Investigations of Estimates of the Network Traffic Entropy of the IIoT for the Purpose of Early Attack Detection

A.V. Sergeichev

National Research University "Higher School of Economics", Moscow, Russia

***Abstract* — The research explores the correlation between the occurrence of an attack and changes in the entropy properties of network traffic. The input data represents a sample of the network communication activity of the IIoT control system, and the attacks that have been realize on it. Network traffic is filtered from service information and digitized by frequency analysis of the content of each recorded packet. This process allows to save the key properties of the traffic. The data is being aggregated by the cumulative function. Then samples can be calculated according to the principle of a sliding window. The window shifts with a set time step, which supports with dynamic monitor changes in network traffic and identify potential threats in real time. Each sample represents a divergence of the distributions. There is no anomaly in traffic if the difference in the distributions is close to zero. The sensitivity of the algorithm to anomaly detection depends on the choice of parameters such as the length of the aggregation time interval, the sliding window dimension, and the offset step. It is expected that the obtained measures of dependence of casual processes allows it resource-efficient and more effective to determine the fact of intrusions into IIoT systems than signature analysis. Such algorithm can potentially increase the level of security and resistance to attack, which is particularly important in the face of growing threats in digital environment.**

Keywords — Information entropy, Communication networks, Anomaly detection, Internet of Things, Computer security

I. INTRODUCTION

Industrial Internet of Things technologies (IIoT) are being actively implemented in the manufacturing processes of various critical industries such as energy, transport, healthcare etc [1]. Such systems provide the ability for autonomous monitoring, reduce production and management costs, and optimize resource utilization. Using control nodes allows operating devices of IIoT remotely [2–3].

Network accessibility of IIoT-components increases the risk of implementation cybersecurity incidents. Unauthorized access causes unavailability of services and creates uncontrollable processes that can lead to economic as well as environmental disasters.

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) are designed to protect the infrastructure from network attacks. Their mechanisms rely on signature and behavior analysis of all packets in traffic. Their efficiency is highly dependent on a current and comprehensive knowledge base of known threats. However, if the threat is unique and ~~s~~pecific, the detection of such anomalies can be very challenging.

It is possible to get network data from IIoT infrastructure with the development of virtualization technologies. The network record contains various attacks, which are classified according to the tactics and techniques of the attackers. Given that categorization, it is possible to analyze both the general activity and the network activity of its individual components.

This research provides the use of statistical methods to detect specific traffic abnormals. Anomalies can be caused either by malicious activity or by system and service misconfigurations. Nevertheless, if anomalous traffic behavior is detected, we assume that there may be potentially illegal activity that requires further analysis. The method is based on the calculation of entropy divergence. The entropy estimation method uses overlapping intervals, which allows both adaptation and preservation of information about traffic behavior over past time periods. The calculation of divergence allows us to realize the differences between typical and abnormal patterns of network traffic dynamics.

The purpose of the research is to identify anomalies and patterns in network traffic by estimating entropy, which indicates potential threats to the security of Industrial Internet of Things control systems. It is expected to evaluate the expediency of using entropy to analyze suspicious activity, as well as to identify the possible relationship between the divergence parameters and correctness of detection.

II. LITERATURE REVIEW

The security of IIoT network systems is still fraught with fundamental problems due to a number of features, despite significant advances in corporate cyber defense. A sufficient part of recent investigations is devoted to statistical methods for detection network anomalies. It has different approaches to searching for suspicious behavior due to the wide variability in the characteristics of network flow and ways to evaluate randomness. The focus will be on studying and collecting the required parameters and calculation methods to receive consistent characteristics that form the basis for analyzing their origin. This literature review looks at the ways of selecting special data from network packets,

estimation of a state of disorder and metrics indicating an anomaly.

The article [4] analyzes delays in updating signature databases for network intrusion detection systems (NIDS) and highlights their weakness. It indicates the inability to counter threats when the attack is already known in the absence of detection rules. This highlights the limitations of signature-based methods, which makes entropy-based anomaly detection a more effective alternative for identifying new and unknown threats in real time.

The choice of the method and its criteria has been studied in many researches. The uncertainty measure was calculated according to the theorems of Shannon, Renyi, and Tsallis. The results of the calculations showed that Renyi and Tsallis entropy demonstrate more accurate measurements [5]. Moreover, Shannon's entropy illustrates a higher percentage of false positive results than others. The high accuracy is achieved by the choice of *a* parameter. It is assumed that the values in the range [–2, 2] are optimal, but it must be selected for each type of attack.

Abnormal activity detection requires exact metrics. The EWMA model [6] predicts anomaly based on historical activity and considers dynamic threshold by using time fixed window function. This method is better adapted to changes and has higher precision. This is explained by the concept of a time interval selection, which updates every step, allowing to evince changes in activity more sensitively.

It is also important to select certain attributes from network packets. They contain fields of the recipient, sender, transmitted data, and service details. The considered technique of detecting DDoS [7] uses the sender's IP-address, flags, and packet's length. The IP-address of the source node can be spoofed during the attack. Therefore, further analysis showed that using packet's length and flag categorizes illegal network traffic more precisely.

Other researchers suppose that the payload of packets [8] an provide valuable insights into network behavior. In this case, changes in entropy can be caused by encryption session absence. Investigators analyzed large datasets of packet data containing legitimate service activity and came up with the conclusion that their entropy value is approximately equal. However, there are some inaccuracies, characterized by a lack of consideration for traffic directions, flags and other special information.

In the next trial, authors add destination addresses and ports to their methodology [9]. This investigation uses Shannon's entropy, which other researchers do not consider suitable for solving the anomaly search problem. The results revealed that attacks have an ambiguous impact on entropy characteristics, which are heavily influenced by the distribution of normal traffic, the strength of the attack, and other factors.

As the volume of data continues to grow exponentially, algorithm optimization issue is a crucial aspect that directly impacts on the performance of the network analysis tool. A model called DoDGE [10] considers scalability and assumes a reduced number of false positives. The method is based on the analysis of the entropy progression of IP-addresses in network traffic. At each point, the Tsallis entropy of the addresses is calculated. Then, a regression line is constructed from several previous entropy values, and its slope is used for analysis. If it goes sharply negative, it specify a possible DoS attack. However, this suggests an increase in legitimate traffic if the entropy of the sources increases symmetrically.

In the context of this research, the authors explored low-rate DDoS [11] attacks and its influence on entropy characteristics. The computational methods were performed on real network data, which were separated into legitimate and attack traffic. In papers [5, 11], Renyi entropy has shown the highest level of accuracy with $a>1$, where a is some coefficient. Outcomes are different from normal and anomalous traffic during low-speed attacks, but this result was achieved over a narrow range of a. In contrast, Shannon's entropy was found to be less sensitive in detecting anomalies because of its more limited flexibility.

The article [12] focuses on detecting flash changes in the network traffic using Shannon's entropy time series analysis. The technique consists of source and destination IP-addresses, the number of ports, protocols of data transmitting, and packet size. The method involves dividing traffic data into fixed time windows, calculating entropy for each window, and identifying changes by statistical techniques. The snapshot of network traffic includes DDoS-attack, the propagation of network worm and different types of scanning, which is classified as reconnaissance [13]. Thus, it was possible to detect flash events. Unlike the previous work [11], the current algorithm does not allow for the detection of long-term and low-rate attacks.

It is important for classification to detect not only the fact of attack but also its reason. The classification allows to assess the risk and consequences. This is necessary for response measures at the time of occurrence and avoidance of similar events in the future. The correct strategy for implementing defenses against network attacks is primarily based on evaluating the existing weaknesses and the categories of attacks that the infrastructure is vulnerable to. The paper [14] provides the most comprehensive classification of IIoT network attacks by various categories, such as: DDoS, IP spoofing, selective forward attack, etc.

III. METHODS

The aim of this research is detection anomalies and patterns in network traffic to identify potential threats to industrial IoT control systems using entropy evaluation. The source network data is a set of legitimate and attack traffic generated by an internal and external attacker.

The architecture of IIoT infrastructure includes two ubuntu servers with control, MQTT subscriber and publisher roles, two attacker virtual machines and two single-board computers with OpenPLC and Wi-Fi access point roles. There are attacks categorized as discovery, persistence, lateral movement, collection, and exfiltration in the illegitimate part of the traffic [15–16].

The input data needs to be processed for analysis. Entropy evaluation method uses information about packet registration time, source IP address, and packet payload.

We use a window that contains the packets recorded within an input fixed time frame. These packets are aggregated into a single unit by concatenating their payloads and using the timestamp of the first packet during the interval. Then, this window is moved across the entire

dataset in an input specified time interval. An array of aggregated data is generated, objects are taken by pairs, and method calculates their information distance [17].

The information distance formula is based on the Renyi (1) and Tsallis (2) entropies for a discrete set:

$$H_\alpha(X) = \frac{1}{1-\alpha} log \sum_{i=1}^{n} p_i^\alpha \qquad (1)$$

$$S_q(P) = \frac{k}{q-1}\left(1 - \sum_{i=1}^{N} p_i^q\right) \qquad (2)$$

In these formulas, *a* and *q* are independent parameters calibrated for a more accurate result. *Pi* represents the frequency distribution of payload symbols in a single entity from the aggregated data set.

It is more appropriate to use Renyi (3) and Tsallis (4) entropy divergences to observe the dynamics of network traffic:

$$D_\alpha(P||Q) = \frac{1}{\alpha-1}\log \sum_{i=1}^{n} p_i^\alpha q_i^{1-\alpha} \qquad (3)$$

$$D_q(A,B) = \frac{k}{q-1}\left(\sum_{i=1}^{N} a_i^q b_i^{1-q} - 1\right) \qquad (4)$$

Hence, we can calculate the information distance between nearby entities in the aggregated data array.

IV. Results

During the investigation, the sample and full data were processed, and the functions for calculating the Renyi and Tsallis divergences (3), (4) were implemented. Fig. 1 shows the temporal distribution of entropy divergence. Vertical lines show activity from the attacker's IP address to calibrate the method and its parameters.

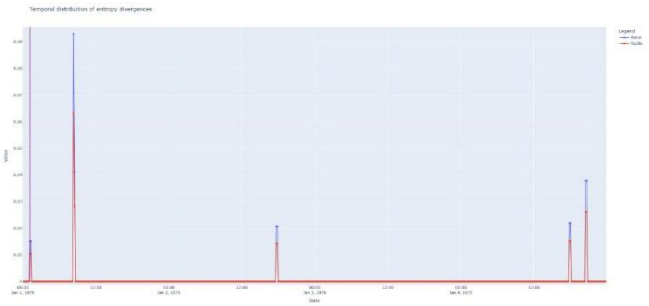

Fig. 1. Temporal distribution of entropy divergences for the test data

In the first case, the attack was detected, but in other cases the activity was legitimate. The calculations were performed on the test data with parameters *a*=0.5 and *q*=0.5, the time step was 5 min, and the aggregation interval was set to be equal to 10 min.

It is planned to continue the investigation and obtain more accurate divergence parameters, as well as optimal time windows and steps.

V. Conclusion

In summary, using entropy estimates with standard parameters allowed to obtain many false positives, but also indicated the real threat.

It becomes clear from a detailed study of numerous examples that the entropy parameters as well as the time interval and the step play an important role in the anomaly detection.

Choosing the exact parameters allow to achieve an increase in the number of true positives. Therefore, the method can be integrated into modern intrusion detection systems, that can mitigate various risks associated with security threats. Technologies are constantly developed, and attacks are becoming more and more complex. This research provides groundwork for a new sight to network security.

References

[1] D. Kutuzov, A. Osovsky, O. Stukach, D. Starov, "Modeling of IIoT Traffic Processing by Intra-Chip NoC Routers of 5G/6G Networks". 2021 International Siberian Conference on Control and Communications (SIBCON). 13-15 May 2021, Kazan, Russia. Publisher: IEEE. Electronic ISBN: 978-1-7281-8504-0, USB ISBN: 978-1-7281-8503-3, Online ISSN: 2380-6516, DOI: 10.1109/SIBCON50419.2021.9438874.

[2] Denis Kutuzov, Alexey Osovsky, Dmitriy Starov, Oleg Stukach, Ekaterina Motorina. "Processing of the Gaussian Traffic from IoT Sources by Decentralized Routing Devices". 2019 International Siberian Conference on Control and Communications (SIBCON). 18-20 April 2019, Tomsk, Russia. Publisher: IEEE. Electronic ISBN: 978-1-5386-5142-1. DOI: 10.1109/SIBCON.2019.8729617.

[3] Kutuzov D.V., Osovsky A.V., Stukach O.V. Model of IoT Trafic Generation and Processing by Parallel Switch Systems // Vestnik SibSUTI, 2019, no. 4, pp. 78-87.

[4] H Gascon, A. Orfila, J. Blasco, "Analysis of update delays in Signature-based Network Intrusion Detection Systems," Computers & Security (2011), DOI: 10.1016/j.cose.2011.08.010.

[5] Bereziński P, Jasiul B, Szpyrka M., "An Entropy-Based Network Anomaly Detection Method. Entropy," 2015; 17(4):2367-2408., DOI: 10.3390/e17042367.

[6] Yu, H., Yang, W., Cui, B. et al., "Renyi entropy-driven network traffic anomaly detection with dynamic threshold," Cybersecurity 7, 64 (2024), DOI: 10.1186/s42400-024-00249-1.

[7] S. Sharma, S. K. Sahu and S. K. Jena, "On selection of attributes for entropy based detection of DDoS," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 2015, pp. 1096-1100, DOI: 10.1109/ICACCI.2015.7275756.

[8] Kenyon A, Deka L, Elizondo D., "Characterising Payload Entropy in Packet Flows—Baseline Entropy Analysis for Network Anomaly Detection," Future Internet. 2024; 16(12):470, DOI: 10.3390/fi16120470.

[9] A.Yu. Efimov, "Using the entropy characteristics of network traffic to determine its abnormality," Programmnye Produkty i Sistemy, no. 1, pp. 83–90, 2021. Available: https://swsys.ru/index.php?page=article&id=4783. [Accessed: Jan. 27, 2025].

[10] O. Subasi, J. Manzano and K. Barker, "Denial of Service Attack Detection via Differential Analysis of Generalized Entropy Progressions," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 219-226, DOI: 10.1109/CSR57506.2023.10224957.

[11] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Information metrics for low-rate DDoS attack detection: A comparative evaluation," 2014 Seventh International Conference on Contemporary Computing (IC3), Noida, India, 2014, pp. 80-84, DOI: 10.1109/IC3.2014.6897151.

[12] Winter, P., Lampesberger, H., Zeilinger, M., Hermann E., "On Detecting Abrupt Changes in Network Entropy Time Series," In: De Decker, B., Lapon, J., Naessens, V., Uhl, A. (eds) Communications and Multimedia Security. CMS 2011. Lecture Notes in Computer

Science, vol 7025. Springer, Berlin, Heidelberg, DOI: 10.1007/978-3-642-24712-5_18.

[13] MITRE, "MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge," [Online]. Available: https://attack.mitre.org. [Accessed: 27-Jan-2025].

[14] Bhukya Madhu, Sanjib Kumar Nayak, Veerender Aerranagula, E. Srinath, Mamidi Kiran Kumar, Jitendra Kumar Gupta, "IoT Network Attack Severity Classification," E3S Web Conf. 430 01152 (2023), DOI: 10.1051/e3sconf/20234300115.

[15] A. Osovsky, D. Kutuzov, D. Starov, R. Bakalaeva, O. Stukach, "Comparison of Machine Learning Methods for IoT and IIoT Traffic Prediction", International Seminar on Electron Devices Design and Production (SED), 2024 October 02-03, Sochi, Russian Federation, Publisher: IEEE, DOI: 10.1109/SED63331.2024.10741069.

[16] D. Kutuzov, A. Osovsky, O. Stukach, N. Maltseva, D. Starov, "Modeling the Processing of Non-Poissonian IIoT Traffic by Intra-Chip Routers of Network Data Processing Devices", Dynamics of Systems, Mechanisms and Machines (Dynamics), 2021, 9-11 Nov., Omsk, Russian Federation, pp. 1-4, doi: 10.1109/Dynamics52735.2021.9653703.

[17] Sergeichev A.V., Stukach O.V. "Entrophy Evaluation of IIoT Trafic for the Anomaly Detection", Electronics, Electrical Engineering and Energetics: 31-th Intern. Sci.-Tech. Conference, MPEI, March 13-15, 2025, 1244 p. ISBN 978-5-907732-36-0, p. 329, https://reepe.mpei.ru/abstracts/Documents/Blok_doklad_2025_fin.pdf

Информация об авторе:

Сергеичев Андрей Викторович, студент департамента Электронной инженерии Московского института электроники и математики им. А.Н. Тихонова Национального исследовательского университета «Высшая школа экономики», г. Москва, Россия, e-mail: avsergeichev@edu.hse.ru

Исследование оценок энтропии трафика промышленного Интернета вещей с целью раннего обнаружения атак

А.В. Сергеичев

Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия

Аннотация **– Исследуется зависимость между возникновением атаки и изменениями энтропийных свойств сетевого трафика. Входные данные представляют собой образцы трафика сетевой системы управления промышленного Интернета вещей и реализуемой там атаки. Сетевой трафик отфильтрован от служебной информации и оцифрован путём частотного анализа содержания каждого записанного пакета. Этот процесс позволяет сохранить ключевые свойства трафика. Данные агрегируются кумулятивной функцией. Затем отсчёты обрабатываются методом скользящего окна. Окно перемещается с шагом во времени, что позволяет в режиме реального времени динамически мониторить трафик и идентифицировать потенциальные угрозы. Каждый отсчёт представляет собой дивергенцию распределений. Если различие в распределениях близко к нулю, аномалии считаются отсутствующими. Чувствительность алгоритма к обнаружению аномалии зависит от выбора параметров, таких как длина временного интервала накопления отсчётов, размера скользящего окна и шага перемещения. Ожидается, что полученные меры зависимости случайных процессов позволят быстрее и эффективнее определять факт вторжений в системы промышленного Интернета вещей, чем сигнатурный анализ. Такой алгоритм может потенциально увеличить уровень безопасности и защиты, что особенно важно в условиях нарастающих угроз в цифровой среде.**

Ключевые слова – информационная энтропия, сети связи, обнаружение аномалий, Интернет вещей, компьютерная безопасность.

Список литературы

[1] Кутузов Д.В., Осовский А.В., Стукач О.В., Старов Д.В. Моделирование обработки трафика промышленного Интернета вещей внутричиповыми маршрутизаторами сетей 5-6 поколения / Международная IEEE-Сибирская конференция по управлению и связи SIBCON-2021. – 13-15 мая 2021, Казань, Россия. – Публ. IEEE. – DOI: 10.1109/SIBCON50419.2021.9438874.

[2] Кутузов Д.В., Осовский А.В., Старов Д.В., Стукач О.В., Моторина Е. Обработка гауссовского трафика от источников Интернета вещей децентрализованными устройствами маршрутизации / Международная IEEE-Сибирская конференция по управлению и связи SIBCON-2019. – 18-20 апреля 2019, Томск, Россия. – DOI: 10.1109/SIBCON.2019.8729617.

[3] Кутузов Д.В., Осовский А.В., Стукач О.В. Модель генерации и обработки трафика IoT параллельными коммутационными системами // Вестник СибГУТИ. – 2019. – N 4. – С. 78-87.

[4] H Gascon, A. Orfila, J. Blasco Analysis of update delays in Signature-based Network Intrusion Detection Systems // Computers & Security. – 2011. – DOI: 10.1016/j.cose.2011.08.010.

[5] Bereziński P, Jasiul B, Szpyrka M. An Entropy-Based Network Anomaly Detection Method. Entropy. – 2015. – 17(4):2367-2408. – DOI: 10.3390/e17042367.

[6] Yu H., Yang, W., Cui, B. и др. Renyi entropy-driven network traffic anomaly detection with dynamic threshold // Cybersecurity. – 2024. – № 7. – Т. 64, – DOI: 10.1186/s42400-024-00249-1.

[7] S. Sharma, S. K. Sahu and S. K. Jena On selection of attributes for entropy based detection of DDoS / 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 2015. – С. 1096-1100. – DOI: 10.1109/ICACCI.2015.7275756.

[8] Kenyon A, Deka L, Elizondo D. Characterising Payload Entropy in Packet Flows – Baseline Entropy Analysis for Network Anomaly Detection," Future Internet. – 2024. – 16(12):470. – DOI: 10.3390/fi16120470.

[9] A.Yu. Efimov Using the entropy characteristics of network traffic to determine its abnormality // Programmnye Produkty i Sistemy. – 2021. – № 1. – С. 83–90. Режим доступа: https://swsys.ru/index.php?page=article&id=4783. [Дата обращения: 27 янв 2025].

[10] O. Subasi, J. Manzano, K. Barker. Denial of Service Attack Detection via Differential Analysis of Generalized Entropy Progressions / 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023. – С. 219-226. – DOI: 10.1109/CSR57506.2023.10224957.

[11] M. H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita Information metrics for low-rate DDoS attack detection: A comparative evaluation / 2014 Seventh International Conference on Contemporary Computing (IC3), Noida, India. – 2014. – С. 80-84. – DOI: 10.1109/IC3.2014.6897151.

[12] Winter P., Lampesberger H., Zeilinger M., Hermann E. On Detecting Abrupt Changes in Network Entropy Time Series," In: De Decker, B., Lapon, J., Naessens, V., Uhl, A. (eds) Communications and Multimedia Security. CMS 2011. Lecture Notes in Computer Science, vol 7025. Springer, Berlin, Heidelberg, – DOI: 10.1007/978-3-642-24712-5_18.

[13] MITRE, "MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge," [Online]. Режим доступа: https://attack.mitre.org. [Дата обращения: 27 января 2025].

[14] B. Madhu, S.K. Nayak, V. Aerranagula, E. Srinath, M.K. Kumar, J. K. Gupta. IoT Network Attack Severity Classification / E3S Web Conf. 430 01152 (2023), – DOI: 10.1051/e3sconf/20234300115.

[15] Осовский А., Кутузов Д., Старов Д., Бакалаева Р., Стукач О. Сравнение методов машинного обучения для Интернета вещей и прогнозирования трафика промышленного Интернета вещей / Международный семинар по проектированию и технологии производства электронных средств (SED), 02-03 октября 2024, Сочи, Россия. Изд. IEEE. DOI: 10.1109/SED63331.2024.10741069.

[16] Кутузов Д., Осовский А., Стукач О., Мальцева Н., Старов Д. Моделирование обработки непуассоновского IIoT-трафика внутрикристальными маршрутизаторами сетевых устройств обработки данных / Динамика систем, механизмов и машин, 9-11 ноября 2021, Омск, Россия, стр. 1-4. – Doi: 10.1109/Dynamics52735.2021.9653703.

[17] Сергеичев А.В., Стукач О.В. Оценка энтропии трафика промышленного интернета вещей с целью обнаружения аномалий / Радиоэлектроника, электротехника и энергетика: 31 междунар. науч.-техн. конф. студентов и аспирантов (13-15 марта 2025 г., Москва): Тез. докл. - М.: ООО “Центр полиграф. услуг "Радуга"”, 2025. - 1244 с. ISBN 978-5-907732-36-0, – С. 329. – https://reepe.mpei.ru/abstracts/Documents/Blok_doklad_2025_fin.pdf