Design of Intrusion Prevention System for OT Networks Using Deep Neural Networks

Akshay Rajapkar
Department of Electrical Engineering
Veermata Jijabai Technological Institute
Mumbai, India
aurajapkar_m18@et.vjti.ac.in

Pranita Binnar
Department of Computer Engineering
Veermata Jijabai Technological Institute
Mumbai, India
pbbinnar_p19@ce.vjti.ac.in

Dr. Faruk Kazi
Department of Electrical Engineering
Veermata Jijabai Technological Institute
Mumbai, India
fskazi@el.vjti.ac.in

***Abstract*—The Automation industries that uses Supervisory Control and Data Acquisition (SCADA) systems are highly vulnerable for Network threats. Systems that are air-gapped and isolated from the internet are highly affected due to insider attacks like Spoofing, DOS and Malware threats that affects confidentiality, integrity and availability of Operational Technology (OT) system elements and degrade its performance even though security measures are taken. In this paper, a behavior-based intrusion prevention system (IPS) is designed for OT networks. The proposed system is implemented on SCADA test bed with two systems replicates automation scenarios in industry. This paper describes 4 main classes of cyber-attacks with their subclasses against SCADA systems and methodology with design of components of IPS system, database creation, Baselines and deployment of system in environment. IPS system identifies not only IT protocols but also Industry Control System (ICS) protocols Modbus and DNP3 with their inside communication fields using deep packet inspection (DPI). The analytical results show 99.89% accuracy on binary classification and 97.95% accuracy on multiclass classification of different attack vectors performed on network with low false positive rate. These results are also validated by actual deployment of IPS in SCADA systems with the prevention of DOS attack.**

***Keywords*—OT Network, SCADA, Intrusion prevention system, Modbus, DNP3, Deep packet inspection, Deep Neural Network**

I. Introduction

Over a period of time wired logic and relays were replaced by a Programmable Logic Controllers (PLC) and adopted by OT networks due to less hardware structure and ease of programming. In industry automation scenarios large number of PLCs handles process operations, quantity measurements and electromechanical tasks. These operations are controlled and monitored by SCADA system that connects different field devices, human-machine interface (HMI), monitoring workstations and networking devices. SCADA communication architecture comprise of different hierarchy levels. Top level contains database, Master Terminal Unit (MTU), SCADA system. Middle layer contains Remote Terminal Unit (RTU), HMI and networking devices and root level contains field devices like PLCs [6]. They are vulnerable to many cyber threats as system architecture consist of devices that works on many IT and ICS protocols. Data logged by SCADA systems is stored by Historian and sent over wireless internet gateways to the remote servers for the further analytics as a part of new emerging era of Industrial Internet of Things (IIOT) also known as Industry 4.0. This increases the risk of numerous cyber-attacks causing threat to integrity and availability of SCADA services.

ICS critical infrastructures like power plants, storage systems, water treatment plants and those provides essential services are always targeted by hackers and on high risks. Injection of malware into systems by means of social engineering and exploit the system by scanning, spoofing and malicious command and data injections. System lost its confidentiality when attacker comes in between communication of SCADA and PLC and can sniff the data related to system parameter, control information. Integrity issue arises when false data and command injected by compromised workstation, leads to force control system to measure wrong parameter and to take decision corresponds to misleading data. Unavailability of system control and communication due to Denial of service (DOS) and flooding attacks can cause havoc in plants like power generators [11]. Available data encryption and threat detection algorithms, firewalls are not enough to get rid of advance attack vectors. This leads to find out methods to detect and prevent network intrusion by monitoring network activities not only on source-sink based but must check the various fields of communication parameters.

In this paper, we propose behavior-based intrusion prevention system for OT networks, capable of identifying and preventing network activities causing threat to critical infrastructure of SCADA system. This paper has three primary contributions

- Design and deployment of all components of Intrusion Prevention System. Also discuss creation of dataset from real SCADA test bed.
- This paper presents attack threats designed for MODBUS and DNP3 protocols along with Malware and backdoor injection. Each attack vector described in detail.
- Proposed system is capable of preventing anomalies based on created baselines as well as deep neural network designed for binary and multiclass classification.

The rest of the paper organized as section II provides existing and related work, section III discusses experimental setup, attack scenario and design methodology of IPS. Finally system is validated by experimental results in section IV.

II. Related work

OT network traffic of SCADA systems is significantly different from IT/corporate network traffic. The features are different from those of most of intrusion detection systems trained on. In [2], hidden features of data can be discovered by applying improved nearest neighbor algorithm and preprocessed using dimensionality reduction algorithms. However, less consideration of features shows low detection rate. Data can be categorized in different groups such as basic characteristic, content characteristic, Traffic characteristics based on time and based on source and destination address of data [3]. However, used dataset is subset of IT dataset and no correlation in different groups and hence cannot predict the series of events. Distributed Intrusion Detection System (DIDS) for SCADA [4], focuses on domain specific features and modification developed for the control system rather than rely on IT based solutions. One class SVM is used to classify outliers and focuses only legitimate data required for ICS systems collected from actual industry scenarios. However, the model does not manage false positive results. Such detection methods also suffer from overfitting of models.

Open source PLC is used to encrypt (AES-256) its data of SCADA [1][5]. Packet interarrival time and packet processing time are two parameters used for training a clustering algorithm to find out the outliers. Despite of encryption that protects against Man-in-the-middle (MITM) attacks, it is less sensitive to flooding attacks. Comprehensive Packet Inspection, which inspect correlation of various fields in packet payload use over conventional SCADA firewalls [7]. However, algorithm with low latency can be used with real system but it has many false positives as system also generates out of sequence packets. The Boltzmann machine-learning algorithm performs the classification process on ICS dataset [8]. However, system latency is high due to dual clustering and finding similar vectors within clusters of data, making this unable to cope up with real time SCADA systems. Data size is reduced while maintaining critical patterns by using STEM (State Tracking & Extraction Method) [9]. However, proposed algorithm is not tested on any Industrial specific protocol to validate its effectiveness in SCADA systems. Proposed methodology to transform behaviour rules to a state machine [10], but additional efforts are necessary to taken to convert protocol-based communication to state model and results can be improved using Machine learning algorithms.

Main challenge of OT networks in ICS security is to deal with unbalanced and pre-processed intrusion datasets [3][5]. Each data is different for different applications of SCADA systems. One of the gaps identified in current mechanisms is inadequacy in methods of data collection, feature extraction and dealing with identified malicious traffic. In this paper, the work is motivated to design complete prevention mechanism which collects data by analyzing application layer of traffic and features are extracted using deep packet inspection (DPI) and models the SCADA network behavior using deep neural network (DNN) to prevent security threats.

III. System Modelling and IPS Design

A. SCADA testbed and Attack scenario

Fig. 1 illustrate a SCADA system consists of PLC and Modbus/TCP gateway connected in network through L2 switch as field devices. One is MOXA MGate-MB3480 as Modbus/TCP gateway, controlling variable frequency device (VFD) which controls the motor speed. The HMI shows speed of the motor, voltage and current readings. HMI controls the speed upto 20 Hz as well as rotation of motor i.e. forward or reverse. All the control commands are excited by SCADA and it keeps the track of communication between PLC and HMI by logging data into database. The entire communication is modeled over MODBUS protocol.

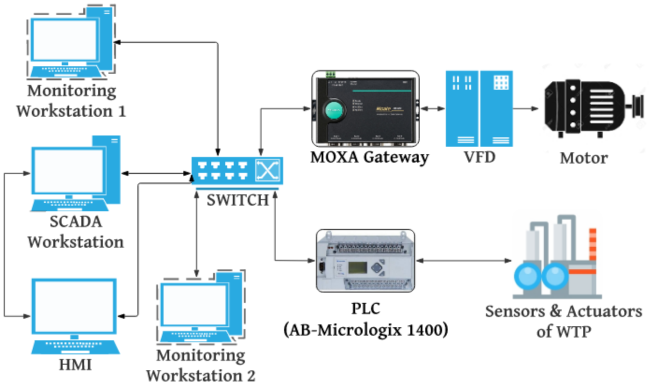

Fig. 1. SCADA test bed

Another system is Industrial wastewater treatment plant (WTP) handled by Allen Bradley MicroLogix-1400 PLC. The system consists of five water tanks in which water level, temperature in tanks and pressure of centrifugal pumps are controlled by setting set points values in SCADA. The PLC can support Ethernet/IP, Modbus TCP and DNP3 protocols. In this setup PLC is configured with Modbus TCP and DNP3 for communication between PLC and SCADA.

In SCADA network attack scenario we assume that attacker is manage to get a machine to perform network scan, gather information or to inject malware by social engineering or by advance remote access techniques. The attacker can enter into network by compromising any legitimate system connected to network. The set of attacks describe in this paper are classified into four main classes Reconnaissance, data and command injection by spoofing, Denial of service (UDP scan and MODBUS flooding), Malware and backdoor injection.

a) Reconnaissance: To perform successful attack, attacker should know entire network architecture, open ports on which services are running and protocols used in communication. All such information is collect by Reconnaissance attacks. In this particular test case, Reconnaissance consists of four types of scan: Ping scan is use to detect active hosts on network by using ICMP request and reply pairs. Open TCP ports and services served on these ports are identified by TCP port scan and service discovery perform on active hosts.

Similar to TCP port scan, UDP ports and their services are also scan by UDP ports and service scan perform by network mapping tool. Finally, hardware firmware version, operating system and information about service software versions is gather by stealth scan for OS and version detection. By knowing firmware and service version, a particular CVE (Common Vulnerabilities and Exposures) and predefined attacks can be launch by attacker.

b) False data and command injection by spoofing: TCP/IP encapsulated MODBUS, DNP3 protocols are not encrypted, while executing commands over PLC there is no security feature that can authorize the communication. Such systems are sensitive to spoofing and Man-in-the-middle (MITM) attacks. Performed MITM by ARP spoofing on Modbus/TCP gateway and SCADA system attacker can listen to communication and gain the knowledge of control commands, function codes and data. Attacker generate same packet and send to Modbus/TCP gateway to start/stop motor and even change the frequency of operation by executing same function code. The frequency of operation can exceeds its safety limit of 20 Hz by attacker, and operate beyond that upto 50 Hz and SCADA system can be spoofed by false acknowledgement sent by attacker.

c) Denial of service (UDP scan and MODBUS flooding): DOS attack performed on PLC, drops the connection with all the hosts in network. Instead of flooding entire network with packets, only PLC is targeted at port 502 with UDP scan to stop the service of Modbus communication. To bypass the Tofino firewall that passes only Modbus traffic to PLC, Modbus-flooding attack is performed and achieved same results as of UDP scan.

d) Malware and backdoor injection: Malware is injected with backdoor embedded in it and execute the malicious code written in python when any user clicks the image or pdf file of malware. Once code is active it can scan the entire subnet of network for active hosts, scans their TCP ports and finds services for ICS protocols, in this case it is Modbus. The code list out the target IPs that serves the Modbus services and start the reverse shell connection with compromise host to download important network information. Once connection is closed, it performs DOS as UDP scan on targets identified during scan and break the communication of Modbus protocol.

B. Data preparation and Methodology

Components of any conventional Intrusion detection or prevention system consist of sniffer, preprocessor, detection engine, rule set and output modules. Sniffer part collects data from the interface connected to network. Different fields of these packets are preprocessed by preprocessor and detection engine checks correlation of packet parameters with rule set. This conventional detection system should have prior knowledge of normal traffic and possible known threats to design rule database for protecting system. However, this works fine for known attacks but such systems are vulnerable for zero-day attacks and even for fine parameter tuning and modified conventional attacks. Proposed Intrusion prevention architecture in Fig. 2 consist all these components but additional features added to overcome drawbacks of rule-based prevention, identifying ICS protocols at application layer and implementation of deep neural network (DNN).

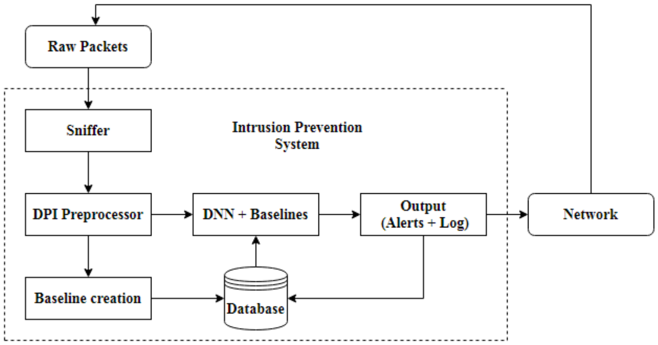

Fig. 2. IPS Architecture

a) Sniffer: Collection of network traffic is achieved by port mirroring of centralized switch of the network but it does not provide the control of packet, either to accept of drop the packet based on decision taken by the detection block. Hence to allow packet flowing through the IPS system policy-based chains in iptables provided by Linux kernel are used. Iptables consist of three types of tables (Filter, Nat, and Mangle) and each table provides different chains which consist of network flow. Filter table with Forward chain is use to design sniffer module which routes the entire traffic coming on switch port through the IPS system.

b) DPI Preprocessor: Raw packets collected by sniffer module are stacked into Netfilterqueue, which allows handling packets matched by iptables chain. Features of raw packets are extracts based on layers of TCP/IP protocol suite. All features that are extracted are described in Table I with corresponding network layer. Ethernet layer provides source and destination MAC address, identifies hosts communicating on network. MAC address for each host is unique and hence it proves an important evidence while detection MITM attacks by ARP spoofing. IP layer at layer 2 consist of IP address of source and destination entities. This layer also specifies protocol, which is use by communication. Length of an IP packet including checksum is also an important feature for detecting integrity of packets.

TABLE I
FEATURES EXTRACTED BY DPI PREPROCESSOR

TCP/IP layer	Network traffic features
L1: Network interface layer	Source MAC address
	Destination MAC address
L2: Network layer	Source IP address
	Destination IP address
	Length of packet
L3: Transport layer	TCP/UDP Source port number
	TCP/UDP Destination port number
	Flags
L4: Application layer	ICS Protocol

Transmission layer specifies type of connection i.e. connection oriented (TCP) or connectionless (UDP). SCADA mostly uses TCP connection that ensures connectivity by three-way handshaking policy of TCP protocol and hence, flags used by the TCP connection is important feature while validating a particular communication. In this layer, port number of source and destination hosts are also mentioned. Port number signifies the type of service use by the communication. In SCADA systems type of services and their port number are fixed (102,502: MODBUS, 20000: DNP3) hence, port number proves and important feature in SCADA communication.

Application layer protocols such as MODBUS and DNP3 which are generally not specified in IP protocol table is an important part that distinguishes SCADA based IPS from normal IT based IPS. Fields of MODBUS and DNP3 protocols are encapsulated within TCP payload and hence deep packet inspection (DPI) is required to identify presence of these protocols. At the start 7 bytes of Modbus Application header (MBAP) is appended. Header of Modbus packet is identified by its protocol identifier, which always set to 0x00 in TCP payloads. Distributed Network Protocol 3.0 (DNP3) comprise of link layer, transport layer and application layer with variable load encapsulated in TCP/ UDP payload. Packet start with link layer consists of magic byte at the start, signaling this is DNP3 protocol with value 0x0564. Along with these 9 features mention in Table I also time of arrival of packet into system also extracted by DPI preprocessor block. Further all packets with these extracted features are logged into CSV file format.

c) Baseline creation and static based detection: Baselines are signatures of normal traffic data created over training period of network traffic analysis and removes the need of create rules for known traffic data. The training period consist of 5 observation sets and each set have records of normal as well as malicious traffic data. The summary of data preparation is shown in Table II. The most common TCP traffic is identified in each observation set as TCP handshakes are initiated before each MODBUS and DNP3 packet transmission. Modbus and DNP3 traffic is legitimate traffic of PLC, Modbus/TCP gateway and SCADA devices. Reconnaissance attack consist of Ping scan, TCP and UDP port scans and finding out their services and OS versions by stealth scan are recorded in observation set 3 and 4. Last observation set is of actual Malware injection and DOS attack by UDP scan and Modbus flooding. Malware data also consist of initial stage of TCP/UDP scans and allows backdoor to record network information. DOS attack is initiated as result of successful target identification of Malware and breaks the communication of legitimate PLC and Modbus/TCP gateway traffic.

TABLE II
NETWORK TRAFFIC DATA PREPARATION

Obs set	Type of traffic	Description	No. of Records
1	Normal	TCP, DNP3 traffic	45674
2	Normal	TCP, ICMP MODBUS traffic	61187
3	Normal + Attack	TCP, MODBUS Ping scan, MITM	58218
4	Normal + Attack	TCP, DNP3, TCP+ UDP port scan Stealth scan and OS detection	68607
5	Normal + Attack	TCP, DNP3 MODBUS Malware injection DOS	57606

In SCADA communication, most of packets and control signals are repeated over a time and hence it is essential to remove such duplicate entries from the database. A data cleaning operation is performed to clean the database and unique set of communication is achieved as a Baselines of SCADA communication. after comparing features of each entry and discarding duplicate traffic, the final database consist of 55998 normal data baselines and 49152 records corresponds to attack data. The protocol distribution of Normal and Malicious traffic shown in Fig. 3. Balanced entries of TCP protocol are observed for both type of traffic, while UDP protocol is used for port scanning and UDP scan flooding hence only exists in attack data. Attack data is further classified into different classes of attacks and separated from normal dataset. Fig. 4 shows percentage-wise distribution of different classes in attack database.

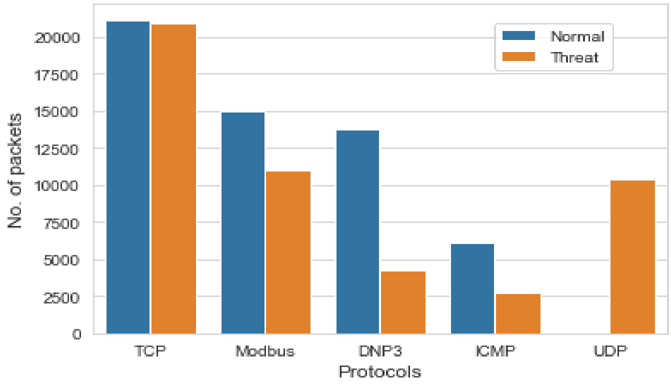

Fig. 3. Protocol distribution of database

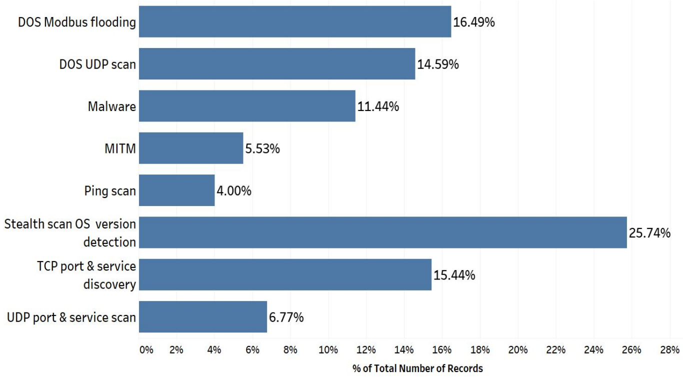

Fig. 4. Attack data distribution (%)

Both normal and malicious traffic is stored into database in

CSV format for carried out analytics and forensic operations. Further these baselines are use as lookup for evaluating packets over real time scenarios as well as it is use as network traffic dataset for training a deep neural network model.

d) Design of Deep Neural Network (DNN): Deep learning is use to identify the behavior of network traffic. The disadvantage of static based intrusion detection is that they susceptible to zero-day attack and unable to find attack patterns. This shortcoming is overcome by applying machine learning techniques to learn patterns in network data and to take decisions based on features extracted from raw packets.

9 essential features extracted from preprocessor layer and created baselines are feed as normal and attack traffic to train deep neural network. Fig. 5 shows design flow of DNN. Preprocessed data collected from baselines, some data cleaning operations need to be perform to prepare dataset for training of neural network. Converting categorical features like source and destination IP and MAC address, protocols, flags into integer format suitable for performing numerical operations during training is required. Hence, these features are encoded using category encoders into binary encoded values, for each unique observation into categorical feature it generates its binary equivalent value. Further to minimize the error due to sudden variations into data points, all data points are normalized and scaled before training. Encoding categorical features increase the dimensionality of data to 39, hence dense input layer consist of 39 neurons for each input value follow by two hidden layers of 20 neurons with 20% of neurons in each layer drop randomly to avoid over-fitting of model. Output layer of 1 neuron in binary classification (39-20-20-1) represent the class of packet i.e. normal or malicious. Another model with 7 neurons in output layer is trained for multiclass classification (39-20-20-7) that identifies different classes of attacks.

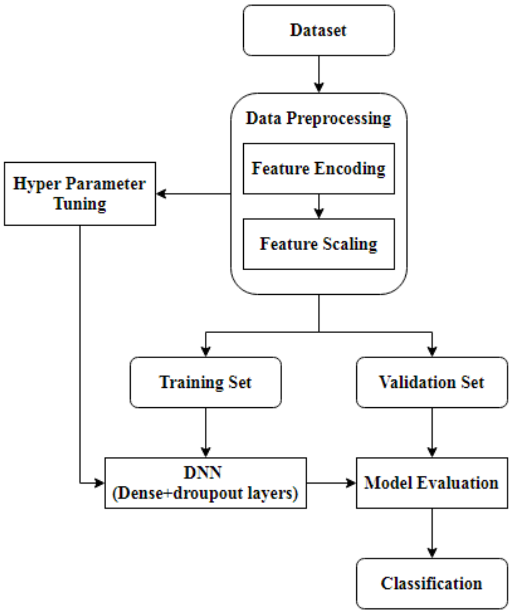

Fig. 5. DNN training and validation flowchart

IV. Results and Discussion

The designed DNN model is evaluated on test set. Accuracy, Sensitivity, Recall, Specificity, precision, F1-score are the metrics used to check the effectiveness of proposed intrusion prevention model on real SCADA data are discussed in Table III. The 70% data points are used for training model and 30% data points use for testing and validating model performance.

TABLE III
Binary classification evaluation metrics

	Precision	Recall	TPR	FPR	F1-score
Binary classes	100	99.75	99.75	0.24	99.98

Proposed model classify normal and malicious traffic with accuracy of 99.89% with low false positive rate (FPR) or Specificity of 0.24% indicates that less probability of misclassification of malicious traffic as normal. Recall with 99.75% value indicates number of data points classified as intrusion class over total number of intrusions. Precision of 100% indicates intrusion is detected as intrusion as this metric is measured for intrusion class. F-measure considers effects of both metrics of recall and precision as a harmonic mean of both. 99.98% of F1-score assures better performance of model. The True Positive Rate (TPR) or Sensitivity corresponds to measure of positive data correctly classified considering all positive data points. This model gives sensitivity of 99.75%.

TABLE IV
Multiclass evaluation metrics

Classes	Precision	Recall	F1-score
Normal	100	98	99
DOS Modbus flooding	90	98	94
DOS UDP scan	97	91	94
MITM	97	100	98
Malware stealth scan	99	99	99
Ping scan	100	100	100
UDP port & service scan	100	97	98

The model with 7 neurons in output layer is trained and tested for different classes of attacks gives overall accuracy of 97.95% and all evaluation metrics for each class is explain in Table IV. Malware, first scans the entire network as discussed in attack scenario, hence TCP port and stealth scan shown in Fig. 4 are merged into Malware class. Normal network traffic, Ping scan and UDP port and service scan are identified with high accuracy. The high accuracy is due to ping scan contains only ICMP packets from unknown source and UDP packets differ from normal behavior of network traffic shown in protocol distribution of network data in Fig. 3. DOS Modbus flooding and DOS UDP scan have relatively low precision and recall respectively. Packet of Modbus flooding and UDP scan are overlap with normal traffic and UDP port scan and hence misclassified as both type of DOS attacks and achieved relatively low accuracy than other classes. Less precision in MITM class is due to less number of observations were recorded in dataset.

The proposed model is implemented in SCADA test bed and its performance is evaluated with execution of DOS attack. The test is performed for both the scenarios with and without IPS. The average normal traffic volume in network ranges from 60-225 bytes. When DOS UDP scan and Modbus flooding is performed, traffic volume abruptly rises to 1500 bytes targeting 502 port of the PLC and SCADA system lost communication with PLC. Fig. 6 illustrates this attack scenario, shows absence of normal traffic after point of injection of DOS UDP scan. After implementation of IPS, during presence of DOS UDP scan and Modbus flooding the communication between PLC and SCADA is uninterrupted as IPS drops the malicious high-volume traffic from attacker machine. Fig. 7 indicates, the traffic shown in red are the packets discarded by the IPS as it is detected as a malicious load. Traffic in blue ensures the connectivity between PLC and SCADA system in presence of both the DOS attacks.

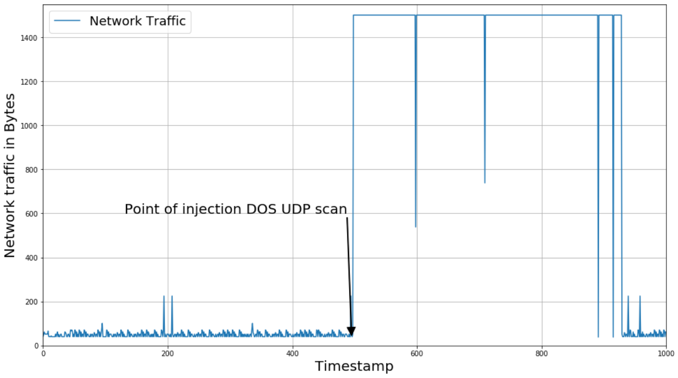

Fig. 6. Network traffic without IPS

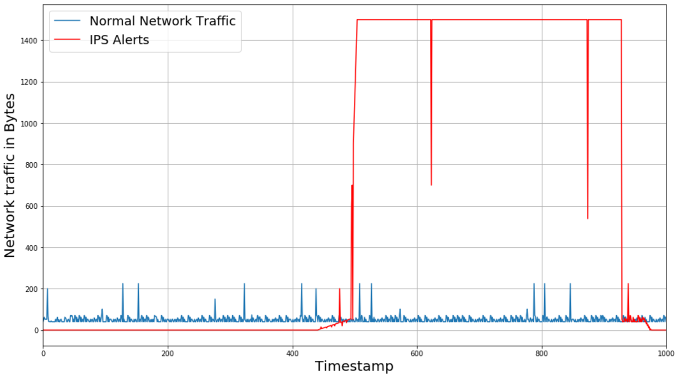

Fig. 7. Network traffic with IPS

From the achieved results, proposed Intrusion Prevention System look promising in preventing intrusion in OT networks. Best results with mentioned accuracies produce by model are obtained after several optimization and analysis and comparing its performance with different machine learning models on same dataset. Model architecture changes with change in network behavior, as detection accuracy depends on type of data, protocols, application and features extracted from dataset.

V. Conclusion

This paper provides background of cyber-attack scenarios in OT networks, design of intrusion prevention system and neural network model design. Data preparation from real SCADA test bed and 9 features mentioned in Table I extracted by DPI Preprocessor are important functionalities of proposed IPS. Along with spoofing false data and command injection, DOS attacks we also implemented malware injection to replicate real cyber-attack scenario in ICS critical infrastructure. Deep neural network model is trained and validated by different evaluation metrics. Proposed intrusion prevention system able to classify binary events with accuracy of 99.89% and 97.95% with multiclass classification and drop the malicious packet before reaching to potential target. The prevention of DOS attack ensures proposed IPS system able to protect SCADA systems in real time.

Inclusion of IPS in real time environment introduces delay in the system. Periodically updating DNN model and its structure is important to keep track of new threats in ICS system. In future by using time series event models, improves effectiveness against cases related to malware activities.

Acknowledgment

We are thankful to Mr. Shahrukh Khan and members of CoE-CNDS lab, VJTI, Mumbai for providing us platform to conduct research on topic ”Design of Intrusion Prevention for OT networks using Deep Neural Network” and for their continuous support during the entire research period.

References

[1] T. Cruz et al., ”A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems,” in IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2236-2246, Dec. 2016.

[2] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain and A. Nawaz, ”HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems,” in IEEE Access, vol. 7, pp. 89507-89521, 2019.

[3] X. L-Novo, M. V-Barbas, V. A. Villagrá and M. Sanz Rodrigo, ”Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies,” in IEEE Access, vol. 8, pp. 9005-9014, 2020.

[4] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, ”Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems,” in IEEE Access, vol. 7, pp. 46595-46620, 2019.

[5] T. Alves, R. Das and T. Morris, ”Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers,” in IEEE Embedded Systems Letters, vol. 10, no. 3, pp. 99-102, Sept. 2018.

[6] S. Ghosh and S. Sampalli, ”A Survey of Security in SCADA Networks: Current Issues and Future Challenges,” in IEEE Access, vol. 7, pp. 135812-135831, 2019.

[7] Li, Dong, et al. ”SCADAWall: A CPI-enabled firewall model for SCADA security.” Computers & Security 80, p. 134-154, 2019.

[8] Selvarajan, Shitharth, et al. ”Mining of intrusion attack in SCADA network using clustering and genetically seeded flora-based optimal classification algorithm.” IET Information Security 14.1, p. 1-11, 2019.

[9] U. Adhikari, T. H. Morris and S. Pan, ”Applying Non-Nested Generalized Exemplars Classification for Cyber-Power Event and Intrusion Detection,” in IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 3928-3941, Sept. 2018.

[10] I. Ullah and Q. H. Mahmoud, ”A hybrid model for anomaly-based intrusion detection in SCADA networks,” 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, pp. 2160-2167, 2017.

[11] J. Tian, R. Tan, X. Guan, Z. Xu and T. Liu, ”Moving Target Defense Approach to Detecting Stuxnet-Like Attacks,” in IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 291-300, Jan. 2020.