Univariate and Bivariate Entropy Analysis for Modbus Traffic over TCP/IP in Industrial Control Systems

Tirthankar Ghosh*, Sikha Bagui*, Subhash Bagui*, Martin Kadzis*,
Logan Day*, and Jackson Bare*
University of West Florida[†], Pensacola, FLORIDA

Abstract

Anomalies in network traffic are usually detected by measuring unexpected deviation from what constitutes a baseline. Several statistical techniques have been proposed to create baselines and measure deviation. However, simply looking at traffic volume to find anomalous deviation may result in increased false positives. Traffic feature distributions need to be created, and deviations need to be measured for these features. An effective approach to finding anomalous deviations starts with entropy analysis on these features. This paper presents an entropy analysis on an industrial control system network using selected features with datasets obtained from an HVAC system. The paper starts with a fundamental question: whether preliminary entropy analysis on Modbus-over-TCP data using only a few TCP/IP features, without going into Modbus traffic, gives information about an anomaly in the network. Relative entropy was computed using Kullback-Leibler divergence to study deviation of malicious traffic from non-malicious. To gain further insight on detecting anomalies within the ICS traffic, the work was extended to bivariate joint entropy analysis using pairs of features. Initial analysis of the bivariate joint entropy also showed some promising results, but as in the univariate analysis, the bivariate joint entropy analysis showed that none of the feature pairs indicated a presence of reconnaissance[†].

Keywords: Industrial control systems security, modbus traffic analysis, entropy analysis.

1 Introduction

Industrial Control Systems (ICS) are networks of devices used in critical infrastructure and industrial environments for control of physical processes. These networks typically span a large geographic area, and some examples of such systems are water distribution systems, gas pipelines, and power transmission systems. An ICS can be a large multifaceted infrastructure like a Supervisory Control and Data Acquisition (SCADA) system, which collects data and processes it in a centralized environment where it can be viewed and interacted with. There are simpler configurations of industrial control systems that are more readily available to any system with lesser changes to an already established system. Programmable Logic Controllers (PLC) are widely used in the area of automation and come equipped with programmable memory, various input and output channels, and communication interfaces that make them incredibly valuable.

Industrial Control Systems are fundamentally different from traditional Information Technology (IT) systems. Because ICSs provide an interface with physical devices like sensors and actuators, they are generally categorized as Operational Technology (OT). Updates and patching play a pivotal role in the differences in maintainability between IT and OT systems (Cardenas [6]). An ICS requires real-time availability for their systems to communicate and function, implying that they must be able to identify, diagnose, and respond appropriately to irregular flow of information as quickly as they appear. This necessitates that updates and patching happen as frequently as possible, making them as less vulnerable as possible to potential attacks. While this is a drawback that is difficult to circumvent, the design of an intrusion detection system may be simpler for ICS because of their static nature and predictability in communication.

Intrusion Detection and Prevention Systems (IDPS) are designed and deployed to monitor traditional IT systems for signs of undesirable and malicious behavior. A common way to secure a traditional system is to deploy an IDPS to monitor and identify anomalies that take automated action or warrant future investigation. There are two broad classifications of IDPS based on their detection technique misuse detection or signature-based, and anomaly detection or behavior-based (Angséus & Ekbom [3]). Signature-based systems are not very effective in ICS environments where very few known signatures are encountered. An effective way to identify communication anomaly in an ICS is to consider the minimal and maximal values in a given feature within the system and have precautionary measures in place that can react to values that defy the provided range (Angséus & Ekbom [3]). In other words, measuring the change in entropy or randomness in the communication pattern of an industrial control system is beneficial in detecting a problem.

There are four levels in a SCADA architecture that need to be secured to ensure a stable environment (Koucham [13]). The lowermost level, or the basic control level, generally consists of sensors and actuators that collect and send information to the upper levels. These machines are found at field sites with Remote Terminal Units. Above the basic control is the

*Email: tghosh@uwf.edu, bagui@uwf.edu, sbagui@uwf.edu, mjk34@students.uwf.edu, ldd14@students.uwf.edu, and cjb86@students.uwf.edu

[†] This work is partially supported by the Office of Naval Research (ONR) under grant number N00014-21-1-2025.

supervisory control level consisting of Distributed Control Systems (DCS) servers and PLCs which are accompanied by the Human Machine Interface (HMI) and engineering stations. This level focuses on the global view of the system's control state and operations and collects the information relayed from the first level for analysis. This information is also presented through the HMI to make it more easily accessible to a user reviewing the system's nodes and features. The engineering workstations allow the specification of setpoints and the programming of controllers, which allows for boundaries to be manipulated. The two uppermost levels are commonly grouped together as the "backbone network" and contain servers that are connected to the enterprise IT systems backbone. This level has a variety of purposes, which can most broadly be classified as the allocation and optimization of resources, maintenance, planning, and quality control. Data collected previously is housed within this level in database servers (Koucham [13]).

Communication characteristics in an ICS setting are also quite different from traditional TCP/IP communication. Sensors and actuators generate a low volume of data that is periodic with short transfer time and low delay (Koucham [13]). The controllers that accompany these nodes use a communication protocol like Modbus (Koucham, [13]), which is an application protocol that defines the syntax and semantics of the communication and structure. The Protocol Data Unit (PDU) is seven bytes long and consists of the transaction identifier, protocol identifier, length, and unit identifier. Figure 1 shows the Modbus frame and its encapsulation in the TCP header. The transaction identifier is used for transaction pairing when multiple messages are sent and make up two of the seven bytes. The protocol identifier also makes up two bytes and is either empty or padded with zeros to be used for future extensions. The unit identifier is one byte and identifies a remote server located on a non TCP/IP network, and the length is the byte count of the remaining fields. Modbus is open source making it the most widely used protocol in ICS environments (Koucham [13]).

In the Supervisory Level, a much higher volume of data is collected than sensors and actuators, and transfer time is restricted to a lesser extent. This level is also much more representative of a traditional IT system, and therefore can be treated as such. Network protocols like OPC DA and OPC UA are commonly utilized in this level, as they cover data access and client/server technology which are important to enable human interaction with the system and the data collected (Koucham [13]).

Although, because of their static nature and predictability in communication, securing industrial control systems may seem trivial at first, but there are several challenges that arise because of these very characteristics. We previously mentioned that having periodic system update is often a challenge in ICS environments, and real-time communication poses a challenge for deploying a security solution that adds latency. In addition, because of the operational technology requirements of ICS, physical interaction with the sensors and actuators poses a challenge to secure the system as a whole. Any intrusion detection and prevention systems that need to be designed for these environments must take into account the need for real-time data transfer and must be aware of stringent latency requirements. Hence, adding detection techniques that are resource-intensive may not be the most efficient approach in these ICS environments.

This paper discusses a univariate and bivariate joint entropy analysis on ICS Modbus over TCP/IP data and an analysis of relative entropy using Kullback-Leibler divergence.

1.1 Entropy

Entropy represents the amount of uncertainty that exists in a random variable X. Suppose the random variable X takes on

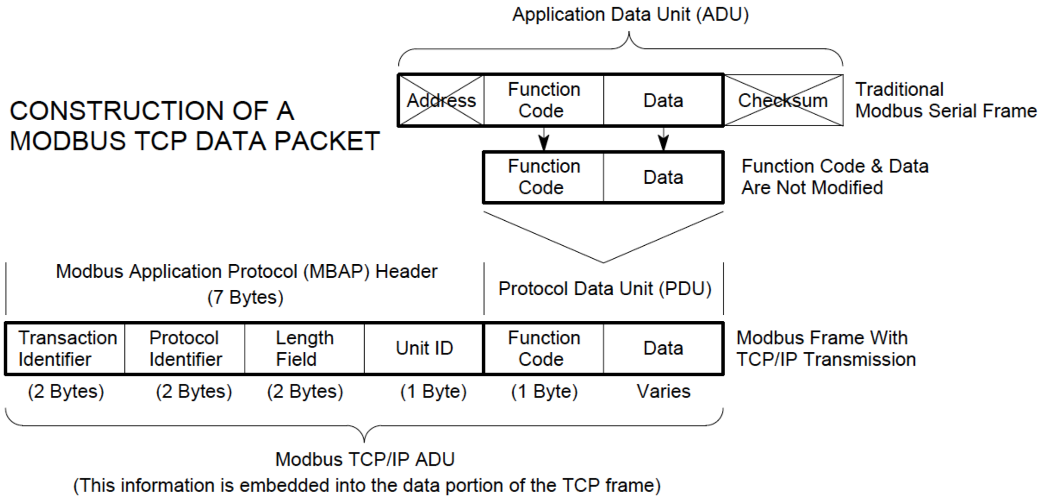

Application Data Unit (ADU)
CONSTRUCTION OF A MODBUS TCP DATA PACKET
Address
Function Code
Data
Checksum
Traditional Modbus Serial Frame
Function Code
Data
Function Code & Data Are Not Modified
Modbus Application Protocol (MBAP) Header (7 Bytes)
Protocol Data Unit (PDU)
Transaction Identifier
Protocol Identifier
Length Field
Unit ID
Function Code
Data
Modbus Frame With TCP/IP Transmission
(2 Bytes)
(2 Bytes)
(2 Bytes)
(1 Byte)
(1 Byte)
Varies
Modbus TCP/IP ADU
(This information is embedded into the data portion of the TCP frame)

Figure 1: Modbus frame[1]

[1] Acromag Modbus TCP/IP Technical Reference.

values $x_1, x_2, \cdots, x_n$ with respective probabilities $p(x_1), p(x_2), \cdots, p(x_n)$, then the entropy of the random variable X is given by

$$E(X) = -\sum_{i=1}^{n} p(x_i)\log p(x_i)$$

which is equivalent to

$$E(X) = \sum_{i=1}^{n} p(x_i)\log(1/p(x_i))$$

where, $E(X)$ is the entropy value for the selected feature X, $p(x_i)$ is the probability that the feature X takes the value x_i. The quantity $-\log p(x_i)$ represents the surprise evoked if X takes on the value x_i. Thus, the expected amount of surprise after learning X is known as the entropy of the random variable X.

Looking at entropy values of a certain traffic feature over a period of time will provide a basis for possible anomalous deviation. However, if traffic features are analyzed independently and their entropy computed, it may not reflect an anomalous behavior and will lead to high false positives. In that respect, relative entropy analysis needs to be conducted. Relative entropy is computed as below:

$$D(p\,||\,q) = \sum_{i=1}^{n} p(x_i)\log(p(x_i)/q(x_i))$$

which shows the relative entropy or deviation of the probability distribution $p(x)$ from the probability distribution $q(x)$. $D(p\,||\,q)$ is called a measure of Kullback-Leibler divergence. The probability $q(x)$ is the probability distribution of non-malicious traffic and $p(x)$ is the probability distribution of malicious traffic.

1.2 Joint Entropy

Consider now two random variables X and Y, which take on respective values $x_1, x_2, \cdots, x_m$ and $y_1, y_2, \cdots, y_n$ with joint probability mass function

$$P(X = x_i, Y = y_j) = p(x_i, y_j) = p_{ij}\ ,$$
$$i = 1,\mathrm{L}\ ,m;\ \ j = 1,\mathrm{L}\ ,n.$$

The joint entropy of the random vector (X,Y), may be denoted by $E(X,Y)$, is given by

$$E(X,Y) = -\sum_{i=1}^{m}\sum_{j=1}^{n} p_{ij}\log p_{ij}\ .$$

The joint entropy $E(X,Y)$ represents the amount of uncertainty that exists in the random vector (X,Y).

As above, the relative entropy in joint probability distribution cases is defined as

$$D(\mathbf{p}\,||\,\mathbf{q}) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_{ij}\log(p_{ij}/q_{ij})$$

where $\mathbf{p} = \{p_{ij} : i = 1,\cdots,m;\ j = 1,\cdots,n\}$ could be the joint probability distribution of malicious traffic and $\mathbf{q} = \{q_{ij} : i = 1,\mathrm{L}\ ,m;\ j = 1,\mathrm{L}\ ,n\}$ could be the joint probability distribution of non-malicious traffic. $D(\mathbf{p}\,||\,\mathbf{q})$ is viewed as a measure of divergence.

2 Related Literature

Supervised learning techniques have been proposed by many to detect malicious traffic in industrial control systems networks. In (Eigner [10]), the authors presented a prototype implementation of an anomaly-detection approach based on Naive Bayes. They ran simulated attacks - Denial of Service (DOS) and Man-in-the-Middle (MITM) - and did a preliminary analysis using the Bayesian classifier. The results were preliminary, and did not justify why and how a Bayesian classifier will be the most appropriate for an ICS network. In (Anthi [1]), the authors used a supervised learning approach to detect attacks. Their proposed attack detection system not only detects malicious packets but also classifies them as specific attack types. A limited number of features from the Modbus data was selected for classification. In (Goh [12]), the authors proposed to use Long Short-Term Memory Recurrent Neural Network (LSTM-RNN) to detect a sequence of patterns for anomaly detection. It was used as a predictor to model normal behavior and then the cumulative sum method was used to identify malicious behavior. The authors tested the approach with data from only one process, limiting its scope and applicability. In (Valdes [16]), the authors used pattern-based and flow-based anomaly detection techniques to identify malicious communications. The pattern-based approach used patterns of communicating hosts to identify normal communication, whereas the flow-based approach used network flow to identify traffic patterns. These approaches typically work well in ICS environments as process related communications are static and predictable; however, they sometimes tend to be resource intensive as the network scales up. In (Feng, [11]), the authors proposed a two-stage anomaly detection technique using a packet level signature analysis and a time-series analysis using Long Short Term Memory Neural Network (LSTM -NN). In the signature analysis stage, a signature database for normal behavior was constructed using communication patterns among devices. The database was then passed through a Bloom filter to detect anomalous behavior. The time series analysis involved using LSTM-NN to learn the most likely package signatures from previously seen network packages. The authors used a SCADA dataset obtained from a gas pipeline to test their proposed technique. In (Caselli, [7]), the authors proposed a sequence-aware intrusion detection system that relied on pattern identification of ICS network events, extraction of semantic meanings, and modeling known behaviors over time. They used discrete time Markov chains to describe several ICS-specific operations and proposed a detection mechanism based on the computation of weighted distance among Markov chain states. In (Yang [17]), the authors proposed an anomaly detection technique using the auto-associative kernel regression model and statistical probability ratio test and applied the technique on a simulated SCADA network.

Not much work has been done using unsupervised learning to isolate malicious from non-malicious traffic. One persistent problem that remains is threshold selection. In (Almalawi [2]), the authors proposed an approach called global anomaly threshold to unsupervised detection (GATUD) that is used as an add-on component to improve the accuracy of unsupervised intrusion detection techniques. They used K-means clustering to initially learn two labeled small datasets from the unlabeled data; each dataset represents either normal or abnormal behavior. Then, a set of supervised classifiers were trained to produce an ensemble-based decision-making model that can be integrated into both unsupervised anomaly scoring, and clustering-based intrusion detection approaches to find a global and efficient anomaly threshold.

The work that came close to our proposed approach is in (Berezinski [4]). The authors proposed an entropy-based network anomaly detector, abbreviated as ANODE, to detect anomalies from network traffic capture. Although the proposed work was not ICS-specific, it provides a very good overall analysis on using entropy for detecting anomalous behavior and is the main motivation behind our approach.

Our paper presents univariate, relative, and bivariate joint entropy analysis on selected features using datasets obtained from an HVAC system. Initial findings from our analysis were reported in (Day [8]). As ICS sensors and actuators are resource constrained, and the OT system itself needs more real time monitoring and response, a computation intensive intrusion and attack detection method may not be suitable. We start from a fundamental question: whether entropy analysis on Modbus-over-TCP data using selected TCP/IP features, without going into Modbus traffic, gives information about an anomaly in the network. In the following sections, univariate entropy analysis and univariate relative entropy using Kullback-Leibler divergence are discussed and results are presented from our initial analysis of the data. Following that, bivariate joint entropy analysis is discussed and results are also presented from our bivariate joint entropy analysis.

3 Entropy Analysis for Modbus Over TCP/IP

3.1 Univariate Entropy Analysis

For the univariate entropy analysis, we based our analysis on a day's worth of Modbus over TCP/IP data collected from an HVAC system at the University of Alabama Huntsville research lab. The data had both malicious and non-malicious traffic representing various stages of the HVAC operations (auto cool, auto heat, normal, and random). Of the various attacks that were simulated, we chose the top three that have been discussed in the literature, namely, Denial of Service (DOS), Man-in-the-middle (MITM), and Reconnaissance.

One of the important considerations in any anomaly detection technique is feature selection. We based our preliminary analysis on only TCP/IP data with the simple objective of answering a fundamental question: whether preliminary entropy analysis on Modbus-over-TCP data using only few TCP/IP features gives us any information about an anomaly in the network. To deduce what features would be relevant in our initial entropy analysis, a correlation matrix was run against the TCP/IP data. The correlation matrix is presented in Table 1.

Three features packet size, inter-packet delay, and packet process time were chosen as they had the most significant

Table 1: Correlation matrix between features

	Packet Size	Inter-Packet Delay	Packet Process Time	Protocol Overhead	Protocol Efficiency	Throughput
Packet Size	1.00	-0.03	-0.44	-0.95	0.95	0.19
IP Delay	-0.03	1.00	0.07	0.02	-0.02	-0.01
PP Time	-0.44	0.07	1.00	0.23	-0.23	-0.04
Protocol Overhead	-0.95	0.02	0.23	1.00	-1.00	-0.20
Protocol Efficiency	0.95	-0.02	-0.23	-1.00	1.00	0.20
Throughput	0.19	-0.01	-0.04	-0.20	0.20	1.00

differences in their relationships with one another. Shannon's entropy, which is a direct measure of the bits needed to store the data in a given variable, was used for entropy computation for each feature for both non-malicious and malicious traffic (DDOS, MITM, and Recon). Table 2 summarizes the results. All three features inter-packet delay, packet process time, and packet size have higher entropy values under Denial of Service (DOS) and Man-In-The-Middle (MITM) attacks. Reconnaissance did not have much impact on entropy for packet size and packet process time but has a small increase for the inter-packet delay. This can be explained by the nature of reconnaissance, where probes are sent with a varying time lag. From Table 2, it can be seen that entropy can be a potential indicator to alert the system of some anomaly, although it will require further investigation to detect the actual nature of the anomaly as such.

3.2 Relative Entropy and Kullback-Leibler Divergence

One persistent question in anomaly detection is how much deviation or change is acceptable. To investigate that, we used relative entropy, or Kullback-Leibler divergence, which is a measure of the deviation of one probability distribution from another and is reflective of a realistic threshold that needs to be set to indicate an anomaly in network traffic. We used Kullback-Leibler divergence to measure deviation of malicious traffic distribution from non-malicious traffic distribution. Before analysis, however, it is important to note that these entropy levels are impacted by the volume of the attack; 45.3%, or nearly half, of the data, was of the attack type MITM, or Man in the Middle; Reconnaissance attacks made up 1.2% of the data; and DOS, or Denial-Of-Service attacks, made up 2.1% of the data. Table 3 summarizes the results from the Kullback-Leibler divergence computation. Divergence was computed for each of the malicious traffic categories from non-malicious traffic. Man-In-The-Middle (MITM) attacks had the largest divergence from non-malicious traffic, especially for packet size. This is not unusual given the nature of MITM attacks and the goals they want to accomplish. Reconnaissance traffic had the lowest divergence, which can be because of the very low volume of reconnaissance traffic within the sample (1.2%). DOS attacks had a similar effect on the system as MITM, however divergence for inter-packet delay was much less compared to the other two features. This could be a result of how DOS attacks flood a system and increase packet process times significantly.

It can be inferred from the results that attacks like MITM and DOS can be detected initially by looking at the entropy values of selected features. In contrast, reconnaissance may be

Table 2: Entropy values for three selected features against three attack types

	Packet Size	Inter-Packet Delay	Packet Process Time
Normal	1.987	2.332	2.957
Normal + MITM	2.173	2.488	3.006
Normal + Recon	1.987	2.393	2.957
Normal + DOS	2.066	2.891	3.008

Table 3: Relative entropy using Kullback-Leibler divergence

	MITM	Recon	DOS
Packet Size KL Divergence	3.176	0	0.952
Inter-Packet Delay KL Divergence	0.949	0.157	0.139
Packet Process Time KL Divergence	0.731	0	0.663

undetectable by initial entropy analysis. However, a more intricate joint entropy may be effective in detecting reconnaissance in the network, hence bivariate joint entropy analysis is done next. It is important to note that the percentage of each attack in the total flow of recorded traffic plays a significant role in the change of entropy; the more infected traffic within the data, the more likely it is to notice changes compared to non-malicious traffic regardless of what attack is being studied.

3.3 Bivariate Joint Entropy Analysis

To gain further insight on detecting anomalies within the ICS traffic, bivariate joint entropy analysis was computed using pairs of features. Bivariate joint entropy was computed for each pair of attributes: packet size, inter-packet delay and packet process time, for non-malicious traffic, malicious traffic, non-malicious + MITM, non-malicious + Recon and non-malicious + DOS. Further, instead of focusing on just a single day's worth of data, this analysis was extended to include eight days' worth of data. Tables 4 and 5 show 8-day average entropy and standard deviation values for each feature pair for non-malicious and malicious traffic, respectively. Results show that bivariate joint entropy analysis with packet process time and inter-packet delay can indicate presence of malicious activities, while the other feature pairs do not convincingly point towards that direction.

Table 4: Entropy averages and standard deviation for each pair of selected features for non-malicious traffic

	PS + IPD	PS + PPT	IPD + PPT
Average Entropy	4.705	4.609	4.839
Standard Deviation	0.063	0.090	0.087

Table 5: Entropy averages and standard deviation for each pair of selected features for malicious traffic

	PS + IPD	PS + PPT	IPD + PPT
Average Entropy	4.425	4.292	5.274
Standard Deviation	0.128	0.194	0.109

Breaking down the analysis into individual attack types, Table 6 shows 8-day average entropy and standard deviation values for each feature pair for non-malicious+MITM traffic. Comparing the results with the values for non-malicious traffic shown in Table 4, it can be inferred that bivariate joint entropy with any two of the selected features can convincingly indicate presence of man-in-the-middle attack in the network. Table 7 shows results for non-malicious+DOS traffic, indicating that bivariate joint entropy with packet size and inter-packet delay as well as with inter-packet delay and packet process time have some indication of denial-of-service attack, while bivariate joint entropy with packet size and packet process time does not indicate any such anomalous activity. Table 8 shows eight days average entropy and standard deviation values for each feature pair for non-malicious+recon traffic. Compared to non-malicious traffic in Table 4, it can be inferred that none of the feature pairs indicates presence of reconnaissance. This confirms with our analysis with univariate entropy computation presented earlier.

Table 6: Entropy averages and standard deviation for each pair of selected features for non-malicious+MITM traffic

	PS + IPD	PS + PPT	IPD + PPT
Average Entropy	4.930	4.847	5.041
Standard Deviation	0.066	0.104	0.083

Table 7: Entropy averages and standard deviation for each pair of selected features for non-malicious+DOS traffic

	PS + IPD	PS + PPT	IPD + PPT
Average Entropy	4.776	4.597	4.897
Standard Deviation	0.065	0.095	0.094

Table 8: Entropy averages and standard deviation for each pair of selected features for non-malicious+recon traffic

	PS + IPD	PS + PPT	IPD + PPT
Average Entropy	4.700	4.598	4.846
Standard Deviation	0.064	0.092	0.091

4 Conclusion and Future Directions

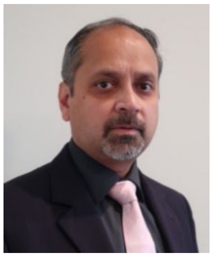
We presented an initial entropy analysis on an industrial control system network using selected features with datasets obtained from an HVAC system. We acknowledge that the initial entropy analysis only provides a starting point in asking several questions and investigating relevant issues that will lead to optimal system design and implementation. We started from the fundamental question: whether a preliminary univariate entropy analysis on Modbus-over-TCP data using only a few TCP/IP features, without going into Modbus traffic, gives us information about an anomaly in the network. For the univariate entropy analysis, we based our work on a day's worth of Modbus over TCP/IP data collected from an HVAC system at the University of Alabama Huntsville research lab. The data had both malicious and non-malicious traffic representing various stages of the HVAC operations (auto cool, auto heat, normal, and random). Of the various attacks that were simulated, we chose the top three that have been discussed in the literature, namely, Denial of Service (DOS), Man-in-the-Middle (MITM), and Reconnaissance. We also used Kullback-Leibler divergence to measure the univariate relative entropy of selected features over non-malicious traffic for each of the malicious activities. Initial analysis showed some promising results using univariate entropy and divergence. To gain further insight on detecting anomalies within the ICS traffic, we extended our work to bivariate joint entropy analysis using pairs of features with more data extending it to eight days-worth of traffic data. Initial analysis of bivariate joint entropy also showed some promising results, but as in the univariate analysis, none of the feature pairs indicated a presence of reconnaissance.

However, there are several questions that need to be addressed as below.

1. Do these entropy and divergence values give us a realistic threshold for anomaly detection? These need to be analyzed with more days' worth of data.
2. Does the percentage of malicious traffic have a causal effect on the entropy values? These would also need to be analyzed with more data and more malicious traffic.
3. What would be the entropy values for the ModBus traffic features? Do those features give us a more holistic view of an anomaly in the network traffic?
4. Would multivariate joint entropies with both Modbus and TCP/IP features give us a better understanding of network anomaly? A multivariate analysis with more features would be needed to answer this question.

References

1. E. Anthi, L. Williams, P. Burnap, and K. Jones, "A Three-Tiered Intrusion Detection System for Industrial Control Systems," *Journal of Cybersecurity,* 7(1):1-10,2021, doi:10.1093/ cybsec/tyab006, 2021.
2. A. Almalawi, A. Fahad, Z. Tari, A. I. Khan, N. Alzahrani, and AS. T. Bakhsh, and S. Qaiyum, "Add-On Anomaly Threshold Technique for Improving Unsupervised Intrusion Detection on SCADA Data," *Electronics,* 9(6):2-20, 1017. doi:10.3390/electronics9061017, 1017.
3. J. Angseus and R. Ekbom, *Network-Based Intrusion Detection Systems for Industrial Control Systems,* Master's Thesis, in Computer Science, Chalmers University of Technology, Gothenburg, Sweden, 2017.
4. P. Bereziński, B. Jasiul, and M. Szpyrka, "An Entropy-Based Network Anomaly Detection Method," *Entropy,* 17(4):2367-2408. doi:10.3390/e17042367, 2015.
5. S. Caltagirone, "Industrial Control Threat Intelligence," *Dragos*, 2018.
6. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for Securing Cyber Physical Systems." *Proc. of Workshop in Cyber Physical Systems*, pp. 9-25, July 23, 2009.
7. M. Caselli, E. Zambon, and F. Kargl, Sequence-aware Intrusion Detection in Industrial Control Systems, *Proc. of the 1st ACM Workshop on Cyber-Physical System Security,* ACM, pp. 13-24, 2015
8. L. Day, T. Ghosh, S. Bagui, and S. Bagui, "Entropy Analysis for Modbus Traffic over TCP/IP in Industrial Control Systems," *Proc. of Computer and its Applications Conference* 2022, CATA'22, pp. 63-71, 2022
9. Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of Attacks on Industrial Control Protocols" *NTDS*, doi:10.1109/NOTERE.2015. 7293513, 2015
10. O. Eigner, P. Kreimel, and P. Tavolato, "Attacks on Industrial Control Systems - Modeling and Anomaly Detection." *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pp. 581-588, 2018, doi:10.5220/000675540 5810588, 2018.
11. C. Feng, T. Li, and D. Chana, "Multi-Level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks," *Proc. IEEE Int. Conf. Depend. Syst. Network*, pp. 261-272, 2017
12. J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks," 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), doi:10.1109/hase.2017.36, 2017.
13. O. Koucham, "Intrusion Detection for Industrial Control Systems," *Universite Grenoble Aples*. Doi:tel-02108208, 2018.
14. Q. Lin, S. Verwer, R. Kooji, and A. Mathur, "Using Datasets from Industrial Control Systems for Cyber Security Research and Education," *Proc. of the 14th International Conference on Critical Information Infrastructures Security CRITIS*, Linköping, Sweden, pp. 122-133, 23-25 September, 2019.
15. T. Morris and W. Gao, "Industrial Control System Traffic Data Sets for Intrusion Detection Research," doi:10.1007/978-3-662-45355-1_5.
16. A. Valdes and S. Cheung, S. (2009). "Communication Pattern Anomaly Detection in Process Control Systems," *2009 IEEE Conference on Technologies for Homeland Security*. doi:10.1109/ths.2009.5168010, 2009.
17. D. Yang, A. Usynin, and J. Hines, "Anomaly-Based Intrusion Detection for SCADA Systems," *Proc. of the 5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology*, Albuquerque, NM, USA, pp. 12-16, 2006.



Tirthankar Ghosh is Professor and Associate Chair in the Department of Computer Science at UWF. He has over seventeen years of experience in cybersecurity education and research in network security, ICS security, anomaly detection and adversary TTPs, and threat intelligence. Dr. Ghosh has received numerous grants from federal and state agencies. He was the co-founder of a state-wide consortium in Minnesota and a regional cybersecurity consortium in St. Cloud. Dr. Ghosh authored a book titled "Security by Practice: Exercises in Network Security and Information Assurance", and several journal papers and book chapters. He serves as an ABET evaluator for Cybersecurity and Computer Science.

Sikha Bagui is Distinguished University Professor and Askew Fellow in the Department of Computer Science, at The University West Florida, Pensacola, Florida. Dr. Bagui is active in publishing peer reviewed journal articles in the areas of database design, data mining, Big Data analytics, machine learning and AI. Dr. Bagui has worked on funded as well unfunded research projects and has 100+ peer reviewed publications, some in highly selected journals and conferences. She has also co-authored several books on database and SQL. Bagui also serves as Associate Editor and is on the editorial board of several journals.

Subhash C. Bagui received his B.Sc. in Statistics from University of Calcutta, M. Stat. from Indian Statistical Institute and Ph.D. from University of Alberta, Canada. He is currently a University Distinguished Professor at the University of West Florida. He has authored a book titled, "Handbook of Percentiles of Non -Central t-Distribution", and published many high quality peer reviewed journal articles. He is currently serving as associate editors/ editorial board members of several statistics journals. His research interests include nonparametric classification and clustering, statistical pattern recognition, machine learning, central limit theorem, and experimental designs. He is also a fellow of American Statistical Association (ASA) and Royal Statistical Society (RSS).

Martin Kadzis (photo not available) is a graduate student of Computer Science at the University of West Florida. He is a recipient of CyberCorps: Scholarship for Service at UWF.

Logan Day (photo not available) is a senior in the Software Development/Computer Science major at the University of West Florida. He is a ROTC cadet at UWF.

Jackson Bare is a senior Cybersecurity major at the University of West Florida (UWF). Mr. Bare has participated in several research projects ranging from the use of drones to achieve political objectives to comparing different methods of growing kale to Industrial Control System entropy analysis. Mr. Bare has presented at the National Center for Undergraduate Research Symposium and the UWF Research Symposium. He is a CyberCorps: Scholarship for Service recipient at UWF.