Vietnam Journal of Science and Technology ***61*** *(6) (2023) 1089-1101*

doi:10.15625/2525-2518/18233

A novel IDS system based on Hedge algebras to detect DDOS attacks in IoT systems

Hoang Trong Minh[1], Vu Nhu Lan[2], Nguyen Nam Hoang[3, *]

[1]*Posts and Telecoms Institute of Technology/Telecoms Faculty, 122 Hoang Quoc Viet Street, Cau Giay district, Ha Noi, Viet Nam*

[2]*Thang Long University/ Informatics Faculty, Nghiem Xuan Yem Street, Hoang Mai district, Ha Noi, Viet Nam*

[3]*University of Engineering and Technology, Vietnam National University Hanoi, 144 Xuan Thuy Street, Cau Giay district, Ha Noi, Viet Nam*

[*]Emails: *hoangnn@vnu.edu.vn*

Received: 7 April 2023; Accepted for publication: 7 October 2023

Abstract. In recent years, we have experienced rapid and beneficial development of IoT solutions throughout all aspects of life. In addition to the apparent advantages, the increased number and variety of devices have resulted in more security issues. The DDoS attack, which originates from a broad range of sources and is a significant challenge for IoT systems, is one of the most prevalent but devastating attacks. Because IoT devices are typically simple and have few computing resources, it puts them at risk of being infected and attacked. IDS intrusion detection systems are considered superior protection against DDoS attacks. Therefore, the IDS system attracts many researchers and implements intelligent techniques such as machine learning and fuzzy logic to detect these DDoS attacks quickly and precisely. Along with the approach of intelligent computation, this study presents a novel technique for detecting DDoS attacks based on hedge algebra, which has never been implemented on IDS systems. We use the PSO swarm optimization algorithm to optimize the proposed model's parameters for performance optimization. Our experiment carried out on the IoT-23 dataset shows that the proposed model's accuracy and performance for DDoS attack detection are better than those proposed by other previous research.

Keywords: Internet of things, intrusion detection system, DDOS, Hedge algebra, PSO algorithm.

Classification numbers: 2.4.2, 2.4.4, 5.2.1.

1. INTRODUCTION

With widespread uses, IoT technologies have benefited society. Recent technologies like 5G have made installing new IoT solutions easier and exponentially expanding IoT devices [1]. The wide reach and variety of devices of IoT applications have produced new security issues. With intelligent computing, threats and attacks are getting more sophisticated, fatal, and devastating. Unfortunately, most simple IoT devices with limited computational resources have been attacked. The factors above have produced new security issues in this industry [2]. Classic attacks like DDoS threaten resource network availability. The enormous and diversified number of IoT devices with distributed operating systems are at risk of attacks. Many geographically

dispersed hacked systems perform DDoS attacks, which have been found for many application domains. Thus, DDoS in IoT applications poses a significant, unforeseen threat and has been studied extensively [3, 4].

Intrusion detection systems (IDSs) are attractive technologies that aim to locate and detect IoT cyberattacks as the first barrier to defense. IDS systems are usually signature-, anomaly-, or hybrid-based [5]. While observing network packets, a signature-based IDS compares them to a database of attack signatures to detect strange patterns. In contrast, anomaly-based intrusion detection systems can detect unknown suspicious behavior. Therefore, anomaly detection techniques are applied in many contexts and research disciplines [6]. Modern DDoS attacks use intelligent technologies to beat statistical probabilities or static threshold solutions, making them dynamic and intelligent. Thus, the current IDS system detects anomalies using artificial neural networks, deep neural networks, Bayesian networks, evolutionary algorithms, fuzzy logic, and Boltzmann Machine [7 - 9]. Data-driven techniques like IDS models using deep learning neural networks are often precise and adaptable to environmental changes [10]. Unfortunately, these networks must optimize several architectural aspects.

Decisions are complicated due to inexperience and expert advice. However, heuristics and fuzzy methods are often utilized to reduce complexity problems [11, 12]. To achieve outstanding results, the right rules must be determined. The IDS-based hedge algebra model, a novel DDoS detection technique for IoT contexts, addresses this challenge. The particle swarm optimization (PSO) algorithm optimizes the proposed system's parameters, correcting subjective errors of the expert's rule set. DDoS attack detection rates up to 99.99 % were achieved utilizing our proposed approach on the IOT-23 attack dataset. Significant contributions of this study include:

- Design a new model for IDS based on hedge algebra to detect DDoS attacks for IoT networks.
- Experimentally verify and compare the results with other proposals to highlight the proposal's advantages.

The paper is organized as follows. The next section presents the related work. The background of the main theoretical issues in our proposed model is briefly described in section 3. Our proposed model will be presented in Section 4. Experiment results on the IoT-23 dataset and related discussions are presented in Section 5. The conclusion and plan for our future investigations are presented in the final section.

2. RELATED WORK

IDS systems analyze traffic patterns to detect sudden and unexpected changes in traffic or other network traffic scenarios [13]. These anomalies usually come from known or undetected computer network and service security threats. Classifications using statistical approaches can increase inaccuracy. The threshold between normal and abnormal activity may be unclear; thus, a small change in monitored traffic may increase false positives and degrade attack detection accuracy.

BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, IoT-23, and IoT-DS1 are popular IDS evaluation datasets [14]. IoT-23 comprises 20 malware captures from IoT devices and three benign traffic captures [15]. The Stratosphere Laboratory, AIC team, FEL, CTU University, and Czech Republic recorded IoT network traffic. Several studies have investigated machine learning, deep learning, and fuzzy logic attack detection algorithms on the IoT-23 dataset [16–18]. In [16], the authors tested several Artificial Neural Network techniques, including Random Forest (RF), Native Bayes (NB), and Multi-Layer Perceptron (MLP), and the Random Forest

algorithm performed best with 99.5 % accuracy. A model for anomaly-based intrusion detection in IoT networks proposed in [17] used a CNN and GRU to categorize IoT network data with 99.5 % accuracy. In [18], the authors proposed a CNN-based anomaly detection model with 99.82 % detection accuracy, better than previous IDS-based CNN models. The previous studies suggest that detection accuracy depends on various parameters and data processing methods.

It is worth noting that several IDSs using fuzzy logic offer several advantages to handling crisp boundary problems caused by unpredictable and uncertain conditions [19, 20]. However, we found that no fuzzy logic usage models have yet been evaluated on the IoT-23 dataset. In our previous works [21, 22], we proposed a Fuzzy Inference System-based IDS that enabled more efficient detection of DDoS attacks in wireless sensor networks than threshold approaches. However, the results are based solely on numerical simulations and not on specific data sets. Following the fuzzy logic approach, to formalize the order-based semantics of the words in the term-domain of linguistic variables, authors in [23] developed hedge algebra (HA), which can be used in a variety of application domains, such as information processing or intelligent control [24] [25]. Hedge algebra's core element is that they capture the nature of fuzzy information by quantifying the qualitative semantics of linguistic concepts. Fuzziness measure, fuzziness interval of terms, and semantically quantifying mapping (SQM) are the three quantitative features of HA (SQM). SQMs provide for the execution of a complete description and the logical and coherent demonstration of a rule set model and approximation inference process. Hedge algebra is used to model the domain of linguistic variables through quantitative semantics. Hence, the fuzzy rule system becomes the quantitative semantic rule system. Therefore, the inference problem becomes an interpolation problem with computational methods of low complexity. This paper will use the hedge algebra method applied to the IDS system to detect DDoS attacks in IoT systems. The experimental results on the IoT-23 dataset show the superior performance of our proposal compared with the previous proposals.

3. BACKGROUND

3.1. Hedge Algebra Overview

Following the definitions and properties of hedge algebras in [23], Hedge Algebra is a mathematical structure that has the order of collection of linguistic items. Several prominent features are listed below.

Definition 1. Hedge algebras of the linguistic variable **X** can be represented as an algebraic structure, the set of five components **AX = (X, G, C, H, ≤)**, where X is a set of values of a linguistic domain regarded as a POSET (partially ordered set); **G** is a set of generators, which are designed as primary terms (semantic tendency expressions) denoted by **c-** and **c+, G = {c-, c+},c- ≤ c+; C** is a set of constants, **C = {0, W, 1}**, (zero, neutral and unit elements, respectively); **H** is a set of urinary operations, **H = H- ∪ H+, H-** and **H+** is two artificial hedges which are generated from **x** by using operations in **H; ≤** is a partial ordering relation on **X**.

Definition 2. Denote ***fm*** is a fuzzy measurement of an element **x** in **X**, and ***μ(h)*** is a fuzziness measure in the **H** domain. [$\mathbf{X} \rightarrow [0, 1], \forall h \in \mathbf{H}$] has the properties as below.

$$\mathbf{fm}(\mathbf{c}^+) + \mathbf{fm}(\mathbf{c}^-) = \mathbf{1} \ \#(\mathbf{1})$$

$$\sum\nolimits_{\mathbf{heH}} \mathbf{fm}(\mathbf{hx}) = \mathbf{fm}(\mathbf{x}), \forall \mathbf{x} \in \mathbf{X} \#(\mathbf{2})$$

$$\mathbf{fm}(\mathbf{0}) = \mathbf{fm}(\mathbf{W}) = \mathbf{fm}(\mathbf{1}) = \mathbf{0} \ \#(\mathbf{3})$$

$$\mu(h) = \frac{fm(hx)}{fm(x)} = \frac{fm(hy)}{fm(y)}, \forall x, y \in H, h \in H \ \#(4)$$

$$\sum_{i=-q, j\neq 0}^{p} fm(hx) = fm(x) \ \#(5)$$

$$fm(x) = fm(h_n h_{n-1} h_1 c) = \mu(h_n)\mu(h_{n-1})\mu(h_1)c \#(6)$$

$$\sum_{i=-1}^{q} fm(h_i) = \alpha, \sum_{i=-1}^{p} fm(h_i) = \beta, \alpha + \beta = 1, \alpha, \beta > 0 \ \#(7)$$

Definition 3. The Semantically Quantifying Mapping (SQM) in **HA** is a function (v) used to transform a linguistic variable into real linguistic values $v: X \to [0, 1], \forall h \in H$.

$$v(W) = \theta = fm(c^-) \#(8)$$

$$v(c^-) = q - a.fm(c^-) = b.fm(c^-) \#(9)$$

$$v(c^+) = q + a.fm(c^+) = 1 - b.fm(c^+) \#(10)$$

3.2. Particle Swarm Optimization

Particle Swarm Optimization (PSO) models its behavior after animals' swarming or flocking patterns [19]. It is very appealing because the simple conceptual framework and the analogy of birds flocking facilitated conceptual visualization of the search process. The basic PSO algorithm is shown in the pseudo-code below.

Start

1. Begin by randomly generating the positions and velocities of the particles to initialize the population.
2. Assign the best fitness value to each particle's current position to establish their initial best positions.
3. Designate the position of the particle possessing the highest fitness value as the global best position.

   Loop

   - Assess the fitness value of individual particles by utilizing the objective function, which represents the optimization problem at hand.
   - If the fitness value of a particle's current position surpasses its best position, proceed to revise the particle's best position accordingly.
   - If the fitness value associated with the best position of each particle surpasses the global best position, proceed to update the global best position.
   - Revise the velocity of each particle based on its present velocity, best position, and the global best position.
   - Adjust the position of each particle using its current position and the newly updated velocity

   Until The condition for termination is satisfied.
4. Provide the optimized solution by returning to the best global position.

End.

PSO has particles that make up its population, called a swarm. Each particle is moved from one location to another over mutation. This mutation is performed directly, moving each particle from its previous location to a new, better location. The PSO algorithm has several advantages that make it an attractive optimization algorithm [26]:

- PSO is easy to set up and code.
- PSO is controlled by only three parameters (inertia weight, cognitive ratio, and social ratio). A slight change in any of these three controlling parameters produces a difference in performance.
- PSO is adaptable and can be combined with other optimization algorithms.

4. THE PROPOSED MODEL

4.1. Preprocessing the Dataset IoT-23

The IoT-23 dataset divides attacks into 16 categories, including 15 malicious and one secure layer. Preprocessed data require training, validation, and testing. Segmentation ensures equal training, validation, and testing samples from each processing stage. Data processing extracts network features from network traffic for training and evaluating models. These features are taken from the little IoT-23 dataset's conn.log.labeled file and exported to CSV. The model removes local network details like stream ID, source IP address, destination IP address, and timestamp because it is not intended for IoT networks. The dataset index features are binary-coded. Instead of 0, NaN values are used. Normalizing the featured columns to [-1 1] eliminates large values and accelerates processing. Additionally, the feature selection method improves model accuracy and minimizes noise. Principal components analysis (PCA) uses to this aim to reduce complexity, overcome limitations in resources, and improve anomaly detection rate. After processing and reduction, we choose the dataset's secure (Benign) and DDoS patterns. This dataset has three sets: Training, Validating, and Testing. Training and Testing sets have equal sample sizes. Training and Validating sets have 80/20 samples. The training set is a standard space for the calculations of the following steps. Figure 1 shows the data processing system.

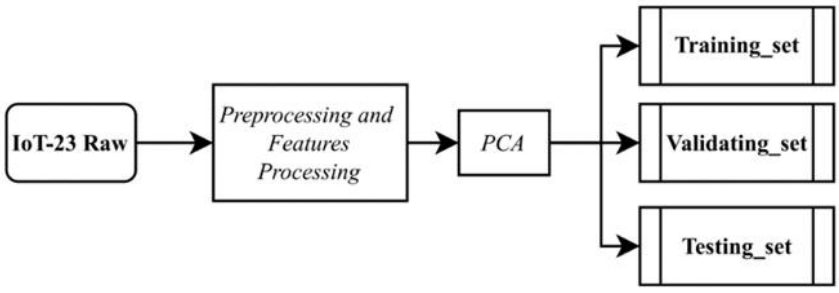

Figure 1. Processing the IoT-23 data set.

4.2. The proposed model

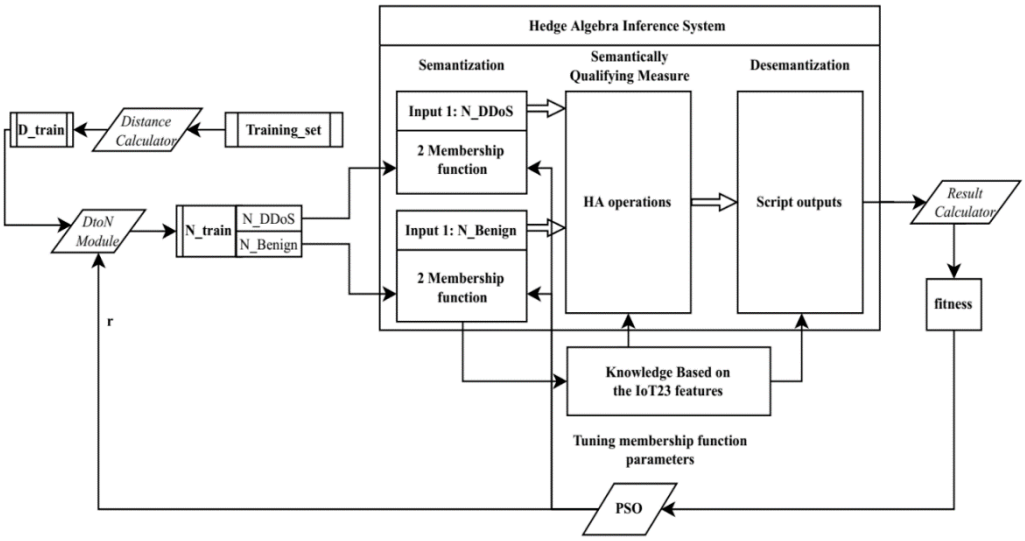

Figure 2. The Proposed Model.

The main components of the proposed model are illustrated in Figure 3. The input training dataset is calculated based on the neighbor data distance to filter out training data for the distance matrix D-train. The *DtoN* module represents the transformation between the distance matrix *D,* and the density matrix *N*. *D* is the matrix of the distance of each point to the remaining points, and *N* is the two-column set containing the number of DDoS points and the number of benign points whose distance from each data point is less than or equal to radius *(r)*, where *r* is the optimal radius from any interesting data point in the data space to other data points. This yields the fuzzy data sets N-DDOS (x_1) and N-Benign (x_2). These data sets are denoted as *L* (Low) and *H* (High) density metrics. The script output (*y*) has presented the probability of DDoS attacks such as *LA* (Low attack), *MA* (Medium Attack), and *HA* (High Attack).

The Semantilization module is responsible for transforming the linguistic variable domain [a b] into their respective linguistic semantics value domain [a_s b_s] over the semantization process. If a_s = 0 and b_s = 1, we have a linear sematization process. If it is not, we have a non-linear sematization process. Denote x is a linguistic variable and (xh) semantic value, and we describe the linear sematization process and non-linear sematization process below.

Case 1: Linear sematization process

$$x_h = \frac{x-a}{b-a}, x = a + (b-a)x_h \#(11)$$

Case 2: Non-linear sematization process.

$$x_h = f(x, sp), x = g(x_h, dp) \#(12)$$

in which, sp is the non-linear semantic parameter, $sp \in [0\ 1]$; dp is the non-linear desemantization parameter, $dp \in [0\ 1]$. The function $f(.)$ is continuous, covariate, and satisfies the condition below,

$$f(x_s, sp) = x_s + sp \times x_s(1-x_s),$$
$$0 \le f(x_s, sp) \le 1, a \le g(x, dp) \le b, \#(13)$$
$$g(x = a, dp) = a, g(x = b, db) = b\ \#$$

Note that semantic-based ordered structure is the key point of the transform process as defined in Definition 1. Assume $x_i, x_j \in X, H(x_i) < H(x_j)$, denote the qualitative linguistic value $H(x_*)$ we have $H(x_i) \le H(x_*) \le H(x_j)$.

Hence, the close degree η_1, η_2 is calculated as

$$\eta_i = \frac{H(x_j) - H(x_*)}{H(x_j) - H(x_i)}; \eta_j = \frac{H(x_*) - H(x_i)}{H(x_j) - H(x_i)} \#(14)$$

where, $0 \le \eta_i, \eta_j \le 1, \eta_i + \eta_j = 1$.

The SQM transforms linguistic semantic values into real values by algebras operators (4)-(6). The rules are illustrated as

$$IF\ x_1 = L\ and\ x_2 = L\ THEN\ y = LA$$
$$IF\ x_1 = L\ and\ x_2 = H\ THEN\ y = HA \#(15)$$
$$IF\ x_1 = H\ and\ x_2 = L\ THEN\ y = MA$$
$$IF\ x_1 = H\ and\ x_2 = H\ THEN\ y = HA$$

The hedge algebra inference system uses piece-wise linear operators. The mathematics description of the model is expressed as.

$$y_k = \frac{\sum_{k-1}^{L} \prod_{i-1}^{n} \eta_k (f_i)_k \times \emptyset_k (x_1, .., x_n)(p_{1k}, \dots, p_{nk})}{\sum_{k-1}^{L} \prod_{i-1}^{n} \eta_k (f_i)_k} \#(16)$$

where the input set is $X, (x_1, x_2 ... x_n) \in X$; a rule set is R, $(1, 2, k ... M) \in R$; the parameters of the rule k^{th} is $(p_{1k}, p_{2k} ... p_{nk})$; $\varphi_k(.)$ is a linear function; f_i is the fuzzy element of a linguistic variable x_i ; the outcome value on the rule k^{th} is y_k.

From equations (7) (11) (12) (16), we construct a model that includes the linguistic domains and variables and their semantic structure elements. Instead of performing fuzzification and defuzzification as in fuzzy logic, we adopted a simple method termed semantization and desemantization.

According to the equation (8) (9) (10) (11), we have a set of semantic transformation equations as follows:

$$Lx_1 = \theta_1 \times (1 - \alpha_1)$$
$$Lx_2 = \theta_2 \times (1 - \alpha_2)$$
$$Hx_1 = \theta_1 + \alpha_1 \times (1 - \alpha_1)$$
$$Hx_2 = \theta_2 + \alpha_2 \times (1 - \alpha_2) \#(17)$$
$$LA = \theta + (1 - \alpha)$$
$$MA = \theta$$
$$HA = \theta + \alpha(1 - \alpha)$$

All input variables are classified as Low and High; output Scripts are denoted as Low Attack, Medium Attack, and High Attack; the hedge parameters are $(\theta_1, \alpha_1, \theta_2, \alpha_2, \theta, \alpha)$.

The PSO algorithm finds the optimal variables $(\theta_1, \alpha_1, \theta_2, \alpha_2, \theta, \alpha)$, r over the mean squared error (MSE) metric. The objective of the model is to use the PSO algorithm to find the optimal

membership function parameters of the two inputs and the optimal radius r so that the following cost function J is minimized:

$$J = \frac{1}{n}\sum_{i=0}^{n} F(x^i - y^i);\ finess^k = \frac{100}{J^k + 1} \#(18)$$

Where n the total number of samples of the test set, x^i the i^{th} sample in the test set, y^i is the sample's label, $F(x^i)$ is the predictive output of the model given the input is the i^{th} sample. The fitness value is used to feed into the PSO algorithm to update the position for each individual.

4.3. The core operations of the proposed model

The proposed model is operated by the initial phase and the optimization phase, as shown below.

Initiate phase. This phase aims to optimize the r parameter. The initial radius r is set randomly between 0, and the set D train is a value related to the input member function parameters. Four parameters represent each membership function of a trapezoidal function with two inputs (a,b,c,d). The encoding parameters for the PSO algorithm are (x,y,z): $a = x = y - z$; $b = x - y$; $c = x + y$; $d = x + y + z$.

Optimization phase. This phase is used to optimize the HA parameters of the proposed model. It is illustrated by the proposed algorithm below:

Function: Hedge algebra parameter optimization.

Input: IoT-23 dataset, encoded parameters.

Output: $(\theta_1,\alpha_1,\theta_2,\alpha_2,\theta,\alpha)$ parameters.

1. Calculate the D-train matrix from the training set.
2. For *i* = 1 to pop-size
3. Initialize position and velocity for individual *i*, *r*:= [0, *AvgD-train*] θ:= [0.25, 0.75], α:= [0.2, 0.8] θ1:= [0.25, 0.75], α1:= [0.2, 0.8] θ2:= [0.25, 0.75], α2:= [0.2, 0.8]
4. Calculation of Fitness score for individual *i.*
5. Update the maximum values of the individual *i* and the best values of the population.
6. End for
7. For *i* = 1 to *max* iterative
8. For *j* = 1 to *max* population size
9. Determine the individual *j's* velocity value. [*v*(*t* + 1) = *w*.*v*(*t*) + *c*1.*r*1.(*pbest*(*t*) - *x*(*t*)) + *c*2.*r*2.(*gbest*(*t*) - *x*(*t*))]
10. Update new location for individual *j* *x*(*t* + 1) = *x*(*t*) + *v*(*t* + 1)
11. Recalculate fitness points for an individual *j*
12. Update the maximum values of the individual *j* and the best values of the population.
13. End for

14. End for
15. Choosing the best individual in the population is the optimal solution for the model.

End Function

5. EXPERIMENTAL RESULT

All IDS-based HA experiments are conducted using the Matlab tool with the practical dataset IoT-23. The parameters of the PSO algorithm used in our simulation are shown in Table 1.

Table 1. The Parameters of the PSO Algorithm.

Parameters	Values
Population	50
Constriction factor	$c_1 = 1, c_2 = 2$
Inertia factor	1
Inertia factor reduction rate	0.99
Number of rounds	50

The system performance is evaluated in terms of accuracy, precision, recall, F1-score, and FPR (False Positive Rate). We denote TP as the true positive, FP as the false positive, and FN as the false negative. We have

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \#(19)$$

$$Precision = \frac{TP}{TP + FP} \#(20)$$

$$Recall = \frac{TP}{TP + FN} \#(21)$$

$$F1 = 2\frac{Precision \times Recall}{Precision + Recall} \#(22)$$

$$FPR = \frac{FP}{FP + TN} \#(23)$$

First, we evaluate the convergence speed of the PSO algorithm in the optimization problem of membership input parameters for the two boundaries *acc* and *val*. As shown in Figure 3 below, several loops (≤10 rounds) have resulted in convergence and stability. This shows that the time complexity of the algorithm is small and efficient.

To examine the efficacy of the model with a varied sample size and a number of features, we apply the IoT-23 dataset to the attack detection model in the following manner. Use sampling at random to separate the test data sets (2500 samples and 5000 samples). We intend to conduct experiments with a modest sample size to enable IDS systems that can be deployed at the network's edge, where computational resources are constrained.

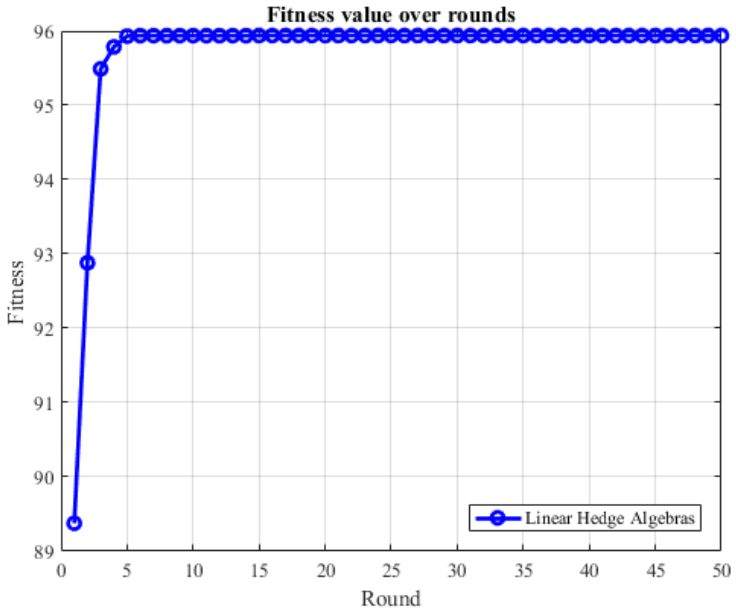

Figure 3. The convergence time of the PSO algorithm.

Using the PCA method, we reduce the original IoT-23 dataset with varying numbers of features (10 features, 23 features, and f32 features). Due to the minimal number of computational spatial dimensions, the small number of features reduces the computational complexity of a training model. We compare the efficiency of non-linear and linear semantics schemes in Figure 4.

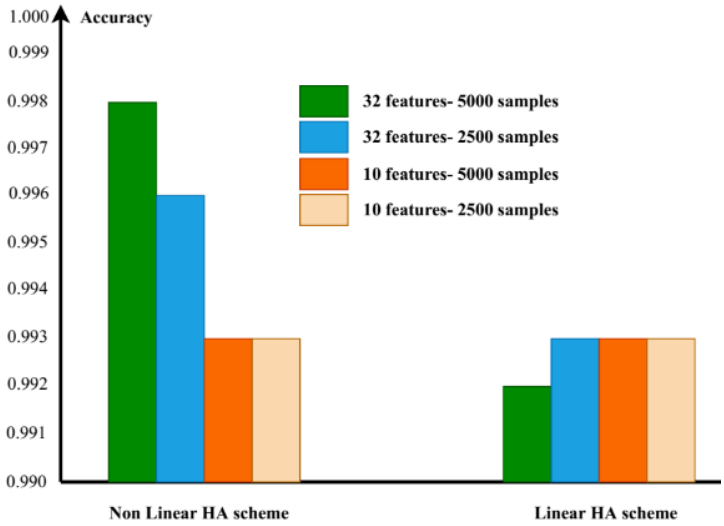

Figure 4. The accuracy values on different schemes.

In Figure 4, two hedge algebra schemes have been evaluated using datasets that have been reduced in dimensionality at various levels to demonstrate the accuracy and applicability of the proposed model. The non-linear approach provides the utmost accuracy for datasets with a large

number of samples, while the accuracy decreases with the number of samples. In contrast, the linear semantic approach provides relatively stable attack detection accuracy results.

Table 2. Experimental Results.

Features	Samples	Acc	Pre	Recall	FPR	F1
10	5000	0.996	0.997	0.995	0.0028	0.996
10	2500	0.994	0.993	0.995	0.0063	0.994
23	5000	0.996	0.996	0.996	0.0032	0.996
23	2500	0.995	0.912	1	0.0008	0.995
32	5000	0.997	0.996	0.999	0.0039	0.997
32	2500	0.993	0.997	1	0.0126	0.993
32	Full	0.998	1	0.995	0	0.998

The test results on different sample sets with a different number of features show the adaptability of the non-linear scheme better than the linear. The results show that the DDoS attack detection accuracy of the non-linear semantic scheme is higher than that of the linear semantic scheme. The results of the performance evaluation of the model with our tests are presented in Table 2. We recognize that the attack detection accuracy is not significantly reduced with a small sample size and a small number of features.

To evaluate the effectiveness of the proposal, we compared the performance results of the proposed model with those of other proposals (Table 3). The results showed that the proposed model gave reasonable results. Although the results of DDoS attack detection accuracy in our proposed model are not outstanding, our model can work on small data sets with an accuracy of up to 99 %. Hence, a significant contribution of our proposed model is that we have used a small number of samples in the dataset and still have a higher attack detection rate than it can be deployed in limited resource devices.

Table 3. A Comparison of Performance Metrics.

Refers	Model	Acc	Pre	Recall	FPR	F1
[16]	ANN	0.995	-	-	-	-
[17]	CNN	-	0.999	0.999	-	0.999
[18]	CNN	0.999	0.995	0.998	-	0.999
Ours	*HA*	0.998	1	0.995	0.0001	0.998

6. CONCLUSIONS

This paper proposes a novel DDoS attack detection model for IDS systems in edge computing. Specifically, the rule systems are processed by the hedging algebra method, and the input variable member functions are optimized through the PSO algorithm. Our proposed model using fuzzy approaches of input parameters for data points in the IoT-23 dataset has resulted in false positive avoidance and optimal classification by the PSO algorithm. Hence, our proposed model can bring a good DDoS detection rate. Moreover, the proposed model combined with dimensionality reduction and data division techniques shows attack detection as high as 99 % with varied small data sets. Therefore, deploying the IDS system on the edge device will be

favorable and greatly reduce the harmful effects of attacks on IoT applications. We will continue to deploy our model on practical devices in future work.

Acknowledgements. The research funding from the Posts and Telecommunications Institute of Technology (PTIT) was acknowledged.

CRediT authorship contribution statement. Trong-Minh Hoang: Conceived and designed the algorithms; Nhu-Lan Vu: Performed the experiments; Nam-Hoang Nguyen: analyzed and interpreted the data; wrote the paper.

Declaration of competing interest. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

1. Khanna A. and Kaur S. - Internet of things (IoT), applications and challenges: a comprehensive review, Wireless Personal Communications **114** (2) (2020) 1687-176.
2. Jayashree M., Mishra S., Patra S., Pati B., and Panigrahi C. R. - IoT security, challenges, and solutions: a review, Progress in Advanced Computing and Intelligent Engineering, 2021, pp. 493-504.
3. Ruchi V. and Jain A. K. - A survey of DdoS attacking techniques and defense mechanisms in the IoT network, Telecommunication systems **73** (1) (2020) 3-25.
4. Mohammed S. M., Rathore S., and Park J. H. - Distributed denial of service attacks and its defenses in IoT: a survey, The Journal of Supercomputing **76** (7) (2020) 5320-5363.
5. Markus R., Wunderlich S., Scheuring D., Landes D., and Hotho A. - A survey of network-based intrusion detection data sets, Computers and Security **86** (2019) 147-167.
6. Gilberto F., Rodrigues J., Carvalho L. F., Al-Muhtadi J. F., and Proenca M. L. - A comprehensive survey on network anomaly detection, Telecommunication Systems **70** (3) (2019) 447-489.
7. Ankit T., and Lohiya R. - A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges, Archives of Computational Methods in Engineering **28** (4) (2021) 3211-3243.
8. Mendonca P., Robson V., Teodoro A., Rosa R. L., Saadi M., Melgarejo D. C., Nardelli P., and Rodrıguez D. R. - Intrusion detection system based on fast hierarchical deep convolutional neural network, IEEE Access **9** (2021) 61024-61034.
9. Rasheed A., and Alsmadi I. - Machine learning approaches to IoT security: A systematic literature review, Internet of Things **14** (2021) 100365.
10. Mohammed M., and Al-sultan G. A. - Network intrusion detection system using deep neural networks, In Journal of Physics: Conference Series **1804** (1) (2021) 012138.
11. Amjad A., Sampalli S., and Bodorik P. - DdoS detection system: Using a set of classification algorithms controlled by the fuzzy logic system in Apache spark, IEEE Transactions on Network and Service Management **16** (3) (2019) 936-949.
12. Mohammad M., and Khezri H. - Towards fuzzy anomaly detection-based security: a comprehensive review, Fuzzy Optimization and Decision Making **20** (1) (2021) 1-49.
13. Tohid J., Masdari M., Ghaffari A., and Majidzadeh K. - A survey and classification of the security anomaly detection mechanisms in software-defined networks, Cluster Computing **24** (2) (2021) 1235-1253.

14. Pajouh H., Dehghantanha H. A., Parizi R. M., Aledhari M., and Karimipour H. - A survey on Internet of things security: Requirements, challenges, and solutions. Internet of Things **14** (2021) 100129.
15. Parmisano A., Garcia S., and Erquiaga M. J. - A labeled dataset with malicious and benign IoT network traffic. https://www.stratosphereips.org/datasets-IoT-23.
16. Stoian N. A. - Machine Learning for anomaly detection in IoT networks: Malware analysis on the IoT-23 data set. Bachelor's thesis, University of Twente, 2020.
17. Imtiaz U., Ullah A., and Sajjad M. - Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks, Internet of Things **2** (3) (2021) 428-448.
18. Imtiaz U., and Mahmoud Q. H. - Design and development of a deep learning-based model for anomaly detection in IoT networks, IEEE Access **9** (2021) 103906-103926.
19. Rameem Z. S., and Chishti M. A. - A generic and lightweight security mechanism for detecting malicious behavior in the uncertain Internet of Things using fuzzy logic and fog-based approach, Neural Computing and Applications **34** (9) (2022) 6927-6952.
20. Mohammad A., Al-Sawwa J., and Alkasassbeh M. - Anomaly-based intrusion detection system using fuzzy logic, In 2021 IEEE International Conference on Information Technology (ICIT), 2021, pp. 290-295.
21. Nguyen V. T., Nguyen T. X., Hoang T. M., and Vu N. L. - A new anomaly traffic detection based on a fuzzy logic approach in wireless sensor networks, In Proceedings of the Tenth International Symposium on Information and Communication Technology, 2019, pp. 205-209.
22. Hoang T. M. - A Study on Anomaly Data Traffic Detection Method for Wireless Sensor Networks, In The International Conference on Intelligent Systems & Networks, 2021, pp. 429-436.
23. Ho N. C., and Wechsler W. - Hedge algebras: an algebraic approach to the structure of sets of linguistic truth values, Fuzzy sets and systems **35** (3) (1990) 281-293.
24. Ngo H. H., Ho N. C., and Nguyen V. Q. - Multichannel image contrast enhancement based on linguistic rule-based intensification, Applied Soft Computing **76** (2019) 744-762.
25. Hoang T., Nguyen T., Vu N., and Nguyen H. - A Novel Fuzzy Inference System Based on Hedge Algebras to Enhance Energy Efficiency in Wireless Sensor Networks, 2018 IEEE 3rd International Conference on Communication and Information Systems (ICCIS), 2018, pp. 73-78.
26. Shami T. M., El-Saleh A. A., Alswaitti M., Al-Tashi Q., Summakieh M. A., and Mirjalili S. - Particle Swarm Optimization: A Comprehensive Survey, In IEEE Access **10** (2022) 10031-10061.