoS attacks are launched on the same EVCS server, which is called distributed DoS (DDoS) attack. Because tracing the origin of the DDoS attack is very hard since it can be launched from various means [17]. For example. by leveraging a legitimate third party server as a part of reflection/amplification attack, or by direct flood attacks from a single device, or by a botnet of multiple devices with spoofed IP of a legitimate user

That is why timely detection of the attack vectors and the identification of digital fingerprints of the DoS/DDoS attack is crucial to defend against them. In our work, we have the following assumptions: hackers exploited the EVCS server to launch the DoS attacks. The attack has changed the attributes of network packets. Also, we have access to network packets before, throughout, and after the attack. The attributes of these data are carefully extracted for further use in deep learning. We assume that CICIDS 2018 DoS data set is an ideal candidate because it incorporates the modern-day DoS attack. Finally, we apply deep learning algorithms to the dataset.

IV. Proposed IDS Methodology

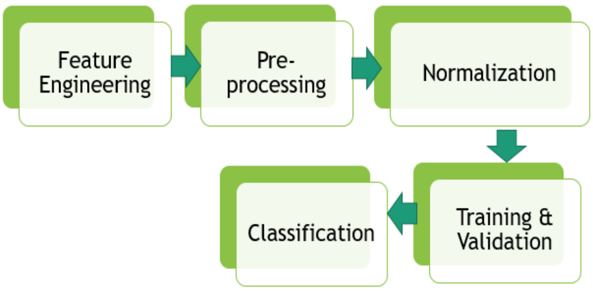

Fig. 3. Steps involved in the Deep learning approach.

Each supervised deep learning algorithm has to go through some necessary steps, as shown in Fig. 3. Training all the features might not be viable due to the limitation of the computation and storage resources. Therefore, choosing the best features for training would save time and computational complexity, which is called feature engineering. The principal component analysis (PCA), filter-based approaches such as information gain (IG) filters, auto-encoder- decoder are implemented in state-of-the-art [18], [19]. Most of the time, the feature sets might have categorical data, integers, floats, therefore, converting them into uniform format is what pre-processing and normalization generally does. Min-max scaling and one hot encoding have been implemented in the algorithm. Both DNN and LSTM algorithm uses 50% of data for training, 20% of data for validation (to check the performance of the model on unknown data) and the remaining 30% for testing purpose. The data in training, validation, and classification are mutually exclusive.

The main goals of our algorithms are first to classify whether the incoming vector is an attack or a benign (Normal) data vector and second to classify the incoming data vector into different attack classes (4 DoS attack classes and one benign class). The former is best known as binary classification, and the latter is termed as multi-class classification. Furthermore, the third is to present a comparative analysis of applied algorithms.

A. Data set

The mostly used datasets available online are KDDCUP 99 [20], NSL KDD [21], UNSW-NB15 [22], Kyoto [23], WSN-DS [24], CICIDS 2017 [25], CICIDS 2018. The CICIDS 2018 DoS attack dataset is used for this research since it includes the recent DoS attacks. Table I. represents the numbers of datasets belonging to different DoS attack classes.

TABLE I. DATASETS OVERVIEW

Benign and Attack data	Numbers
Benign	1426795
DoS attacks-GoldenEye	41508
DoS attacks-Slowloris	10990
DoS attacks SlowHTTPTest	139890
DoS attacks-Hulk	461912

B. Deep Neural Network (DNN)

A three-layered DNN with two hidden layers, each layer with 64 hidden neurons for the binary classification and 128 hidden units for multi-class classification, is implemented for IDS development in EVCS. Apart from that, the hidden layer uses the ReLu function since it has better convergence property and prevents the problem of the sigmoid function, which tends to produce vanishing and exploding gradients. The defacto standard for the optimizer, Adam, is implemented to the DNN [26]. The only difference between the architecture of binary vs. multi-class DNN is the number of units in the hidden layer, output layer, and the corresponding activation function and loss function. The default activation function in the output layer and the loss: are softmax and categorical cross-entropy respectively for multi-class classification; are sigmoid and binary cross-entropy respectively for binary classification. The proposed model implements the L1-L2 regularizers. These Regularizers apply penalties on layer parameters or layer activity during optimization. These penalties are incorporated in the loss function that the network optimizes [27].

C. Long Short term Memory (LSTM)

LSTM is the variant of the recurrent neural network (RNN) developed to eliminate the vanishing gradient problem of RNN and is significantly more complex than traditional neural units. LTSM Cell Architecture: Each cell has four sets of weights which feed into it (instead of one), Output squashing can take any activation function we want though. It learns 1. What/when to let something in, 2. When to forget, 3. What/when to let something out. Most of the architecture is similar to that of DNN shown [28] except the cell structure. A 76, 16, 16, 16, 1 architecture is used for binary classification while 76, 32, 32, 32, 5 architecture is used for the multiclass classification with neuron dropout of 10 % between each hidden layers. The architecture mentioned above is read as # of input units=76, # of LSTM cells in first hidden layer= 32, # of LSTM cells in second hidden layer= 32, # of LSTM cell in third hidden layer= 3, and # of output units=5. More simply, first and last layers being the input and output layers with corresponding nodes, while the middle layers represent the hidden layers with corresponding nodes.

V. RESULTS AND DISCUSSION

In this work, all the simulations and codings are created in Python 3.7.4 in the Jupyter lab (version 1.1.4) under the free and open-source Anaconda distribution. Intel® Core™ i5-3470 @ 3.20 GHz processor with 8.00 GB RAM and 64 -bit Windows 10 OS is used in the experiment.

A. Plot Based Responses

Fig. 4 represents the variance captured by the singular values. Each singular value represents a prominent feature. The most prominent feature ranges from the left to right. At least four features could represent 93.57% of the variance. The more the variance captured, the more will be the significant features. As shown in Fig.5., The PCA plot of the features in 2D showed that any linear classifier function could not classify the given datasets, so deep neural network with the hidden layers is the ultimate solution to classify the data.

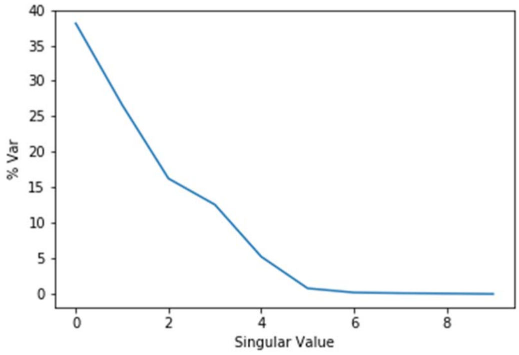

Fig. 4. Variance captured by singular values.

Accuracy: it estimates the correctly classified data out of all datasets. The higher the accuracy, the better the ML model. ($Accuracy \in= [0,1]$)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

As shown in Figs. 6-9, the 99% accuracy has been achieved within less than 10 epochs for the LSTM while it took 30 epochs and 70 epochs, respectively, for binary and multiclass classification using DNN. It means LSTM is superior in terms of speed and accuracy as compared to DNN. Also, training and validation are smoother for LSTM as opposed to DNN.

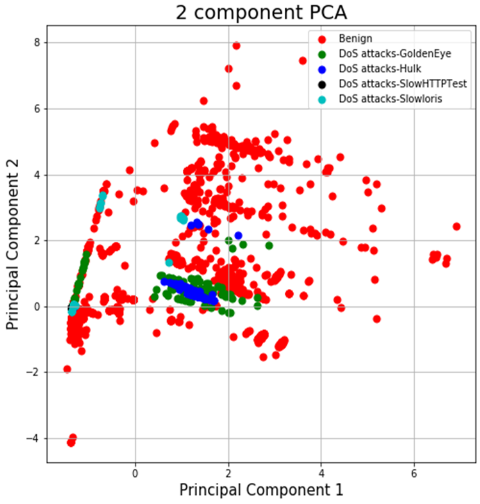

Fig. 5. Two-component PCA plot.

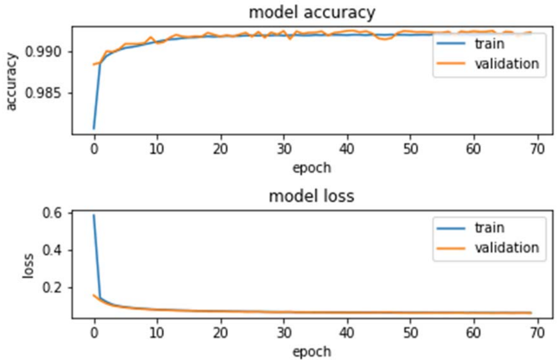

Fig. 6. Model accuracy vs. model loss for the binary classification using DNN.

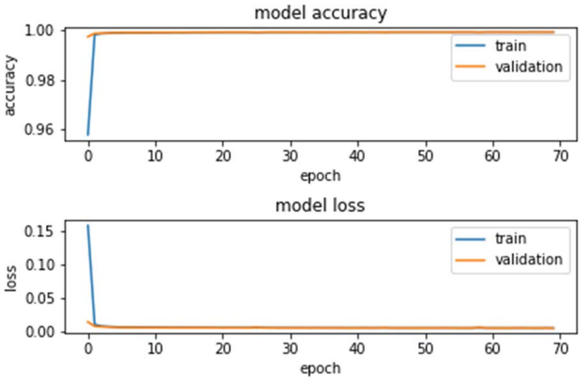

Fig. 7. Model accuracy vs. model loss for the binary classification using LSTM.

Fig. 10 gives the comparative training and testing accuracy for the binary classification of the data (whether the data is normal (benign) or the attack) using the DNN and LSTM-based IDS. As compared to DNN, The training and testing accuracy for the LSTM-based IDS are found to be superior by 0.76 and 0.67, respectively. Similarly, as illustrated in Fig. 11, the training and testing accuracy for the multiclass classification using LSTM are found to be superior by 0.63 and 0.62 respectively.

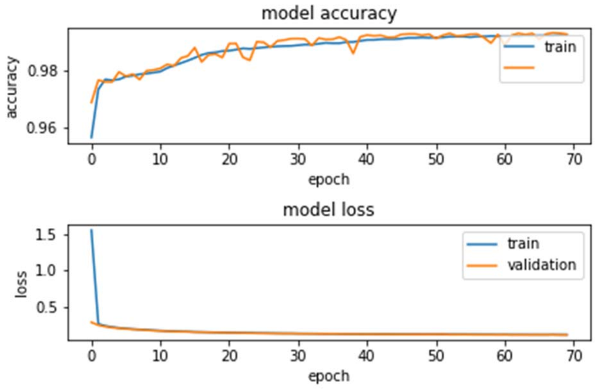

Fig. 8. Model accuracy vs model loss for the multiclass classification using DNN.

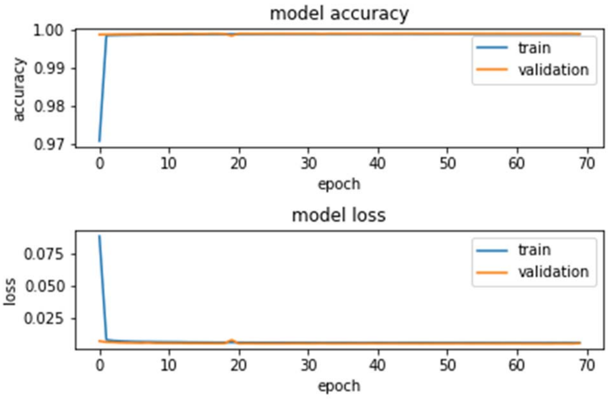

Fig. 9. Model accuracy vs model loss for the multiclass classification using LSTM.

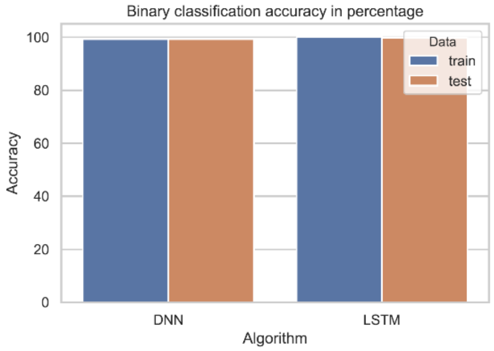

Fig. 10. Binary classification accuracy.

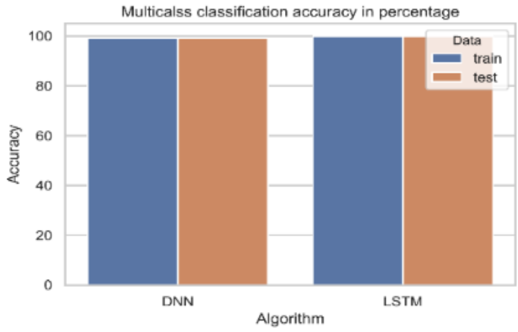

Fig. 11. Multi-class classification accuracy

B. Performance Metrics

In this work, in order to quantify the performance of the proposed detection method, some performance metrics have been considered, such as accuracy, precision, recall, and F-1 score (defined below) from the confusion matrix. The confusion matrix generally reflects how efficiently a particular machine/algorithm classifies the actual data. It is the most ubiquitous matrix for the performance evaluation of the classifier, which is shown in table 2, where the meaning of TP, FP, FN, and TN are described below.

TABLE II. CONFUSION MATRIX

Actual class↓\Predicted class→	Anomaly	Normal
Anomaly	TP	FN
Normal	FP	TN

- True positive(TP): correctly classified intrusion,
- False-positive(FP): non-intrusive behavior wrongly classified as an intrusion,
- False-negative(FN): intrusive behavior wrongly classified as non-intrusive,
- True negative(TN): correctly classified non-intrusive behavior.

Precision: it estimates the ratio of correctly classified attacks to the number of all identified attacks. Precision represents the repeatability and reproducibility of the model ($Precision \in= [0,1]$). The higher the precision, the better the ML model.

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

True positive rate/Recall: It estimates the ratio of a correctly classified anomaly to all anomaly data. A higher value is desired to be a better ML model and is given by: ($Recall \in= [0,1]$)

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

F1-Score/Measure: It is the harmonic mean of precision and recall. A higher value of F1-score represents the good ML model ($F1 - score \in= [0,1]$) and given by

$$F1 - score = 2 * \frac{Precision * Recall}{Precison + Recall} \tag{4}$$

TABLE III. CLASSIFICATION METRICS FOR DNN AND LSTM FOR BINARY CLASSIFICATION

Algorithm	Data	Precision	Recall	F1-score
DNN_Binary	Attack	1	0.99	0.99
DNN_Binary	Benign	0.98	1	0.99
LSTM_Binary	Attack	1	1	1
LSTM_Binary	Benign	1	1	1

The perfect score of all three metrics (precision, recall, and F1-score) suggests that LSTM-based IDS has superior classification performance as compared to DNN-based IDS for the binary classification (attack or benign), as shown in Table III.

TABLE IV. CLASSIFICATION METRICS OF DNN FOR MULTI-CLASS CLASSIFICATION

Attack Class	Precision	Recall	F1-score	support
Benign	1.00	1.00	1.00	430408
DoS attacks-GoldenEye	0.99	0.80	0.88	12361
DoS attacks-Hulk	0.98	1.00	0.99	138678
DoS attacks-SlowHTTPTest	0.99	1.00	1.00	42022
DoS attacks-Slowloris	1	0.70	0.82	3268

TABLE V. CLASSIFICATION METRICS OF LSTM FOR MULTI-CLASS CLASSIFICATION

Attack Class	Precision	Recall	F1-score	support
Benign	1.00	1.00	1.00	430977
DoS attacks-GoldenEye	1.00	1.00	1.00	12348
DoS attacks-Hulk	1.00	1.00	1.00	138126
DoS attacks-SlowHTTPTest	1.00	1.00	1.00	41959
DoS attacks-Slowloris	1.00	0.99	0.99	3327

Tables IV and V represent the detailed performance metrics of our proposed classifiers (DNN and LSTM, respectively) with respect to each category (4 different attack categories and a normal/benign category) for multiclass classification. The support in the Tables represents the number of samples of true responses that lie in that class. As shown in Tables IV and V, the LSTM-based IDS is superior in terms of multi-class classification compared to the DNN-based IDS as represented by higher precision, recall, and F1-score. Also, for the imbalanced classes and class having comparatively less data (for instance: DoS attacks-Slowloris), the LSTM-based IDS exhibits good performance metrics with precision=1, recall=0.99, and F1-score of 0.99 as opposed to the DNN-based IDS with precision=1, recall=0.70 and F1-score= 0.82.

VI. CONCLUSION

We proposed the novel, deep learning-based IDS model to detect the DoS attacks in the EVCS. The proposed LSTM based IDS outperformed another proposed DNN based IDS in terms of accuracy, precision, recall, and F1-score for the binary as well as multiclass classification and achieved the desired training accuracy of around 99.95% within the 10 epochs as opposed to 70 epochs in the DNN approach. Therefore, the LSTM can be considered as an effective algorithm to detect the DoS attack in the EVCS. This novel application could safeguard the EVCS and its stakeholders from possible cyber threats. Adding new kinds of attack data in training, the proposed model could easily scale up to detect more and diverse attacks. It ensures the scalability and interoperability of our model.

The future research direction would be towards the reinforcement-based IDS development for the same problem.

All the deep learning-based IDS suffer from traffic imbalance as well as a high false alarm rate. These topics would be addressed in the future for the EVCS.

Acknowledgment

The authors would like to thank the University of Memphis for providing Carnegie R1 doctoral fellowship and all required resources to complete this research.

References

[1] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical System Security of Vehicle Charging Stations," in *2019 IEEE Green Technologies Conference(GreenTech)*, Lafayette, LA, USA, 2019, pp. 1–5, doi: 10.1109/GreenTech.2019.8767141.

[2] I. S. Bayram and I. Papapanagiotou, "A survey on communication technologies and requirements for internet of electric vehicles," *EURASIP J. Wirel. Commun. Netw.*, vol. 2014, no. 1, p. 223, Dec. 2014, doi: 10.1186/1687-1499-2014-223.

[3] K. Harnett, B. Harris, D. Chin, and G. Watson, "DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report," p. 44.

[4] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, "A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures," in *2018 26th Telecommunications Forum (TELFOR)*, Belgrade, 2018, pp. 1–4, doi: 10.1109/TELFOR.2018.8611847.

[5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[6] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[7] D. Niyato, D. T. Hoang, P. Wang, and Z. Han, "Cyber Insurance for Plug-In Electric Vehicle Charging in Vehicle-to-Grid Systems," *IEEE Netw.*, vol. 31, no. 2, pp. 38–46, Mar. 2017, doi: 10.1109/MNET.2017.1600321NM.

[8] P. T. Krein and M. A. Fasugba, "Vehicle-to-grid power system services with electric and plug-in vehicles based on flexibility in unidirectional charging," vol. 1, no. 1, p. 11, 2017.

[9] "IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html.

[10] "Cyber-security in smart grid: Survey and challenges - ScienceDirect." [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790617313423#aep-article-footnote-id1.

[11] "Applied Cyber Security and the Smart Grid - 1st Edition." [Online]. Available: https://www.elsevier.com/books/applied-cyber-security-and-the-smart-grid/knapp/978-1-59749-998-9.

[12] "The Basics of Hacking and Penetration Testing - 2nd Edition." [Online]. Available: https://www.elsevier.com/books/the-basics-of-hacking-and-penetration-testing/engebretson/978-0-12-411644-3.

[13] "A denial of service attack in advanced metering infrastructure network - IEEE Conference Publication." [Online]. Available: https://ieeexplore.ieee.org/document/6883456.

[14] "Delayed inputs attack on load frequency control in smart grid - IEEE Conference Publication." [Online]. Available: https://ieeexplore.ieee.org/document/6816508.

[15] "Time Synchronization Attack in Smart Grid: Impact and Analysis - IEEE Journals & Magazine." [Online]. Available: https://ieeexplore.ieee.org/document/6400273.

[16] "Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems - IEEE Journals & Magazine." [Online]. Available: https://ieeexplore.ieee.org/document/7127023.

[17] "The Importance of DDoS Attack Visibility - Corero | Corero." [Online]. Available: https://www.corero.com/blog/the-importance-of-ddos-attack-visibility/.

[18] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[19] S. Park, M. Kim, and S. Lee, "Anomaly Detection for HTTP Using Convolutional Autoencoders," *IEEE Access*, vol. 6, pp. 70884–70901, 2018, doi: 10.1109/ACCESS.2018.2881003.

[20] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, 2009, pp. 1–6, doi: 10.1109/CISDA.2009.5356528.

[21] "NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB." [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html.

[22] N. Moustafa and J. Slay, "The Significant Features of the UNSW-NB15 and the KDD99 Data Sets for Network Intrusion Detection Systems," in *2015 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, Kyoto, Japan, 2015, pp. 25–31, doi: 10.1109/BADGERS.2015.014.

[23] J. Song, H. Takakura, and Y. Okabe, "Description of Kyoto University Benchmark Data," p. 3.

[24] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *J. Sens.*, vol. 2016, pp. 1–16, 2016, doi: 10.1155/2016/4731953.

[25] "IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html.

[26] "Optimizers - Keras Documentation." [Online]. Available: https://keras.io/optimizers/.

[27] "Regularizers - Keras Documentation." [Online]. Available: https://keras.io/regularizers/.

[28] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," in *2016 International Conference on Platform Technology and Service (PlatCon)*, 2016, pp. 1–5, doi: 10.1109/PlatCon.2016.7456805.