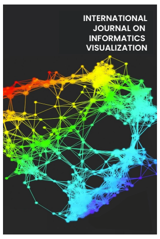
INTERNATIONAL JOURNAL
ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv



Network Attack Detection Using NeuroEvolution of Augmenting Topologies (NEAT) Algorithm

Tamara Zhukabayeva [a,b,c], Aigul Adamova [a,c,*], Khu Ven-Tsen [a], Zhanserik Nurlan [a], Yerik Mardenov [a], Nurdaulet Karabayev [a,c]

[a] *International Science Complex "Astana", Kabanbay Batyr 8, Astana, 020000, Kazakhstan*
[b] *L.N. Gumilyov Eurasian National University, Satpayev 2, Astana, 010008, Kazakhstan*
[c] *Astana IT University, Mangilik El 55/11, Astana, 010000, Kazakhstan*
*Corresponding author: *aigul.adamova@astanait.edu.kz*

***Abstract*—The imperfection of existing intrusion detection methods and the changing nature of malicious actions on the attacker's part led to the Internet of Things (IoT) network interaction in an unsafe state. The actual problem of improving the technology of the IOT is counteracting malicious network impacts. In this regard, research and development aimed at creating effective tools for solving applied problems within the framework of this problem are becoming increasingly important. This study seeks to develop tools for detecting anomalous network conditions resulting from malicious attacks. In particular, the accuracy of the identification of DoS and DDoS attacks is sufficient for operational use. This study analyzes various multi-level architectures, relevant communication protocols, and different types of network attacks. The presented research was conducted on open datasets TON_IOT DATASETS, which include multiple data sources collected from IoT sensors. The modified HyperNEAT algorithm was used as the basis for the development. The NEAT methodology used in the study allows you to combine various network nodes. Results of the study: a neuro-evolutionary algorithm for identifying DoS and DDoS attacks was implemented, integrated, and real-tested based on a multi-level analysis of network traffic combined with various adaptive modules. The accuracy of identifying DoS and DDoS attacks is 0.9242 in the Accuracy metric. The study implies that the proposed approach can be recommended for network intrusion detection, ensuring security when interacting with the IoT.**

***Keywords*—Internet of Things; attacks; HyperNEAT; neuro-evolutionary algorithm; wireless sensor network.**

Manuscript received 8 Oct. 2023; revised 17 Jan. 2024; accepted 23 Feb. 2024. Date of publication 31 Mar. 2024.

I. INTRODUCTION

Detection of network attacks is one key element of protecting computer networks. To improve the current tools, intensive research is being conducted to create new, more efficient algorithms, including those based on hybrid and adaptive recognition systems [1]. Recently, due to the rapid spread of various Internet of Things systems, this problem has become significantly more urgent. This resulted from the emergence of multiple vulnerabilities due to the lack of an advanced encryption and authentication system and the lack of commercial solutions available on the market to ensure appropriate security [2].

The target of an attack can be any Internet of Things device, but cameras and routers are most often attacked (due to their prevalence and large number). Attackers build botnets from compromised devices, which are then used for DDoS attacks [3]. At the same time, developments are constantly updated, focusing on new vulnerabilities in devices [4]. For example, from year to year, more and more new versions of Mirai appear, a botnet that spreads on its own and, first, threatens the Internet of Things devices. With its help, a large-scale DDoS attack was organized on the servers of the DNS provider Dyn [5]. As a result, the websites of many of the company's clients, including Twitter, PayPal, Amazon, Netflix, and CNN, were temporarily unavailable.

According to Statista.com, the number of Internet of Things attacks worldwide exceeded 10.54 million in December 2022. Compared to 2021 data, recorded IoT attacks have dropped to six million. The highest figure was recorded in June 2022, reaching 13 million attacks. Currently, many works study the applicability of the methods under consideration in attack detection tasks [6]. In [7], the authors propose a method for detecting information security threats using supervised and unsupervised learning algorithms.

It is proposed that public datasets be analyzed, and the system be trained for further classification of events based on machine learning methods. It should be noted that this approach, despite modern algorithms, is volatile to the perception of new threats [8]. At the same time, the results of computational calculations for various algorithms presented in the work show that some of them successfully cope with the task, which may mean a positive prospect for this approach. At the same time, the possibility of data visualization when using the specified software analysis tools is indicated [9].

As a possible direction for using machine learning in attack detection tasks, the authors of [10] investigated using an unsupervised machine learning system in an information system. They found that because the problem being solved is poorly formalized, the selection of classification characteristics cannot always be successful. The study results showed high values for false negatives and false positives.

An important area of application of machine learning is the search for solutions to open questions on IoT information security. These problems include the behavior policy for the Internet of Things in the face of malicious attacks. For example, situations in which wireless sensor network nodes independently learn to adapt to ongoing attacks. The result of such training can be the corresponding operation of the protection system. As soon as attacks start to activate, using the weak factors of the nodes, the latter change their tactics of behavior, which can make it more challenging to achieve the expected result of the attack. This type of technology will improve the overall security level of wireless sensor networks [11], [12].

These approaches were used in developments, the results of which are presented in this article. The article consists of two sections. The first section displays the various types of IoT architecture. At the same time, various interconnected multi-layer architectures and the current protocols for each layer are analyzed. Moreover, the first section describes the research methodology used in scientific literature to analyze the types of network attacks. The proposed neuro-evolutionary algorithm for detecting DoS and DDoS attacks and the results of its research and testing are presented in the second section.

II. Materials and Method

A. *Architecture of the Internet of Things*

IoT consists of various info-communication technologies that enable its operation. Its architecture has a multi-level structure and reflects the relationship between these technologies [13]. There are architectures with different numbers of layers, as shown in Fig. 1. 3-layer architecture is considered a traditional architecture with the primary layers of perception, network, and application [14]. 4-layer architecture is one layer, added to the basic architecture between the network and application layers and three support layers. This architecture provides additional security to the underlying architecture. 5-level architecture is two additional levels to the basic architecture, three process levels, and five business levels [15]. The 7-layer architecture is published by the IoT World Forum (IoTWF) [16]. The architecture is focused on data management. New levels are being added to the traditional architecture: 3 Edge Computing, 4 DATA Accumulation/storage, 5 DATA Analysis, and 7 Collaboration Layer.

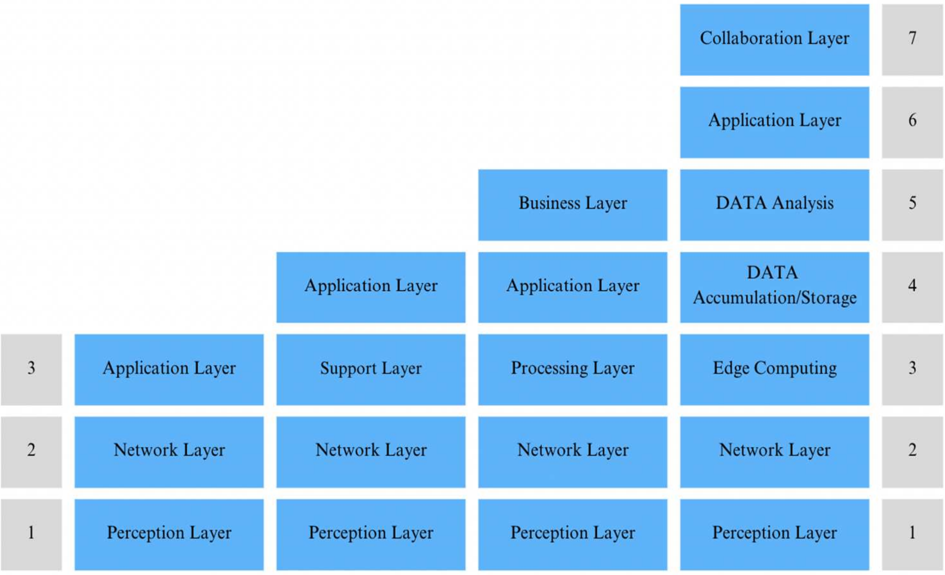


Fig. 1 Variation of IoT architecture

The IoT architecture promotes a systematic understanding of methodologies, technologies, and tools that uniquely play a development role. Its goal is to connect the digital with the physical world, creating an entire infrastructure [17]. The network protocol stack is based on a 7-layer architecture. Individual protocols can represent only one layer or be used several times for reliable operation. Internet of Things protocols are divided into two categories: network protocols and data protocols [18]. Network protocols provide edge device connections, while data protocols focus on information exchange. Each category contains several protocols with unique features (Fig. 2).

The perceptual layer is the hardware where data comes in unstructured form from physical objects. Next, the network layer is responsible for the interaction between devices, networks, and cloud services, which, in turn, make up the IoT network infrastructure. The IoT edge layer detects and impacts other devices and performs data pre-processing. The DATA Accumulation/storage and DATA Analysis levels accumulate, store, and process data from the previous level. All these tasks are solved using IoT platforms and include two main stages with data: accumulation and abstraction. The general purpose of the data accumulation step is to sort through a large amount of diverse data and store it most efficiently. The data abstraction phase completes the data preparation so that consumer applications can use it to obtain information. Data accumulation and abstraction steps hide hardware details, increasing smart device interoperability. Further, at the application level, information is analyzed using additional software to provide answers to crucial business questions. At the final level of collaboration, data-driven solutions are implemented. All information generated in the previous levels is only helpful if it leads to problem-solving and business goals.

At the next stage, messaging protocols are connected to exchange data between devices and the cloud. Fig. 2 shows some IoT network protocols and data protocols [19]. The most popular protocols used in the IoT interaction process are as follows:

- LoRaWAN: a network protocol that ensures the interaction of devices in IoT infrastructure.
- DDS: a protocol connecting IoT devices and the application in real time.
- AMQP: a protocol designed for data exchange between servers of the same rank.
- CoAP: a protocol designed for interaction with end nodes with limited memory and power.
- MQTT: messaging protocol used to collect data from IoT end devices.

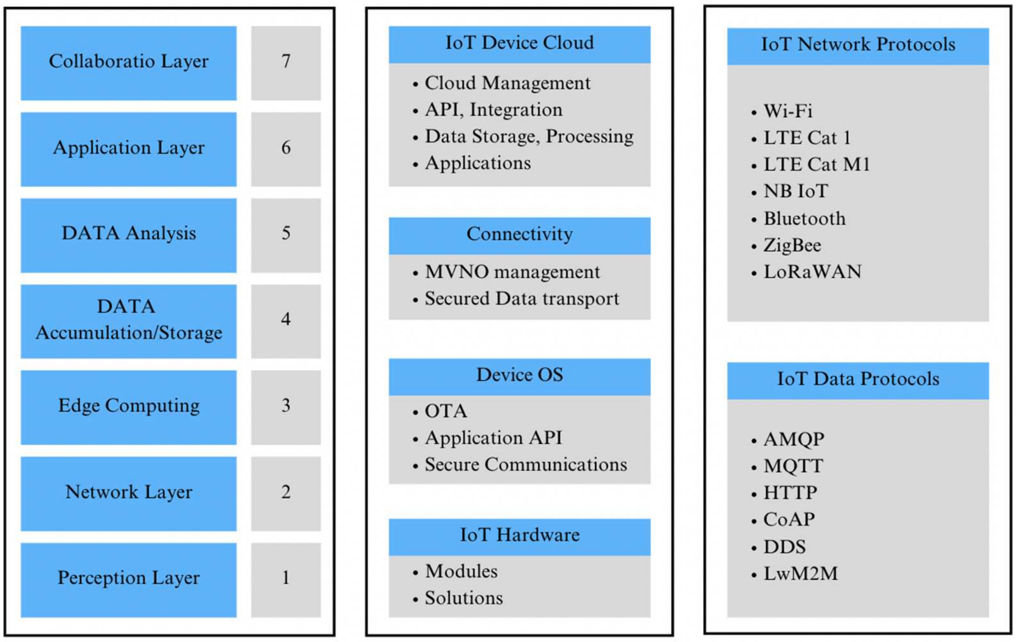


Fig. 2 The IoT Protocols Stack

B. Research Methodology and Analysis of Network Attacks

Currently, scientists and researchers from different countries are actively researching this area in connection with the actual entry of IoT into our lives. In 2023 alone, Google Scholar issued 8330 papers for the keyword "IoT security". The research on security and IoT attacks is based on analyzing many published scientific literature. The research process consists of several stages: searching for research papers in various databases by keywords, eliminating repetitions, and selecting scientific documents according to specific criteria, for example, publications containing IoT attack detection methods, in the 2023-year publication period. Next, scientific articles related to the direction of our research (Fig. 3).

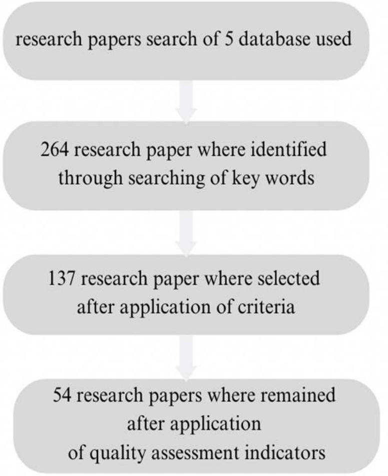

research papers search of 5 database used
264 research paper where identified through searching of key words
137 research paper where selected after application of criteria
54 research papers where remained after application of quality assessment indicators

Fig. 3 Methodology of research

Scientific papers were searched using Google Scholar, IEEE, Springer, Science Direct, and Academia. Search results for scientific works in databases were made using keywords such as "IoT attack," "IoT Physical attacks," "IoT Network attacks," "Cryptanalysis attacks, IoT," and "Side channel attacks, IoT" (Table 1).

TABLE I
DATABASES USED TO SEARCH RESEARCH PAPERS

Key Words	Database				
	Google Scholar	IEEE	Springer	ScienceDirect	Academia
IoT attacks	4720	553	4952	2019	249
IoT Physical attacks	3520	117	3845	1365	623
IoT Network attacks	4590	472	4825	1955	2068
Cryptoanalysis attacks, IoT	1020	2	238	59	267
Side channel attacks, IoT	2020	13	2030	570	1278

Various technological advances have recently introduced different types of IoT devices. These devices are connected to many networks and actively interact with each other, making them vulnerable and easy to attack. To reduce the vulnerabilities of devices that exchange sensitive information, it is essential to identify all possible attacks to take countermeasures or defense strategies [20]. Different types of attacks are likely at varying levels of the IoT architecture (Fig. 4). Based on the traditional three-level architecture, examples of possible attacks are given for each level [3], [21]. Fig. 5 shows frequently encountered attacks on a three-layer architecture, and simultaneously, practically implemented response mechanisms are noted.

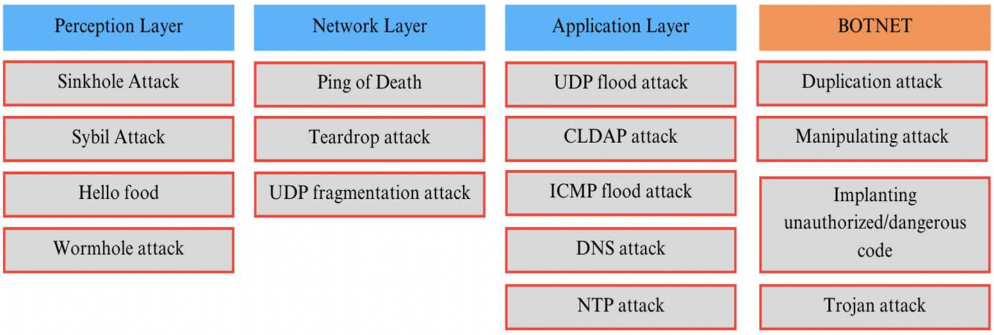


Fig. 4 Types of attacks at different levels of the IoT architecture

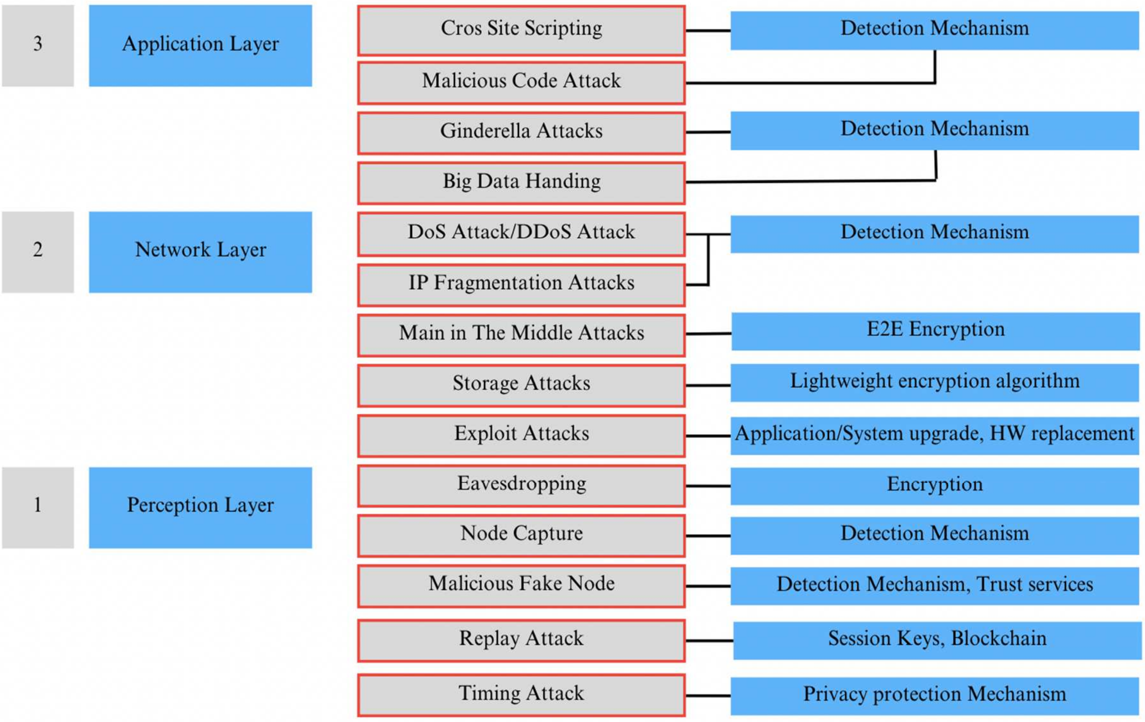


Fig. 5 Examples of possible attacks on a three-layer architecture and response mechanisms

III. Results and Discussion

A. Neuro-evolutionary Algorithm for Detecting Network Attacks based on HyperNeat

NEAT was developed by Ken Stanley in 2002 at the University of Texas at Austin [22]. NEAT uses a genetic algorithm that allows the network to evolve by choosing the best topology and connection weights between nodes for the neural network. It has vital functions such as complexity, avoidance of competing conventions through historical marking, speciation, and fitness sharing. Over the years, the performance of NEAT has become increasingly better, with more advanced approaches such as HyperNEAT and CoDeepNEAT [23,24].

NEAT is an algorithm that reduces the search space size for parameters by gradually developing a neural network through evolution. The evolutionary process begins with simple genomes and progressively increases their complexity with the advent of new generations (Fig. 6). Each genome in NEAT includes a list of junction genes, each of which refers to two connected node genes. The NEAT methodology allows for capturing a complex structural network and, thanks to marks, makes it possible to combine different network nodes [24], [25].

The link genome contains the input node ID, the output node ID, the link weight, the bit (presence/absence of link), and the update number. The node genome contains the node ID, node type, and function type [26], [27], [28]. The HyperNEAT method is an extended version of NEAT that uses multidimensional geometric structures. HyperNEAT stores a pattern of connections, where each point encodes a connection between two nodes and computes a four-dimensional function S=F(x1,y1,x2,y2), where (x1,y1) are the coordinates of the source node and *(x_2,y_2)* are the coordinates of the target node.

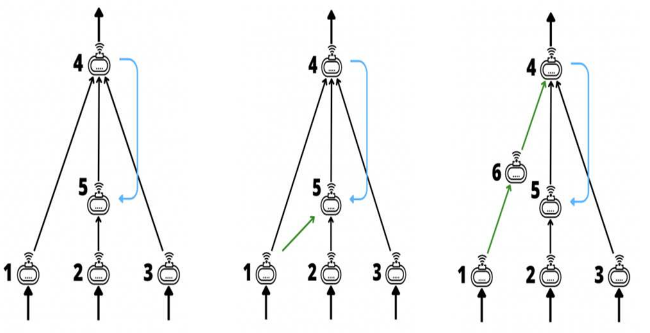


Fig. 6 Evolutionary processes with the addition of links and a node

The distance between two network nodes *(D)* is determined using a linear combination of factors such as the number of redundant *(I)* and non-overlapping genes *(E)*, as well as the difference in the weight of matching genes *(W)*.

$$D = k_1 \frac{I}{Q} + k_2 \frac{E}{Q} + k_3 \underline{W} \tag{1}$$

where *k_1,k_2, and k_3* - coefficients regulate the importance of factors, *and the Q - coefficient governs the number of genes in a large genome; for large genomes,* it will equal 1.

B. Implementation of the Circuit Detection Method Using NeuroEvolution of Augmenting Topologies (NEAT)

The neural network was built and trained using a modified hypercube algorithm using the NEAT library in Python [25, 26]. The NEAT-Python library uses a set of hyperparameters that affect the performance and accuracy of the NEAT algorithm. The attack detection method consists of two stages shown in the block diagram (Fig. 7).

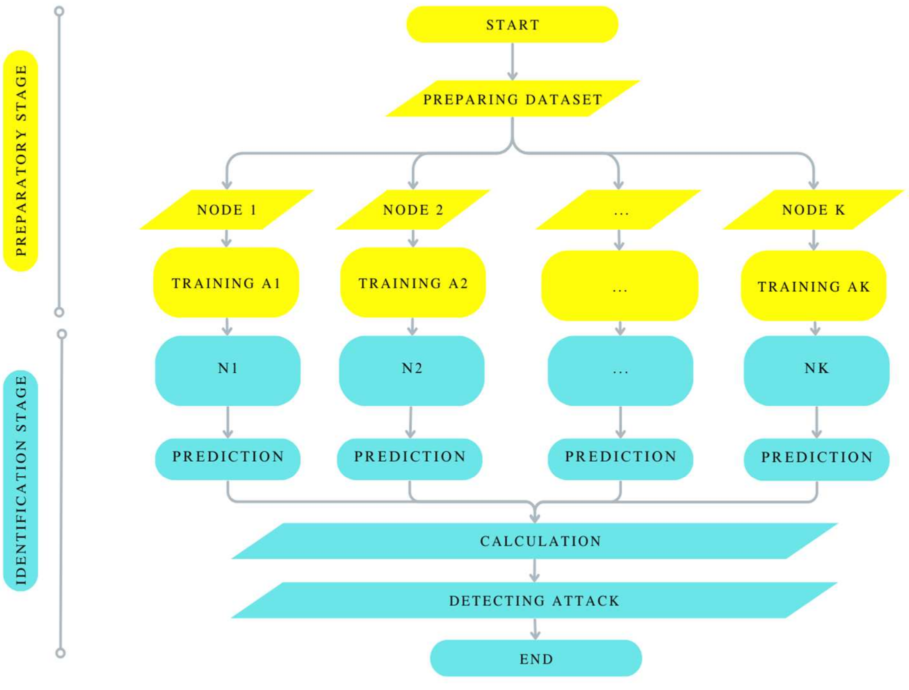


Fig. 7 Intrusion detection flowchart

TABLE II

DESCRIPTION OF THE STEPS OF THE ATTACK DETECTION METHOD

Stages	Steps	Results
	Preparing Dataset	Formation of a multidimensional series
Preparatory Stage	Node 1 Node 2 Node k	The neural network receives a multidimensional series generated by the user.
	Training A1 Training A2 Training Ak	Trained neural network
Identification Stage	N1 N2 Nk	Formation of a multidimensional series
	Prediction	Predicting the future series
	Calculation	Difference between actual and predicted series
	Detecting attack	Presence/absence of attacks

The TON_IOT DATASETS data set was used to implement methods for detecting network attacks. Fig. 8 shows the stages of data processing.

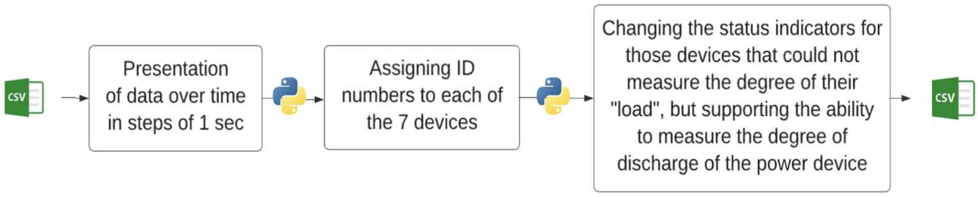

CSV
Presentation of data over time in steps of 1 sec
Assigning ID numbers to each of the 7 devices
Changing the status indicators for those devices that could not measure the degree of their "load", but supporting the ability to measure the degree of discharge of the power device
CSV

Fig. 8 Data processing steps

The data set includes the states and transmitted data of each of the seven network devices: each operates with two main variables and two secondary variables (load and current state value). The considered period of the system operation includes one period equal to two days of functioning in the normal state, during which DoS was discreetly carried out; DDoS attacks on the system are shown in Fig. 9.

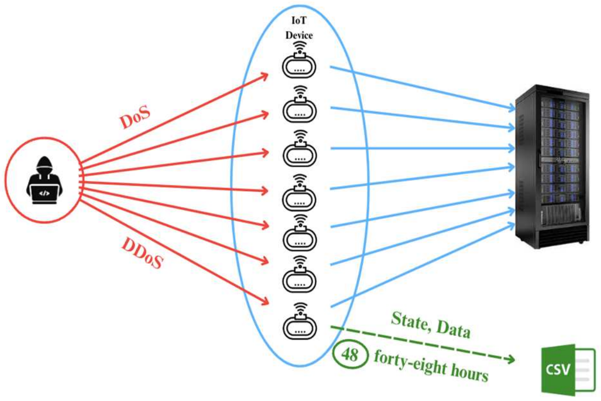


Fig. 9 Schematic representation of the network

C. Evaluation Metrics for Classification of Network Events

The following metrics are used to evaluate the performance of network event analysis classifiers [27]-[31]: accuracy, precision, predictive value, correlation coefficient, and F-score [29], [30]. For any classification algorithm, four classification cases are possible: true positive results (True Positives, TP), false positive results (False Positives, FP), true negative results (True Negatives, TN), and false negative results (False Negatives, FN). The characteristics of these classification cases are given in the following Table 3.

TABLE III

EVALUATION METRICS OF THE CLASSIFICATION METHOD

Positive (P)	total IoT normal state
Negative (N)	total IoT normal state with attacks
true positive	number of IoT normal state detections
true negative	number of correct IoT attack detections
false positive	number of unrecognized attacks on IoT
false negative	number of IoT normal states recognized as attacks

The mathematical formulas shown in Fig. 10 were used to calculate the values.

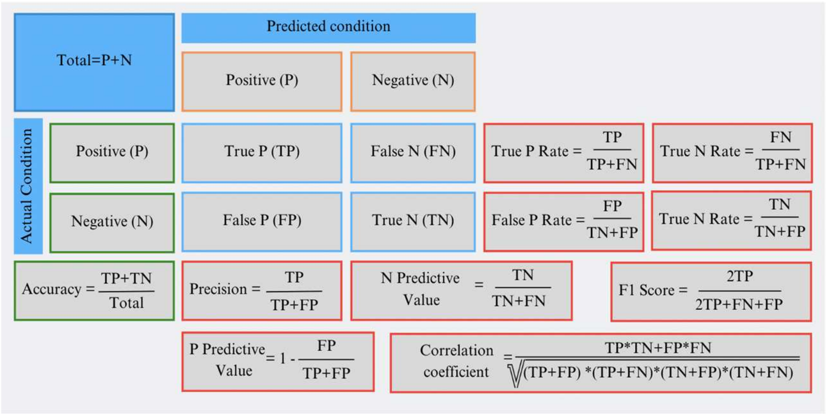

Total=P+N
Predicted condition
Positive (P)
Negative (N)
Actual Condition
Positive (P)
True P (TP)
False N (FN)
$\text{True P Rate} = \frac{TP}{TP+FN}$
$\text{True N Rate} = \frac{FN}{TP+FN}$
Negative (N)
False P (FP)
True N (TN)
$\text{False P Rate} = \frac{FP}{TN+FP}$
$\text{True N Rate} = \frac{TN}{TN+FP}$
$\text{Accuracy} = \frac{TP+TN}{Total}$
$\text{Precision} = \frac{TP}{TP+FP}$
$\text{N Predictive Value} = \frac{TN}{TN+FN}$
$\text{F1 Score} = \frac{2TP}{2TP+FN+FP}$
$\text{P Predictive Value} = 1 - \frac{FP}{TP+FP}$
$\text{Correlation coefficient} = \frac{TP*TN+FP*FN}{\sqrt{(TP+FP)*(TP+FN)*(TN+FP)*(TN+FN)}}$

Fig. 10 Formulas for calculating quantities

The values obtained for the considered time intervals are presented in histograms. The values were broken down by types of DoS, and DDoS attacks and are displayed in Fig. 11 and Fig. 12 for the considered time intervals. The first histogram shows the received data without attacks on DoS and DDoS attacks within two days. The second histogram shows the method's accuracy based on the results of calculations for two days. In particular, the accuracy without attacks approached one, demonstrating the method's incorrect operation, although the technique used shows a good indicator in the interval between DoS and DDoS attacks.

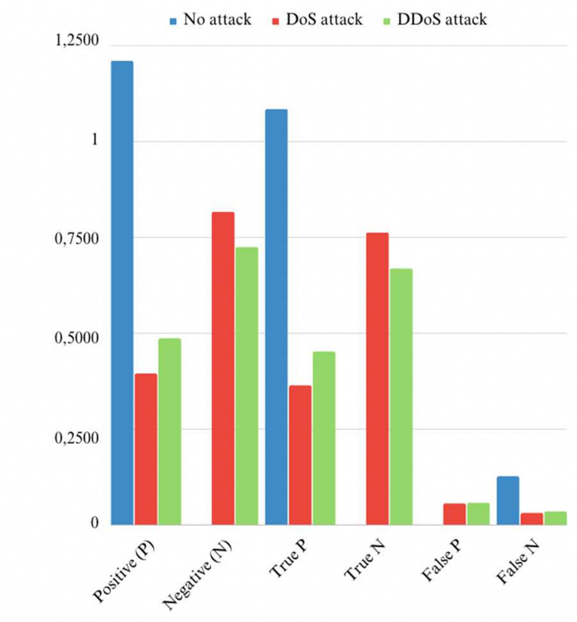


Fig. 11 Obtained data without attacks.

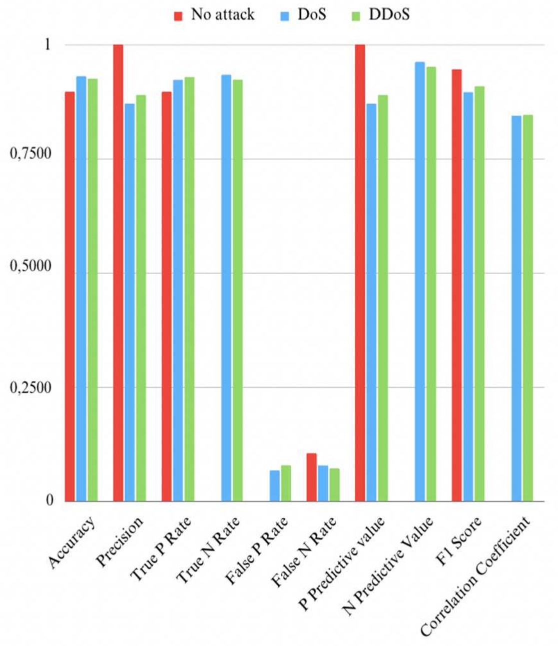


Fig. 12 Method accuracy

Let us note the values of “False P Rate” and “False N Rate”; their values are close to 0.1 and prove that the number of false attack detections is minimal. As a result, the accuracy was 0.9242 (Table 4).

TABLE IV
RESULTS

Accuracy	0.9242
Precision	0.8961
False Positive Rate	0.1209
False Negative Rate	0.1075

The results indicate the absence of model overtraining and the high reliability of this method.

IV. Conclusion

Security and privacy issues are becoming increasingly relevant with the growing number of IoT devices and the volume of exchanged data. This requires the development of new security and data protection standards that help ensure the confidentiality of protected user data. An effective neuro-evolutionary algorithm for detecting DoS and DDoS attacks has been developed. The results of experimental studies and testing of the algorithm on the TON_IOT DATASETS data set are presented.

Research and testing results showed that the proposed approach is workable/feasible and provides sufficiently high accuracy in detecting class network attacks. Compared with known approaches to solving similar problems evaluated on these sets, the proposed aggregation scheme allows for a compromise between recognizing unknown threats and false positives.

Further research is advisable to find and apply other hybrid approaches to attack detection, create experimental data sets, and conduct evaluation test experiments. In summary, we can conclude that the proposed approach and the neuro-evolutionary algorithm can be recommended for use in information and event management systems to secure IoT objects.

Acknowledgment

This research has been funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19680345).

References

[1] M. Aljabri *et al.*, “Intelligent Techniques for Detecting Network Attacks: Review and Research Directions,” *Sensors*, vol. 21, no. 21, p. 7070, Oct. 2021, doi: 10.3390/s21217070.

[2] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, “The Rise of ‘Internet of Things’: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, Aug. 2022, doi:10.1155/2022/8669348.

[3] P. Kumari and A. K. Jain, “A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures,” Computers & Security, p. 103096, Jan. 2023, doi:10.1016/j.cose.2023.103096.

[4] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, “Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects,” Electronics, vol. 11, no. 9, p. 1502, May 2022, doi:10.3390/electronics11091502.

[5] A. Jerkins, “Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code,” 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2017, doi:10.1109/ccwc.2017.7868464.

[6] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, “A machine learning-based intrusion detection for detecting internet of things network attacks,” Alexandria Engineering Journal, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi:10.1016/j.aej.2022.02.063.

[1] K. Levchenko, Ramamohan Paturi, and G. Varghese, “On the difficulty of scalably detecting network attacks,” *Computer and Communications Security*, Oct. 2004, doi:10.1145/1030083.1030087.

[2] T. Talaei Khoei and N. Kaabouch, “A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems,” *Information*, vol. 14, no. 2, p. 103, Feb. 2023, doi:10.3390/info14020103.

[3] H. Bai, R. Cheng, and Y. Jin, “Evolutionary Reinforcement Learning: A Survey,” *Intelligent Computing*, Apr. 2023, doi:10.34133/icomputing.0025.

[4] B. Kaur *et al.*, “Internet of Things (IoT) security dataset evolution: Challenges and future directions,” *Internet of Things*, p. 100780, Apr. 2023, doi:10.1016/j.iot.2023.100780.

[5] M. A. Umer, K. N. Junejo, M. T. Jilani, and A. P. Mathur, “Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations,” *International Journal of Critical Infrastructure Protection*, p. 100516, Feb. 2022, doi:10.1016/j.ijcip.2022.100516.

[6] A. Adamova, T. Zhukabayeva, and Y. Mardenov, “Machine Learning in Action: An Analysis of its Application for Fault Detection in Wireless Sensor Networks,” *2023 IEEE International Conference on Smart Information Systems and Technologies (SIST)*, May 2023, doi:10.1109/sist58284.2023.10223548.

[7] M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov, and M. Derawi, “A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey,” *IEEE Access*, pp. 1–1, 2022, doi:10.1109/access.2022.3207472.

[8] A. Raj and S. D. Shetty, “IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey,” *Wireless Personal Communications*, Aug. 2021, doi:10.1007/s11277-021-08958-3.

[9] R. Nath N and H. V Nath, “Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges,” *Computers and Electrical Engineering*, vol. 100, p. 107997, May 2022, doi:10.1016/j.compeleceng.2022.107997.

[10] B. Nagajayanthi, “Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective,” Wireless Personal Communications, Nov. 2021, doi:10.1007/s11277-021-09308-z.

[11] S. Graziani and M. G. Xibilia, “Innovative Topologies and Algorithms for Neural Networks,” Future Internet, vol. 12, no. 7, p. 117, Jul. 2020, doi:10.3390/fi12070117.

[12] B. Patel and P. Shah, “Operating system support, protocol stack with key concerns and testbed facilities for IoT: A case study perspective,” Journal of King Saud University - Computer and Information Sciences, Jan. 2021, doi:10.1016/j.jksuci.2021.01.002.

[13] S. Mahmoodi Khaniabadi, A. Javadpour, M. Gheisari, W. Zhang, Y. Liu, and A. K. Sangaiah, “An intelligent sustainable efficient transmission internet protocol to switch between User Datagram Protocol and Transmission Control Protocol in IoT computing,” *Expert Systems*, Sep. 2022, doi:10.1111/exsy.13129.

[14] W. Bekri, T. Layeb, R. Jmal, and L. Fourati, “Intelligent IoT Systems: security issues, attacks, and countermeasures,” 2022 International Wireless Communications and Mobile Computing (IWCMC), May 2022, doi:10.1109/iwcmc55113.2022.9825120.

[15] B. B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, “Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers,” Computers & Electrical Engineering, vol. 98, p. 107726, Mar. 2022, doi:10.1016/j.compeleceng.2022.107726.

[16] K. O. Stanley and R. Miikkulainen, “Evolving Neural Networks through Augmenting Topologies,” Evolutionary Computation, vol. 10, no. 2, pp. 99–127, Jun. 2002, doi:10.1162/106365602320169811.

[17] M. Y. Ibrahim, R. Sridhar, T. V. Geetha, and S. S. Deepika, “Advances in Neuroevolution through Augmenting Topologies – A Case Study,” 2019 11th International Conference on Advanced Computing (ICoAC), Dec. 2019, doi:10.1109/icoac48765.2019.246825

[18] A. Behjat, N. Maurer, S. Chidambaran, and S. Chowdhury, “Adaptive Neuroevolution with Genetic Operator Control and Two-Way Complexity Variation,” IEEE Transactions on Artificial Intelligence, pp. 1–14, 2022, doi:10.1109/tai.2022.3214181.

[19] J. Hohenheim, M. Fischler, S. Zarubica, and J. Stucki, “Combining Neuro-Evolution of Augmenting Topologies with Convolutional Neural Networks,” arXiv (Cornell University), Oct. 2022, doi:10.48550/arxiv.2211.16978.

[20] H. Yang and Y. Kim, “Design and Implementation of Fast Fault Detection in Cloud Infrastructure for Containerized IoT Services,” Sensors, vol. 20, no. 16, p. 4592, Aug. 2020, doi:10.3390/s20164592.

[21] M. Rodríguez, Á. Alesanco, L. Mehavilla, and J. García, “Evaluation of Machine Learning Techniques for Traffic Flow-Based Intrusion Detection,” *Sensors*, vol. 22, no. 23, p. 9326, Jan. 2022, doi:10.3390/s22239326.

[22] S. Kumar, S. Gupta, and S. Arora, “Research Trends in Network-Based Intrusion Detection Systems: A Review,” *IEEE Access*, vol. 9, pp. 157761–157779, 2021, doi:10.1109/access.2021.3129775.

[23] Y. Mardenov, A. Adamova, T. Zhukabayeva, and M. Othman, “Enhancing Fault Detection in Wireless Sensor Networks Through Support Vector Machines: A Comprehensive Study,” *Journal of Robotics and Control (JRC)*, vol. 4, no.6, pp. 868-877, 2023. doi:10.18196/jrc.v4i6.20216

[24] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges,” Computers & Security, vol. 28, no. 1–2, pp. 18–28, Feb. 2009, doi:10.1016/j.cose.2008.08.003.

[25] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: A survey,” Journal of Network and Computer Applications, vol. 77, pp. 18–47, Jan. 2017, doi:10.1016/j.jnca.2016.10.015.

[26] Kotenko, V. Desnitsky, and E. Novikova, “Defect Detection in Industrial IoT-based Machines: Case of Small Training Dataset,” 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Nov. 2023, doi:10.1109/iotais60147.2023.10346064.

[27] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, “Survey of Machine Learning based intrusion detection methods for Internet of Medical Things,” Applied Soft Computing, vol. 140, p. 110227, Jun. 2023, doi:10.1016/j.asoc.2023.110227.

[28] A. Jamalipour and S. Murali, “A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey,” IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9444–9466, Jun. 2022, doi:10.1109/jiot.2021.3126811.

[29] P. Gupta, L. Yadav, and D. S. Tomar, “Internet of Things: A Survey on Fused Machine Learning-Based Intrusion Detection Approaches,” Advanced Machine Intelligence and Signal Processing, pp. 147–161, 2022, doi:10.1007/978-981-19-0840-8_11.

[30] M. V. R. Sarobin, P. Rukmani, and E. A. M. Anita, “Machine Learning-Based Intrusion Detection for Internet of Things Network Traffic,” Handbook of Research of Internet of Things and Cyber-Physical Systems, pp. 315–335, Mar. 2022, doi:10.1201/9781003277323-17.