Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

Introduction

The importance of Internet and communication networks in our daily life and in any organization's daily operations is well known and cannot be overstressed. A nation's economy is fully reliant on its critical infrastructure. Energy sector is one of the 16 Critical Infrastructure Sectors identified by the Department of Homeland Security (DHS, 2018). Securing these critical infrastructure sectors is challenging but is also of utmost priority in this day of constant and persistent cyber threats. Threat is any circumstance or event that has the potential to adversely impact an agency's assets and operations (CNSS, 2015). Cyber Threat Intelligence (CTI) is the process of collection, analysis, and identification of potential cyber threats to the organization. This goal of current research performed at the Savannah River National Laboratory (SRNL), Aiken, SC, is to develop a Cyber Threat Intelligence framework for gathering Threat Intelligence passively from the network traffic from and to a real or simulated Critical Control Systems.

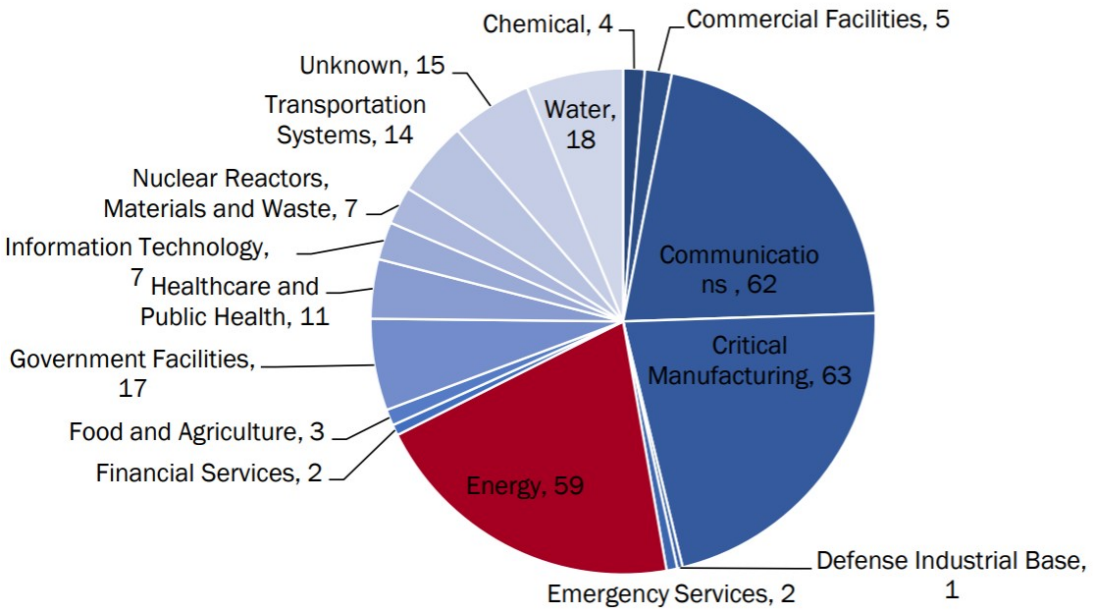
Background

In the age of Internet of Things (IoT), or Industrial Internet of things (IIoT) where all the control systems in industry are well connected to the networks, the concerns for possible cyber attacks to disrupt the critical services are very real. The Cyber Incidents reported in 2016 by Critical Infrastructure Sectors is given in Figure 1 (US DoE, 2017). The consequences of such attacks include disruption to daily life and losses to the nation's economy. It is estimated that the impact on the economy can be anywhere between US $240 billion to $1 trillion depending on the cyber attack scenario (Lloyd's and the University of Cambridge Centre for Risk Studies, 2015). These kinds of scenarios prompted for actions and policies from the federal government such as the Presidential Executive Orders in 2013 for "Improving Critical Infrastructure Cybersecurity", and in 2017 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", and in 2013 the Presidential Policy Directive (PPD)-21 "Critical Infrastructure Security and Resilience".

The existing ICS (Industrial Control Systems) and SCADA (Supervisory Control And Data Acquisition) systems that support our critical infrastructure are facing a growing threat from latest and more sophisticated cyber threats. Most of our country's critical infrastructure including power sector is more than half-a-century old (Solomakhin et al., 2010). Securing these legacy systems demands gathering any needed information passively without hampering their functionality or adding any latency to it.

There have been research studies in the application of machine learning in cyber threat intelligence (Yao et al., 2017; Mamdouh et al., 2018; Zakroum et al., 2018). However, there has been a continuous increased sophistication in the techniques used by the adversaries to go undetected. This results in a gap of our knowledge to identify the new threats and prompts for a cyber threat intelligence framework for a given target system that can enable us to better gather the cyber threat intelligence that is timely, accurate, actionable, and relevant, while not affecting the functionality of these legacy control systems.

Figure 1. Reported Cyber Incidents by Critical Infrastructure Sectors, 2016
(from US DoE, 2017)



Hypotheses and Research Objectives and Goals

Hypothesis: Even though there has been research in application of Machine Learning in Cyber Threat Intelligence, Customizing the process of Cyber Threat Intelligence gathering for a given Critical Infrastructure improves the quality of Threat Intelligence since the Adversaries' behavior and Cyber Threats or Risk to the Assets are based on the target Agency, System, or Assets.

Research Objective(s):

1. Classifying the potential Threats/Attacks in the Network Traffic using Machine Learning Techniques
2. Identifying and Extracting potential Threat Indicators from the network packets

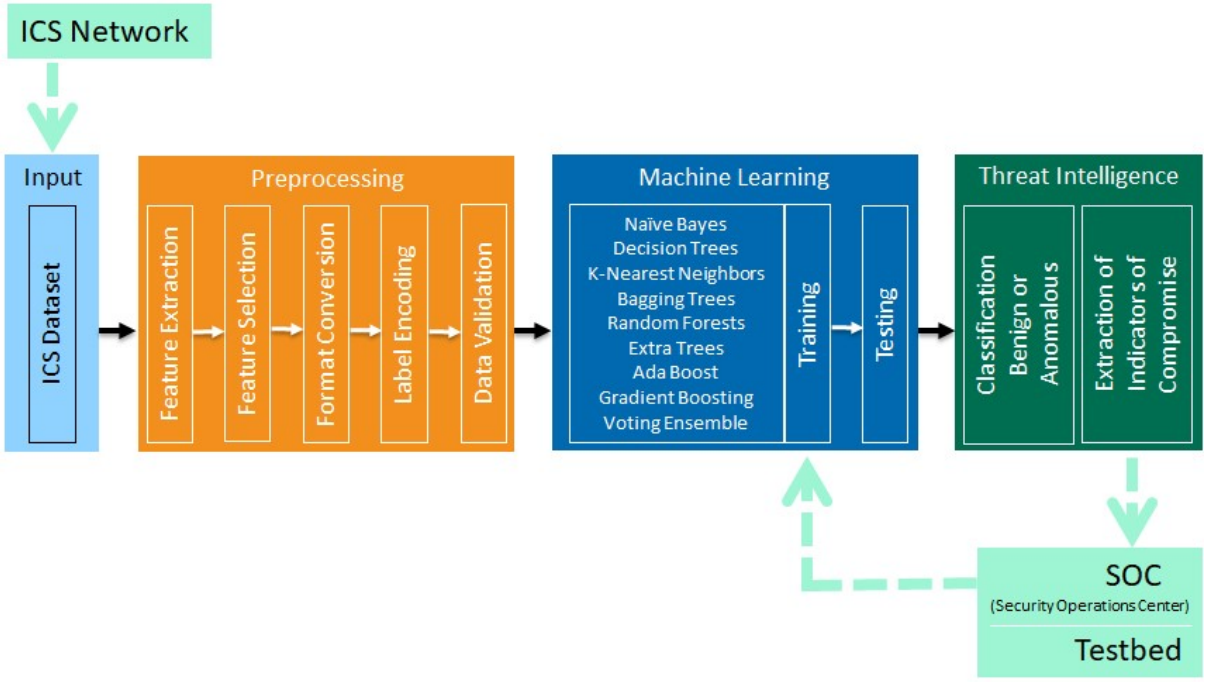
Goal: The goal of the current proposal is to develop a framework that can help provide Reliable, Timely, Actionable, and Relevant Cyber Threat Intelligence to the Incident Response Team or the SOC (Security Operations Center).

Methodology

The Cyber Threat Intelligence Framework

The framework of the system used in this research is given in figure 2. The main components and stages of the framework used consists of the Acquiring the Dataset; Preprocessing: Feature Extraction (1132 features), Feature Selection (84 features), Format Conversion, Label Encoding, and Data Validation; Machine Learning Classification: Training (80% of the dataset) with 10-fold Cross-Validation, and Testing (20% of the dataset); Evaluation using the metrics - Accuracy, Precision, Recall, and F1-score; and extraction of the Indicators of Compromise.

Figure 2. Architecture of the Cyber Threat Intelligence Framework used.



Dataset

The ICS Testbed Dataset used in this research is a subset of a public dataset available from the internet (Frazão et al., 2018). A total of 120025 network packets are used consisting of Benign (Normal Testbed Operation, no simulated attacks) and Anomalous (simulated attacks). The attack types are: Man-in-the-Middle Change attack (MITM_C), Man-in-the-Middle Read attack (MITM_R), Modbus Query Flooding, Ping Flood DDoS, TCP SYN Flooding DDoS.

Preprocessing

The dataset is processed to extract and select the features and format is to be ready for the Machine Learning algorithms for classification.

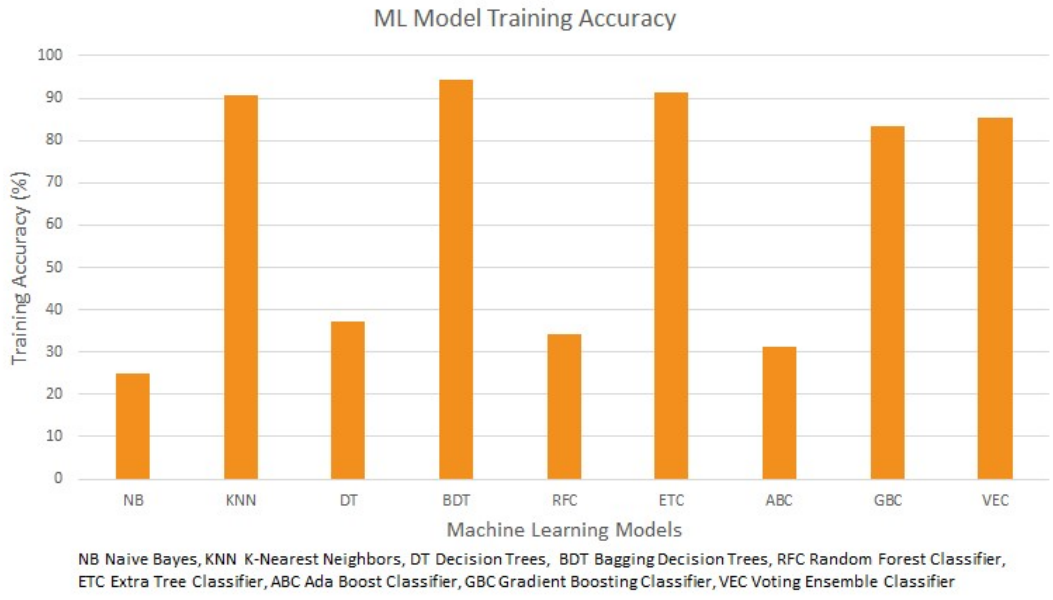
Machine Learning Algorithms

A total of 9 machine learning algorithms are used in this research for the classification of the benign from the attach network traffic. These are: Naïve Bayes (NB), K-Nearest Neighbors (KNN), Decision Trees (DT), and 6 Tree-based Ensemble Strategy algorithms - Bagging Decision Trees (BDT), Random Forest Classifier (RFC), Extra Tree Classifier (ETC), Ada Boost Classifier (ABC), Gradient Boosting Classifier (GBC), Voting Ensemble Classifier (VEC). All the tools needed for preprocessing of the dataset, the machine learning algorithms, and the extraction of the Indicators of Compromise are implemented in Python.

Results

The comparative results of the training of the 9 machine learning algorithms used are given in figure 3.

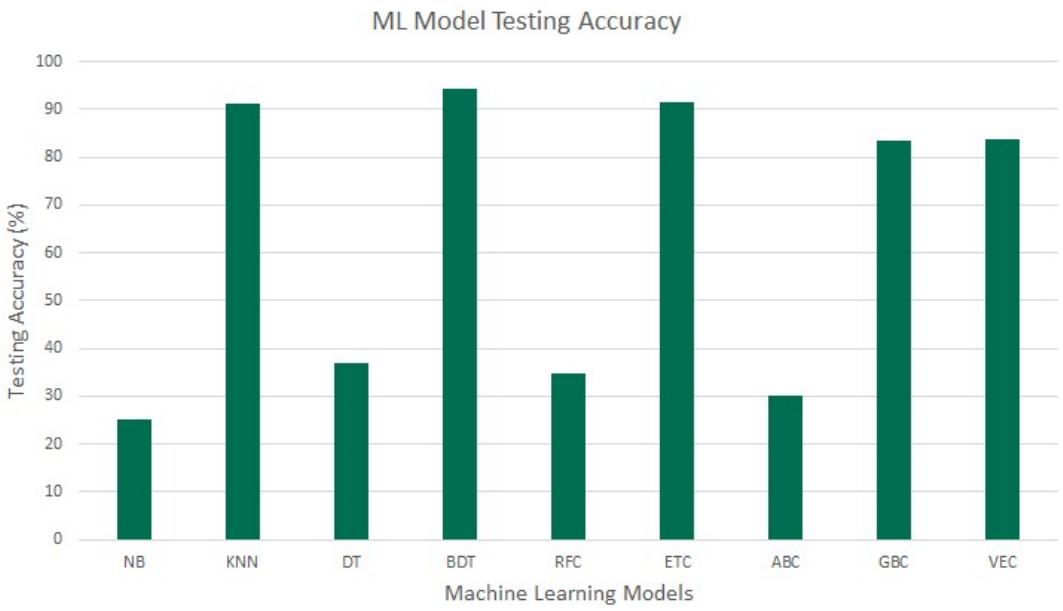
Figure 3. Results of the training of the 9 machine learning algorithms used.



The results show that BDT (Bagging Decision Tree) classifier has the best training followed by KNN (K-Nearest Neighbors), and ETC (Extra Tree Classifier), among the 9 used.

The Testing results of the 9 machine learning algorithms are given in figure 4.

Figure 4. Results of the Testing of the 9 machine learning algorithms used.



NB Naive Bayes, KNN K-Nearest Neighbors, DT Decision Trees, BDT Bagging Decision Trees, RFC Random Forest Classifier, ETC Extra Tree Classifier, ABC Ada Boost Classifier, GBC Gradient Boosting Classifier, VEC Voting Ensemble Classifier

The results show that BDT (Bagging Decision Tree) classifier has the best testing results in the classification of the anomalous network traffic from the benign traffic, followed by KNN (K-Nearest Neighbors), and ETC (Extra Tree Classifier), among the 9 machine learning algorithms used.

Evaluation Metrics

The evaluation metrics of Precision, Recall, and F1-Score are shown in figure 5. The results of the false positives and false negatives by each of the 9 machine learning algorithms used are given in figure 6.

Figure 5. Evaluation metrics of the 9 Machine Learning Algorithms used.

Naive Bayes

CLASS	Precision	Recall	F1-score	Support
1	0.24	0.01	0.03	6006
2	0.26	0.03	0.05	6029
3	0.25	0.95	0.4	6054
4	0	0	0	1959
5	0	0	0	1935
6	0	0	0	2022

K-Nearest Neighbors

CLASS	Precision	Recall	F1-score	Support
1	0.91	0.95	0.93	6006
2	0.92	0.87	0.89	6029
3	0.86	0.9	0.88	6054
4	0.96	0.9	0.93	1959
5	0.98	0.94	0.96	1935
6	0.99	0.94	0.96	2022

Decision Trees

CLASS	Precision	Recall	F1-score	Support
1	1	0.19	0.32	6006
2	0.55	0.1	0.17	6029
3	0.29	1	0.45	6054
4	0	0	0	1959
5	1	0.35	0.52	1935
6	1	0.2	0.33	2022

Bagging Decision Trees

CLASS	Precision	Recall	F1-score	Support
1	0.95	0.93	0.94	6006
2	0.91	0.95	0.93	6029
3	0.92	0.94	0.93	6054
4	1	0.95	0.98	1959
5	1	0.97	0.98	1935
6	1	0.95	0.97	2022

Random Forests

CLASS	Precision	Recall	F1-score	Support
1	1	0.28	0.44	6006
2	0.29	0.93	0.44	6029
3	0.22	0.09	0.13	6054
4	0	0	0	1959
5	0	0	0	1935
6	1	0.23	0.37	2022

Extra Tree Classifier

CLASS	Precision	Recall	F1-score	Support
1	0.95	0.93	0.94	6006
2	0.82	0.92	0.87	6029
3	0.91	0.86	0.89	6054
4	1	0.95	0.97	1959
5	1	0.96	0.98	1935
6	1	0.95	0.97	2022

Ada Boost Classifier

CLASS	Precision	Recall	F1-score	Support
1	1	0.19	0.32	6006
2	0.26	0.93	0.41	6029
3	0.31	0.08	0.13	6054
4	0	0	0	1959
5	0	0	0	1935
6	0	0	0	2022

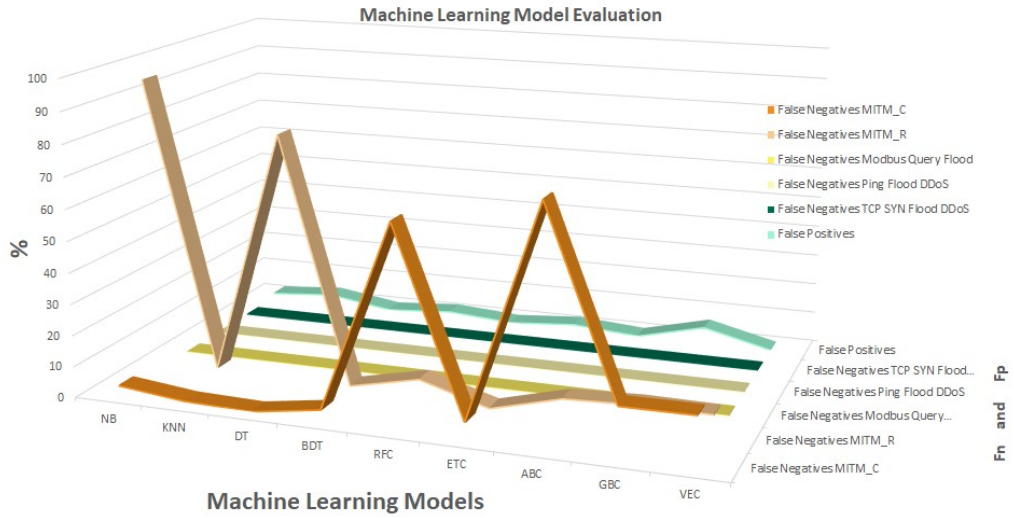
Gradient Boosting Classifier

CLASS	Precision	Recall	F1-score	Support
1	0.82	0.76	0.79	6006
2	0.77	0.90	0.83	6029
3	0.76	0.73	0.75	6054
4	1	0.95	0.97	1959
5	1	0.96	0.98	1935
6	1	0.95	0.97	2022

Voting Ensemble Classifier

CLASS	Precision	Recall	F1-score	Support
1	1	0.76	0.86	6006
2	0.67	0.93	0.78	6029
3	0.79	0.72	0.75	6054
4	1	0.95	0.97	1959
5	1	0.96	0.98	1935
6	1	0.95	0.97	2022

Figure 6. Evaluation metrics showing the number of False Positives and False Negatives for each of the 9 Machine Learning Algorithms used.



The evaluation metrics from figures 5 and 6 show that Decision Trees, Random Forests and Ada Boosting Classifier showed none and Naïve Bayes, Bagging Decision Trees, Extra Trees Classifier showed low False Positives, while K-Nearest Neighbors, Extra Tree Classifier, Bagging Decision Trees showed low False Negatives mainly for the MITM and none for the rest of the attacks.

Extraction of Indicators of Compromise

The Indicators of Compromise (IoC) for the 5 different attacks were extracted. The extracted Indicators of Compromise for the Man-in-the-Middle attack as a sample is given below. These IoCs need to be further evaluated so they can be used for use as a Threat Intelligence in a Security Operation Center.

Indicators of Compromise - MITM READ ATTACK

STP Port Identifier, 0

STP Protocol Identifier, 0

ARP Protocol Type, 0, 2048

IP Total Length, 40, 52, 71, 0, 41, 44, 328, 203, 68, 50, 1023, 48

Frame Length, 60, 66, 85, 64, 342, 86, 62, 90, 838, 146, 217, 1057, 82, 84, 1037, 70, 110

Modbus Function Code, Read Holding Registers, Preset Single Register

ARP Sender MAC address, 00:C2:94:D5:11:60, 00:80:F4:09:51:3B

ARP Sender IP, 0.0.0.0, 10.254.0.194, 172.27.224.250

ARP Target MAC address, 48:5B:39:64:40:79

ARP Target IP, 0.0.0.0, 10.254.0.254, 172.27.224.251

IP Source, 172.27.224.251, 172.27.224.70, 172.27.224.250, 0.0.0.0

IP Destination, 172.27.224.250, 172.27.224.70, 0.0.0.0, 172.27.224.251, 255.255.255.255, 172.27.224.255, 224.0.0.22, 224.0.0.252, 239.255.255.250

IP Protocol, Transmission Control Protocol, IPv6 Hop-by-Hop Option, User Datagram Protocol, Internet Group Management Protocol

TCP Source Port 0, 502, 49201, 49205, 49217, (49922-49935), (49937-50096), (51487-51495), (51497-51514), (51516-51563), (51565-51612), (51614, 51648), (51650-51659), (54935-54965), (54967-55031), (55033-55058), (55060-55106)

TCP Destination Port 0, 502, 49201, 49205, (49922-49939), (49941-49944), (49946-49951), (49953-49959), 49961, (49963-49969), (49971-49974), 49976, (49979-49981), (49983-49986), (49988-50010), (50012-50031), 50033, (50036-50042), (50044-50049), (50051-50057), (50059-50061), (50063-50064), (50066-50075), (50077-50079), (50081-50089), (50092-50096), 50530-51054, (51487-51508), (51510-51512), (51514-51517), 51521-(51523-51524), (51528-51529), 51531, (51533-51536), (51538-51547), (51550-51551), (51553-51563), (51565-51576), (51578-51579), (51584-51586), (51589-51593), 51595-(51597-51598), (51600-51602), (51604-51606), (51608-51611), (51613-51615), (51618-51621), (51623-51626), (51629-51632), (51634-51636), 51638, (51640-51641), 51644, (51646-51649), 51651, (51653-51658), 52024, (54935-54950), (54952-54956), 54958, 54960, (54962-54972), (54974-54975), (54978-54981), (54983, 54987), (54989-54998), (55001-55002), (55004-55006), (55008-55012), (55014-55039), (55041-55047), (55049-55051), (55053-55057), (55059-55064), (55066-55106)

Summary

The Cyber Threat Intelligence Framework that was proposed, developed, and tested shows that it was able to Classify the anomalous from the Benign Network Traffic, Classify the Five different Attacks from each other, achieve >90% accuracy with some Machine Learning algorithms (ETC, KNN) with low False Positives and False Negatives and Extract the Indicators of Compromise for these attacks studied.

References Cited

CNSS, 2015. Committee on National Security Systems Glossary, CNSSI No. 4009, April 16, 2015.

DHS, 2018. Critical Infrastructure Sectors, CISA, https://www.dhs.gov/cisa/critical-infrastructure-sectors, accessed January 3, 2019.

Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf

Frazão, I. and Pedro Henriques Abreu and Tiago Cruz and Araújo, H. and Simões, P., "Denial of Service Attacks: Detecting the frailties of machine learning algorithms in the Classification Process", in 13th International Conference on Critical Information Infrastructures Security (CRITIS 2018), ed. Springer, Kaunas, Lithuania, September 24-26, 2018, Springer series on Security and Cryptology, 2018.

Lloyd's and the University of Cambridge Centre for Risk Studies, 2015. The insurance implications of a cyber attack on the US power grid, Emerging Risk Report – 2015, pages 65.

Mamdouh, M., Elrukhsi, M., and Khattab, A., 2018. Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey, 2018 International Conference on Computer and Applications (ICCA), Pages 215-218.

Solomakhin, R., Tsang, P., and Smith, S., 2010. High Security with Low Latency in Legacy Scada Systems, Chapter 3 in T. Moore and S. Shenoi (Eds.): Critical Infrastructure Protection IV, IFIP AICT 342, pp. 63–79, 2010.

US DoE, 2017. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities, https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf (accessed December 2018) from National Cybersecurity and Communications Integration Center, Industrial Control Systems Cyber Emergency Response Team, "FY 2016 Incidents," https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf.

Yao, D., Shu, X., Cheng, L., Stolfo, S., Bertino, E., and Sandhu, R., 2017. Anomaly Detection as a Service: Challenges, Advances, and Opportunities, Morgan and Claypool eBooks.

Zakroum, M., Houmz, A., Ghogho, M., Mezzour, G., Lahmadi, A., FranÇois, J., and Koutbi, M., 2018. Exploratory Data Analysis of a Network Telescope Traffic and Prediction of Port Probing Rates, November 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL., pages 175-180.

-~~-