2022 IEEE International Performance, Computing, and Communications Conference (IPCCC) | 978-1-6654-8018-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/IPCCC55026.2022.9894305

MODLSTM: A Method to Recognize DoS Attacks on Modbus/TCP

Hao Zhang*[1,2], Yuandong Min[1,2], Sanya Liu[1,2],Hang Tong[1,2], Yaopeng Li[1,2]
[1] National Engineering Research Center for E-Learning, Faculty of Artificial Intelligence in Education, Central China Normal University, Wuhan 430079, China
[2] National Engineering Laboratory for Educational Big Data, Faculty of Artificial Intelligence in Education, Central China Normal University, Wuhan 430079, China
{zhanghao,lsy5918}@mail.ccnu.edu.cn,{yuandong,tonghang,liyaopeng}@mails.ccnu.edu.cn

***Abstract*—With the rapid development of technology, the scale of traffics in industrial control networks is increasing day by day. More malicious traffics brought terrible impacts on industrial areas. Modbus plays a momentous role in the communications of Industrial Control Systems (ICS), but it's vulnerable to Denial of Service attacks(DoS). Traditional methods cannot perform well on fine-grained detection tasks which could contribute to locating targets of DoS and preventing the destruction. Considering the temporal locality and high dimension of malicious traffic, we proposed a Neural Network architecture named MODLSTM, which consists of three parts: input preprocessing, feature recoding, and traffic classification. By virtue of the design, MODLSTM can perform high-precision identification and fine-grained classification of DOS attacks in the Modbus/TCP-based system. To test our model's performances, we conducted experiments on our traffic dataset collected from the industrial control network, and the models achieved excellent performances in comparison with previous work(accuracy increased by 0.74%). The results show that our proposed method has satisfactory abilities to detect DoS attacks related to Modbus, it could help to build a reliable firewall to address the DoS traffic in industrial environments.**

***Index Terms*—Modbus, DoS, Deep Learning, Fine-grained Classification.**

I. Introduction

As a common network protocol of Industrial Control Systems (ICS), Modbus plays a momentous role in the function of monitoring and controlling field devices. Yet, facilities related to Modbus are becoming more and more vulnerable to malicious traffic. One of the reasons is the emergence of attacks within the more prosperous Internet Of Things (IoT), not only in ICS, but also every industry is plagued by malicious traffic [1]; another cause is Modbus itself is an insecure protocol, and most central Supervisory Control and Data Acquisition Systems (SCADA) are built on legacy systems because of the updating is high-costed [2]. Due to the internal defects of the Modbus protocol, and the rapid development of the external Industrial Internet of Things (IIoT), these systems are threatened by more and more malicious traffic, in particular broken by Denial of Service Attacks (DoS) [3], e.g. Internal infiltrators paralyzed Venezuela's power grid in 2020 and caused huge accident cost. Hence, building a reliable and effective detector in the industrial field is necessary and urgent.

Two reasons cause the insecurity of Modbus protocol. On the one hand, Modbus was designed initially to focus on satisfying efficient instruction delivery in industrial scenarios, **its fields contain only the control codes related to coils and registers, but not the function codes that guarantee secure transmission**; on the other hand, **Modbus often runs on the base of TCP/IP protocol so inherits the insecurity of the lower layer**. These two issues have led to the vulnerability of the Modbus protocol. Because of the low cost of implementation and the obvious destructive power, DoS attacks pose a more serious security risk to Modbus-based industrial equipment.

Lots of researchers wants to get out of the dilemma from the perspective of bypass traffic analysis. To simulate malicious traffic, a Modbus penetration testing framework named SMOD was firstly developed, which could launch different types of DoS attacks in SCADA [4]. Based on SMOD, researchers used to build a rules base to defend against malicious traffic [5], this method can generally quickly locate the traffic but is no longer applicable in the emergencies of a new type of DoS attack. With the application of big data, some methods of Machine Learning (ML) were utilized in the field of network traffic detection, Modbus is no exception [6], ML technique did improve the security of Modbus devices, and lots of works could locate and solve the problem accused by DoS attacks like recently given 81% accuracy in the detection of DoS cyberattacks related to Modbus/TCP [7]. However, there're some challenges to feature selection in ML techniques. By virtue of the excellent power of feature extraction, Deep learning(DL) techniques are introduced to solve the problem of attack detection in industrial networks. A Multi-Layer Perceptron (MLP) and binary-based IDS were introduced and give good performances but they cannot do multi-classification task [8]. Recently a Generative Adversarial Network (GAN)-based method was given in the multi-classification experiment but there is a gap between simulation with an accuracy of 96.4% and real plant environment with an accuracy of 88.3% [9].

To overcome the challenges of existing research, a Neural Network architecture named MODLSTM based on time stream features extraction is introduced by our work, to effectively recognize the five types of DoS attacks(SINGLECOIL, MULTICOILS, SINGLEREGIS, MULTIREGIS, and GALILRIO) in the Modbus-based industrial environment. We utilized

the form of a time window to fuse traffic features and built a detector that can be applied to fine-grained identification of Modbus-based DoS attacks. Our method gives 90.03% accuracy in the experiment, it shows the reliable ability to locate malicious traffic related to DoS in the industrial area. Our work gave some contributions as follows.

1) A taxonomy is built around the attacks via Modbus/TCP, which is conducive to locating attack targets.
2) Presenting a universal malicious traffic detection model based on realizing the fusion of the latent features and its time series characteristics.
3) The effectiveness of a feature extraction method based on time window is verified, which provides a new idea for building an industrial firewall against DOS attacks.

II. Related Works

This section presents recent works on our topic. The former part expounds on the sources of Modbus insecurity, and introduces related works on enhancing security at the protocol level; the latter part organizes relevant research on preventing DoS attacks in Modbus-based networks, we also discuss the progress and shortcomings of current research.

A. The security of Modbus

ICS systems based on Modbus protocol are widely used in industrial fields [10]. However, Modbus does not provide complete security guarantees at the protocol level, because ICS is only designed to meet the communication needs in a small range at the beginning [11]. And with the expansion of the scope of ICS and the increase of data scale, many researchers have made enhancements to the Modbus protocol to ensure the security of the ICS system.

Lots of security enhancement research have been done in existing works. First, the TCP/IP protocol and the Modbus protocol are integrated at the protocol level into the industrial control system, then forming the Modbus/TCP protocol. However, the protocol will inherit the design defects of the TCP/IP protocol [12], [13]; Then based on the one-way feature of the cryptographic hash function, Liao et al. enhanced the reliability of the Modbus protocol while ensuring the storage cost in their work [14]; Luo and Li proposed a Modbus-E protocol in [11], which uses a hash function to ensure data uniqueness, and further uses symmetric key and digital signature technology to strengthen data authentication and confidentiality. Fovino et al. integrated integrity, authentication, non-repudiation, and anti-replay mechanisms to implement a Modbus-safe version for SCADA, and verified the availability of the protocol in a real-world environment in a power plant [15]. Further, Hayes et al. integrated hash message authentication and flow control transmission protocol, and designed a secure, compatible and stable authentication mechanism [16].

In summary, due to the limitations in the design of the Modbus protocol itself, researchers are accustomed to making enhancements at the transport layer to propose new security versions, which can be used to ensure the security of ICS systems in real scenarios properties (such as power grid) [17]. Pan et al. mentioned in a review [10] on the security of the Modbus protocol that there are three main problems with Modbus: lack of authentication, lack of authorization, and lack of encryption. Although existing methods have the potential to solve the above problems, protocol-based enhancements still have some disadvantages, such as: only filtering data but not traceability, which leads to such protocol-based enhancements in the face of increasing DoS attacks method does not guarantee security.

B. The detection of DoS attacks related to Modbus

In recent years, quantities of approaches were proposed to detect malicious attacks on devices using Modbus. In [3], S. Bhatia et al. confirm that the device used Modbus/TCP protocol is vulnerable to flooding attacks, and they described an experiment to show that their proposed signature-based detector is capable of detecting flooding attacks. In [5], T. Morris et al. wanted to use a rules-based approach to keep devices from being hacked. These works offer some demonstrations of the necessities of defending the Modbus device from intrusion, but it is unable to perform excellent detection abilities while facing strangers.

As mentioned above, building a large knowledge base can evade attacks of known malicious behaviors at the rule level, but when faced with unfamiliar malicious traffic, the rules will be useless. Therefore, S. Li et al. conducted experiments in a simulated environment and found that Decision Tree (DT) outperformed NN [6] while identifying unfamiliar traffic. Furthermore, Radoglou P et al. introduce an anomaly-based intrusion Detection System (IDS) capable of detecting DoS cyberattacks related to Modbus/TCP in [7], these efforts move away from the pre-knowledge base building but still rely on manual feature selection, which introduces subjectivity into the classification of malicious attacks.

The review of [18] shows that dividing traffic into two categories (benign or malicious) is not a challenge. So, one of the points of the work is to find a suitable model, which can be better applied to the scenarios related to Modbus' abnormal multi-classification problems. The work in [19] demonstrates DL models have easier training periods and better performance in the detection of attacks in general situations. Then some DL methods are recently introduced to get better performances in industrial areas, MLP shows satisfying performance in the binary classification problem and GAN gets a high accuracy while trying to divide the attacks into diverse categories [8] [9]. Among them are excellent works such as [9], however, these works do not validate its generalization abilities on a public dataset.

III. Methodology

In order to identify malicious traffic and locate the attack target, we demonstrate a high-dimensional temporal feature extraction method, the agriculture of our model is shown in Fig. 1. First, a traffic window is used to condense the flow feature in a specific time threshold, then we built a feature extraction module realized by Convoluted Auto Encoder(CAE),

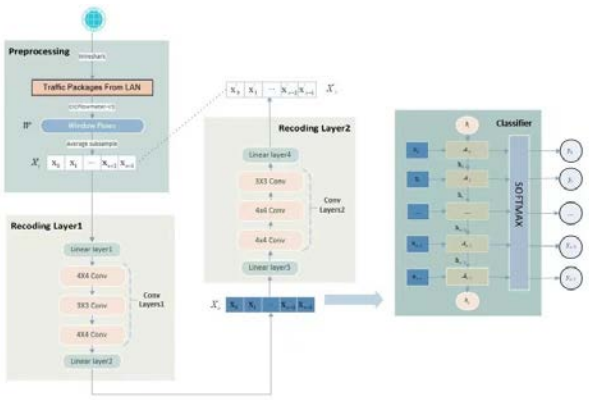

Fig. 1. Our proposed agriculture

TABLE I
TRAINING SET FEATURES

Types	Packets(pkts)	Flow
Counts/size	Tot Bwd Pkts,TotLen Fwd Pkts	Flow Byts/s,FIN Flag Cnt
	Bwd Header Len,TotLen Bwd Pkts	Subflow Fwd Byts
	Fwd Pkt Len Max,Fwd Pkt Len Min	Subflow Fwd Pkts
	Fwd Pkt Len Mean,Fwd Pkt Len Std	SYN Flag Cnt
	Bwd Pkt Len Max,Bwd Pkt Len Min	Init Bwd Win Byts
	Bwd Pkt Len Mean,Bwd Pkt Len Std	Down/Up Ratio
	Pkt Len Min,Pkt Len Var,Pkt Size Avg	Subflow Bwd Byts
	Pkt Len Mean,Tot Fwd Pkts	PSH Flag Cnt,Flow Pkts/s
	Bwd Seg Size Avg,Fwd Header Len	Subflow Bwd Pkts
	Fwd Seg Size Avg,Pkt Len Std	Init Fwd Win Byts
	Pkt Len Max,Fwd Act Data Pkts	ACK Flag Cnt
Time/Velocities	Fwd IAT Tot,Fwd IAT Mean	Flow Duration,Active Min
	Fwd IAT Std,Fwd IAT Max	Flow IAT Std,Flow IAT Max
	Fwd IAT Min,Bwd IAT Tot	Flow IAT Min,Active Mean
	Bwd IAT Mean,Bwd IAT Std	Active Max,,Flow IAT Mean
	Bwd IAT Max,Bwd IAT Min	Idle Mean,Idle Max,Idle Min
	Bwd PSH Flags,Fwd Pkts/s,Bwd Pkts/s	

at last, an appropriate classifier has been built to work on recognizing the malicious attacks.

A. Question presentation

Malicious traffic detection is a multi-classification problem. We intercepted all packages T in our LAN with a specific time window, then the features of time windows $X = [x_0, x_1, ...x_{n-1}]$ can be derived by G, where n represents the number of the window, and $Y = [y_1, y_2, ..., y_6]$ represents six categories of the traffic. Therefore, the task of our work is to recognize the type of our windows by our detector $F(X : G(T)) = \hat{Y}$.

B. Input preprocessing

Individual packets contain command information in network communication, while network flows can characterize the traffic. To extract the flow features during Modbus communication, we design a method: **compress the cut packets into continuous network streams with time windows and extract the flow characteristics.**

1) Traffic representation: We captured our real-time packages with the length of time windows is 10s, which can be aligned to the production of common public datasets. Then CICFlowmeter-V3 is utilized to extract the traffic flow features W:

$$W = \{w_0, w_1, ..., w_i, ...\}^T \tag{1}$$

from window flows, in which w_i is a matrix:

$$w_i = \begin{bmatrix} f_{(0,0)} & f_{(0,1)} & \cdots & f_{(0,dim-1)} \\ f_{(1,0)} & f_{(1,1)} & \cdots & f_{(1,dim-1)} \\ \cdots & \cdots & \cdots & \cdots \\ f_{(k_{i-1},0)} & f_{(k_{i-1},1)} & \cdots & f_{(k_{i-1},dim-1)} \end{bmatrix} \tag{2}$$

where $i \in N^+$ represents the index of traffic windows, $f_{(p,q)}$ is the value of the q-th feature of the p-th stream in the window, k_t represents the number of flows in t-th window.

2) Feature screening: There are 83 generated features in our flows [20], we located attacks' types Y by source IP in our work, where

$$Y = \{y_0, y_1, ...y_i, ...\}^T \tag{3}$$

, and y_i is One-Hot code which represents the type of our attacks. After our selection, there are 60 remained features marked with W', as shown in TABLE I.

3) Traffic window subsampling: Given each feature-selected w_i' for our flow windows' blocks, we extracted the condensed characters X by average subsampling options, which was inspired by the principle of the Average Pooling proposed by Lin [21]. X and W' have the same dimension:

$$X = \{x_0, x_1, ..., x_{n-1}\}^T \tag{4}$$

and there is a balanced transformation(BT) performed on the traffic flows' set from given w_i' in Eq. (2) :

$$x_i = BT(w_i') \tag{5}$$

which is defined as follows :

$$x_i = \frac{1}{k_t}\left[\sum_{m=0}^{k_t-1} f'_{(m,0)}, \sum_{m=0}^{k_t-1} f'_{(m,1)}, ..., \sum_{m=0}^{k_t-1} f'_{(m,dim-1)}\right] \tag{6}$$

then, By the above definitions, the condensed windows' features are calculated by the following expression: $X = BT(W')$.

C. Latent features recoding

As a type of unsupervised learning method, AE utilizes the output $X_i{}'$ which is reconstructed from the X_o to fit the initial input X_i. In our work, we improved the structures of Encoder and Decoder by some convolution kernels with different sizes.

$$X_o = L_2(C_1(L_1(BT(W')))) \tag{7}$$

and we need to reconstruct our input by the Convolutional Decoder:

$$X_i \approx X_i{}' = L_4(C_2(L_3(X_o))) \tag{8}$$

where L represents the Linear layer and C is the convolutional layer, and Mean Squared Error (MSE) is introduced, So there is our high-dimensional feature X_o given by optimizing related parameters β_1 in

$$\triangle\beta_1 \propto \frac{\partial Loss(X_i, X_i')}{\partial\beta_1} \tag{9}$$

D. Traffic classification

Our classification module absorbs Long short-term memory (LSTM) neural network architecture [22] to improve our classification periods. We used Softmax to calculate the probability distribution of estimated traffic categories Y', then BCELoss to measure the errors in our classification.

This structure based on the LSTM neural network realizes the function, which can divide the high-dimensional space formed by the training set samples with potential features X_o into different categories Y', thereby helping us build an excellent detector.

E. MODLSTM Model

In our work, the MODLSTM model is defined by the following descriptions:

- After preprocessing the initial data W, the selected traffic W' in each window is compressed into the corresponded features X by the method of Eq. (6).
- We used CAE to perform features extraction on X_i, so as to achieve the purpose of finding the nonlinear hidden code X_o, it's worth mentioning that a linear layer is utilized to prepare for our convolutional transformation.
- The latent feature X_o is taken as input to classification module, there we simplified the formulation of LSTM to $Y, H_t = LSTM(H_{t-1}, X)$, which H_t represents the hidden state including all gated neural units' situations in time t.

Above all, we could give a formal mathematical description that, our proposed method is aiming to get our detection F by using Back-Propagation(BP) to optimize BCELoss in the classification module with the classes' set Y and the input X_o, which is obtained from the minimizing of loss function by reconstructing X_i after we have gained the selected data W' without useless features in W.

IV. Experiments

To evaluate our proposed method's performance on DoS attack recognition, we demonstrated the experiment in our simulated ICS. To be specific, we applied the model (MODLSTM) to our dataset to evaluate its performance, traditional ML methods like K-Nearest Neighbor(KNN), Support Vector Machine(SVM), Random Forest(RF), and Based DL models such as Convolutional Neural Network(CNN), Recurrent Neural Network(RNN) and Long Short-Term Memory(LSTM) are utilized to make comparisons with our proposed model so as to verify the advances of our structure. The flow sequences in the experiment are labeled as six types, the details of the dataset are shown in TABLE II.

A. Dataset

To simulate the DoS attacks in ICS, we set up a local area network and conducted related attack experiments with the SMOD tool, 83 network traffic characteristics were extracted from our traffic [20]. Our work divided the traffic actions into six classes: benign, single coil (SINGLECOIL), multi coils (MULTICOILS), single register (SINGLEREGIS), multi registers (MULTIREGIS), and Galil RIO-47100 Programmable Logic Controller (GALILRIO), which depend on the aim object of attacks as [2] and [7]'s works, the data distribution is shown as Table II. All correspondences lasted more than five hours, and more than five hundred thousand flows were recorded.

TABLE II
Attacks Descriptions

Attack Type	Description	Windows Count	Flows count
GALILRIO	Attacks to Galil RIO-47100	97	43890
SINGLECOIL	Attacks to one coil	156	120090
SINGLEREGIS	Attacks to one register	134	33584
MULTICOILS	Attacks to selected coils	107	26812
MULTIREGIS	Attacks to selected registers	107	27966
BENIGN	Normal flows	1204	258100
ALL	-	1805	510442

B. Experiments Settings

All the models were trained on the same server equipped with AMD Ryzen 7 4800U and 16GB memory. We chose 25% and 75% of traffic for testing and training. Particularly, appropriate convolution kernels can extract better representations, according to our examinations, the Convolutional Encoder could catch the best performance when 3x3 and 4x4 filters are utilized in CAE, then generating 30 numbers of latent features. About our metrics, the confusion matrix is utilized to weight our performances of models, we also calculated the Accuracy, Precision, and Recall to show the abilities of each model.

C. Results and Analyses

Our model has the best comprehensive performance as Table III shows. In our experiments, the non-sequential methods, such as KNN, RF, and CNN, cannot play good roles in the fine-grained classification to attack targets, that verifies the characteristics of network attacks flow are temporal, so the experimental performances are improved when we use models such as RNN, LSTM. Furthermore, Our ablation experiments demonstrate that our constructed CAEs have better feature extraction capabilities than traditional AE methods, and LSTM has better recall than MLP, MODLSTM has the best performance which performs an accuracy of 90.04%.

Fig. 2 gives the confusion matrix, which shows two points: First, the non-sequential deep network cannot play a good role in the fine-grained classification to attack targets, and the temporal model has a better representation ability as the comparison between Fig. 2(a) and (b) show; Second, the ability of RNN model to judge whether the attacks are sent to multiple coils or multiple registers is weaker, we guess that the patterns of these two types of attacks are so similar that the loss is small, which leads to the disappears of the gradient, the LSTM model will improve this problem, our proposed model utilizes CAE to enhance the performance about recognizing the type of malicious actions, as shown in Fig. 2(c) and (d).

TABLE III
BEST RESULTS OF SIMILAR METHODS IN OUR DATASET OR CORRESPONDING WORKS

Model	Recall	Precision	Accuracy
KNN [23]	52.106	80.935	82.288
RF [7]	59.255	76.132	84.686
CNN [24]	58.051	57.567	84.133
DNN [19]	65.467	70.5	87.085
RNN	64.183	69.033	87.085
AE+RNN	64.467	71.417	86.901
CAE+RNN	67.017	72.383	87.823
MLP	53.674	74.1297	82.472
AE+MLP [25]	48.256	64.621	80.996
CAE+MLP	53.630	**81.631**	80.812
LSTM [26]	**70.733**	75.35	89.114
AE+LSTM	70.583	77.35	**89.299**
MODLSTM	**72.95**	**79.2**	**90.037**

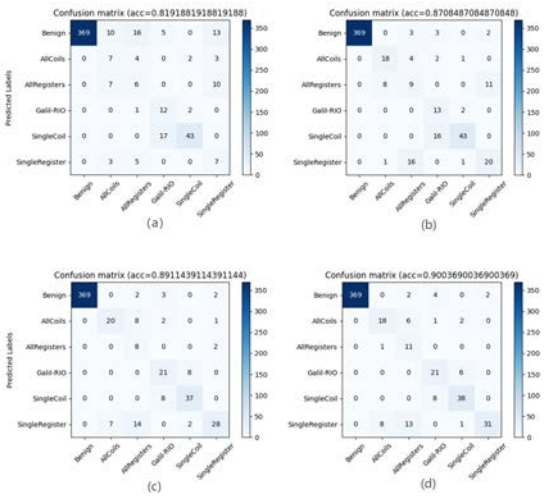

Fig. 2. Confusion matrix of (a)CNN (b)RNN (c)LSTM (d)MODLSTM

V. CONCLUSIONS

To cope with the increasing DoS attacks in ICS, our work designs a Neural Network architecture named MODLSTM that can be used for DoS attacks fine-grained classification related to Modbus protocol. The model consists of three parts: input preprocessing, feature recoding, and traffic classification, by virtue of the design, MODLSTM can form continuous stream semantics based on fragmented packets, discover potential low-dimensional features and finally classify traffic at a fine-grained level. The performance of our model in fine-grained classification is tested by DoS attacks in industrial scenarios. Experiments show that our model has the best overall multi-classification performance due to the consideration of the low-dimensional hidden features of network flows and their temporal relationships, which indicates that MODLSTM can be placed inside switches or routers to find the target module of malicious traffic, thereby isolating attacks.

ACKNOWLEDGMENT

This study was supported in part by grants from the National Natural Science Foundation of China(no.62077024).

REFERENCES

[1] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *Eai Endorsed Transactions on Security and Safety*, vol. 3, no. 9, p. e2, 2016.

[2] J. Luswata, P. Zavarsky, B. Swar, and D. Zvabva, "Analysis of scada security using penetration testing: A case study on modbus tcp protocol," in *2018 29th Biennial Symposium on Communications (BSC)*. IEEE, 2018, pp. 1–5.

[3] S. Bhatia, N. S. Kush, C. Djamaludin, A. J. Akande, and E. Foo, "Practical modbus flooding attack and detection," in *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]*. Australian Computer Society, 2014, pp. 57–65.

[4] N. Kapoor, "Scada penetration testing: Do i need to be prepared?" [EB/OL], https://research.aurainfosec.io/scada-penetration-testing/ Accessed April 19, 2017.

[5] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, "Deterministic intrusion detection rules for modbus protocols," in *2013 46th Hawaii International Conference on System Sciences*. IEEE, 2013, pp. 1773–1781.

[6] S.-C. Li, Y. Huang, B.-C. Tai, and C.-T. Lin, "Using data mining methods to detect simulated intrusions on a modbus network," in *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*. IEEE, 2017, pp. 143–148.

[7] P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Kourouniadis, K. Rompolos, and P. Sarigiannidis, "Implementation and detection of modbus cyberattacks," in *2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2020, pp. 1–4.

[8] A. El Safadi and J.-M. Flaus, "A deep learning approach for intrusion detection system in industry network," in *The first international conference on Big Data and Cybersecurity intelligence*, 12 2018.

[9] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1137–1151, 2021.

[10] X. Pan, Z. Wang, and Y. Sun, "Review of PLC Security Issues in Industrial Control System," *Journal of Cyber Security*, vol. 2, no. 2, pp. 69–83, 2020.

[11] X. Luo and Y. Li, "Security enhancement mechanism of modbus tcp protocol," *DEStech Transactions on Computer Science and Engineering*, 04 2019.

[12] W. Yu-bin, "Research on industrial control system security defense [j]," *Netinfo Security*, vol. 9, pp. 35–39, 2016.

[13] X. Chen and Z. Jia, "Industrial control network information security threats and vulnerability analysis and research," *Computer Science*, vol. 39, no. 10, pp. 4188–4190, 2012.

[14] G.-Y. Liao, Y.-J. Chen, W.-C. Lu, and T.-C. Cheng, "Toward authenticating the master in the modbus protocol," *IEEE Transactions on Power Delivery*, vol. 23, no. 4, pp. 2628–2629, 2008.

[15] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and Implementation of a Secure Modbus Protocol," in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, vol. 311, pp. 83–96, series Title: IFIP Advances in Information and Communication Technology.

[16] G. Hayes and K. El-Khatib, "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol," in *2013 Third International Conference on Communications and Information Technology (ICCIT)*. Beirut, Lebanon: IEEE, Jun. 2013, pp. 179–184. [Online]. Available: http://ieeexplore.ieee.org/document/6579545/

[17] M. K. Ferst, H. F. M. de Figueiredo, G. Denardin, and J. Lopes, "Implementation of Secure Communication With Modbus and Transport Layer Security protocols," in *2018 13th IEEE International Conference on Industry Applications (INDUSCON)*. São Paulo, Brazil: IEEE, Nov. 2018, pp. 155–162. [Online]. Available: https://ieeexplore.ieee.org/document/8627306/

[18] M. Gohil and S. Kumar, "Evaluation of classification algorithms for distributed denial of service attack detection," in *2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)*. IEEE, 2020, pp. 138–141.

[19] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of ddos attacks with feed forward based deep neural network model," *Expert Systems with Applications*, vol. 169, p. 114520, 2021.
[20] A. H. Lashkari, Y. Zang, G. Owhuo, M. Mamun, and G. Gil, "Cicflowmeter," 2017.
[21] M. Lin, Q. Chen, and S. Yan, "Network in network," *arXiv preprint arXiv:1312.4400*, 2013.
[22] S. Hochreiter, "The vanishing gradient problem during learning recurrent neural nets and problem solutions," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 6, pp. 107–116, 04 1998.
[23] H. Qu, J. Qin, W. Liu, and H. Chen, "Instruction detection in scada/modbus network based on machine learning," in *International Conference on Machine Learning and Intelligent Communications*. Springer, 2017, pp. 437–454.
[24] Y. Hu, D. Zhang, G. Cao, and Q. Pan, "Network data analysis and anomaly detection using cnn technique for industrial control systems security," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*. IEEE, 2019, pp. 593–597.
[25] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "Ae-mlp: A hybrid deep learning approach for ddos detection and classification," *IEEE Access*, vol. 9, pp. 146 810–146 821, 2021.
[26] P. Mieden and R. Beltman, "Network anomaly detection in modbus tcp industrial control systems," University of Amsterdam, Tech. Rep., 2020.