information

MDPI

Article

An Accurate Detection Approach for IoT Botnet Attacks Using Interpolation Reasoning Method

Mohammad Almseidin [1,*,†] and Mouhammd Alkasassbeh [2,†]

[1] Department of Computer Science, Aqaba University of Technology, Aqaba 11191, Jordan;
[2] Department of Computer Science, Princess Sumaya University for Technology, Amman 11941, Jordan; m.alkasassbeh@psut.edu.jo
* Correspondence: msoudi@aut.edu.jo or alsaudi@iit.uni-miskolc.hu
† These authors contributed equally to this work.

Abstract: Nowadays, the rapid growth of technology delivers many new concepts and notations that aim to increase the efficiency and comfort of human life. One of these techniques is the Internet of Things (IoT). The IoT has been used to achieve efficient operation management, cost-effective operations, better business opportunities, etc. However, there are many challenges facing implementing an IoT smart environment. The most critical challenge is protecting the IoT smart environment from different attacks. The IoT Botnet attacks are considered a serious challenge. The danger of this attack lies in that it could be used for several threatening commands. Therefore, the Botnet attacks could be implemented to perform the DDoS attacks, phishing attacks, spamming, and other attack scenarios. This paper has introduced a detection approach against the IoT Botnet attacks using the interpolation reasoning method. The suggested detection approach was implemented using the interpolation reasoning method instead of the classical reasoning methods to handle the knowledge base issues and reduce the size of the detection fuzzy rules. The suggested detection approach was designed, tested, and evaluated using an open-source benchmark IoT Botnet attacks dataset. The implemented experiments show that the suggested detection approach was able to detect the IoT Botnet attacks effectively with a 96.4% detection rate. Furthermore, the obtained results were compared with other literature results; the accomplished comparison showed that the suggested method is a rivalry with other methods, and it effectively reduced the false positive rate and interpolated the IoT Botnet attacks alerts even in case of a sparse rule base.

Keywords: IoT environment; botnet attacks; interpolation reasoning methods; intrusion datasets

check for updates

Citation: Almseidin, M.; Alkasassbeh, M. An Accurate Detection Approach for IoT Botnet Attacks Using Interpolation Reasoning Method. *Information* **2022**, *13*, 300. https://doi.org/10.3390/info13060300

Academic Editor: Willy Susilo

Received: 25 April 2022
Accepted: 13 June 2022
Published: 14 June 2022

1. Introduction

The notion of the Internet of Things (IoT) has grown into solutions for a wide range of applications, including smart urban, manufacturing, medical services, and traffic control. The goal of adopting the Internet of Things concept is to improve humanity in terms of productivity and convenience. Thanks to the Internet of Things technology, machine-to-machine communication is now possible through an Internet connection. Many devices may be linked together and share information as a connected network. These gadgets function as "objects" that can reflect data from their surroundings. According to [1], IoT networks will connect approximately one trillion IP addresses or gadgets to the Internet. That is to say, Internet of Things (IoT) technologies are quickly expanding in several aspects of human existence. Any IoT-enabled environment has a variety of sensors that work together to accomplish various activities. Several heterogeneous devices are connected in the Internet of Things (IoT) ecosystem via various wireless sensors. These sensors, in addition to IPv6, and wireless communication, provide a benefit in extending the IoT environment to service a wide range of application domains; according to [2], different levels of security may exist among the many devices in the IoT environment. Some IoT devices have little or no security built in. This issue might jeopardize the availability of the IoT-connected network and introduce security vulnerabilities. The secure IoT concept underpins the availability of smart environments [3].

As a result, protecting IoT-connected devices in smart environments using the IoT paradigm is a difficult task. Security, privacy, and any system vulnerabilities in IoT systems are all concerns that an environment built on IoT faces, and these difficulties can directly impact environment applications. Securing IoT networks is difficult, because they are vulnerable to a variety of attacks. Large Distributed Denial of Service (DDoS) attacks were launched against numerous IoT systems in the United States in 2016, and the IoT-BotNet attack damaged online services including PayPal and Netflix, according to al2020detection.

When it comes to protecting computers and networks from various sorts of cyber-attacks, the Intrusion Detection System (IDS) is an actual option. IDS may be classified as either a signature-based system or an anomaly-based system [4–7]. Traditional IDSs protect the network layer in IoT systems. A successful IoT environment should contain the following critical criteria: real-time network protection and traffic investigation and analysis, the ability to analyze network traffic with various layers in an IoT environment, and the ability to respond and handle various protocols in the IoT environment [1].

Typical IDS may not be suited for IoT environments because of the restricted CPU and storage capabilities of IoT devices as well as the particular protocols used [2,8]. As a result of the fast growth of attack strategies, such as IoT Botnets, and their various devices, securing the IoT environment is a constant problem. The major contributions of this research are summarized as follows:

- To design a detection method against the IoT Botnet attacks using the interpolation reasoning method.
- To discusses the main characteristics that influence IDS performance in the IoT environment.
- To identify how the interpolation reasoning method extends the binary decision to the continuous space. This feature might help protect the IoT environment while also delivering more accurate results.

The interpolation reasoning method could be applied where there is a lack of knowledge base. The interpolation reasoning method overcomes the lack of knowledge base by interpolation of the required conclusion, even if some observations appear and do not overlap with any of the detection rules.

The rest of paper is organized as follows: Section 2 presents recent works related to detect Botnet attacks within the IoT environment. Section 3 introduces the suggested detection approach in detail, which is followed by the experiments and results in Section 4. Finally, Section 5 concludes the paper.

2. Related Works

This section presents some recent related works to detect the IoT Botnet attacks within the IoT smart environment. It also briefly reviews the various methodologies and methods for applying machine learning algorithms to identify attacks.

Typical IDSs were used in the IoT environment to secure the network layer. Because of the increasing growth of IoT devices and their heterogeneous components, the next generation of IDSs must be able to cope with multiple IoT layers and protocols stacks. The Electronic Product Code (EPC) number was first established in 1999 at the Massachusetts Institute of Technology (MIT) [9]. This was the beginning of the IoT's core technology. The IoT layers are defined as follows by the Institute of Electrical and Electronics Engineers (IEEE): sensor layer, application layer, and data transmission and networking layer. As a result, IoT architecture may be a feasible solution for use in a variety of sectors.

Forestiero proposed in [10] an intrusion detection method using footprints in an IoT environment with a multi-agent algorithm. Within the testbed environment, devices and services were represented with dense vectors. The proposed method was able to map the sequence of digital footprints for a given device along with a real-valued vector. The vectors are mapped to mobile agents, each acting sequentially in a modified bio-inspired model.

The suggested model was able to predict the emergence of intelligent global behavior based on simple local motion rules observed by all agents in a 2D virtual space.

Pokhrel et al. in [11] proposed a mitigation model to detect the distributed denial of service attacks in the IoT environment. Different machine learning algorithms were performed, such as neural network and K nearest neighbor. The authors employed an IoT Botnet attacks dataset as a testbed environment. In addition, they performed attributes engineering and Synthetic Minority Oversampling Techniques (SMOTE) to construct the required mitigation models. Various performance parameters were recorded to compare the suggested mitigation methods, such as F1, recall, and detection rate. The obtained results demonstrated that the suggested mitigation methods recorded acceptable performance parameters using the SMOTE technique. According to the experiments, K nearest neighbor was more accurate in detecting the distributed denial of service attack in the IoT environment.

In [12], Khurma et al. were concerned about the heterogeneous devices in the IoT environment, which makes them a target for intruders. The lack of IoT standardization is considered a severe challenge in protecting the IoT environment from different attacks. The authors proposed a wrapper attributes selection method using the salp swarm algorithm and ant lion optimization techniques. The suggested method could be beneficial in reducing the high-dimensional attributes within the IoT environment. Therefore, the suggested method could reduce the attributes space and detect different types of intrusions by combining the salp swarm algorithm and ant lion optimization techniques and the IDS detection method. The experiments were carried out, and the results demonstrated that the suggested method could reduce the attributes space and detect intrusions in the IoT environment. Popoola et al. proposed in [13] an accurate deep learning-based approach that detects the IoT botnet attack by adapting several resampling techniques such as SMOTE. Using the SMOTE produced more samples to reach the class balance and handle the imbalance issue associated with the studied IoT Botnet attacks dataset. The deep recurrent neural network was learned from representing the attribute within the studied IoT Botnet attacks dataset to execute the required detection procedure. The authors proposed DRNN and SMOTE to train and test the suggested method. The results show that the suggested method could detect the IoT Botnet attacks within the studied dataset.

Ashraf et al. in [14] studied the effects of different types of intrusion, such as Mirai and BASHLITE intrusions, in the IoT smart cities environment. The authors suggested a detection approach using a statistical learning-based framework to detect the IoT Botnet attacks. The suggested approach was performed by capturing the expected behavior of IoT traffic and applying the statistical learning-based techniques to define a normal behavior baseline that could be used to define the abnormal behavior. The beta mixture technique was used to define the expected behavior baseline, and the deviation from the expected baseline was considered an abnormal alert. The performed experiments showed that the suggested approach was able to detect the IoT intrusions within the simulated environment.

Arrington et al. [15] suggested a Host Intrusion Detection System (HIDS) to identify aberrant behavior within the IoT environment to determine if the present IoT network behavior is normal or unhealthy; the suggested method was constructed using artificial immune systems. The suggested approach proved successful in detecting anomalous behavior within the simulated setting. It might also be readily verified. The following modules were used to implement the suggested framework: data collection and anomaly detection. These modules serve as signature-based intrusion detection systems. The data-collecting module sends capturing data to the detecting module from several layers.

The SNORT-IDS rule-based detection module was developed for the identification of anomalies. The suggested framework's strength is its capacity to aggregate traffic from various data sources. The suggested framework was put to the test in an information security lab that was powered by an Arduino board. The results of the experiments reveal that the proposed framework can identify abnormal traffic within linked IoT devices.

Nevertheless, one of the suggested framework's challenges is privacy, resulting from the detection modules thorough traffic inspection.

Research is still being performed to determine the best detection strategy for IoT networks. To detect DDoS in the IoT context, Drio et al. [16] updated the deep learning approach. They demonstrated a distributed IDS-based deep learning approach; in general, distributed IDS is well-suited to meet the needs of IoT systems. The deep learning algorithm's strength is that given enough training data and time, it may achieve a high accuracy rate; also, it is a self-taught algorithm. The suggested method outperformed centralized IDS-based deep learning in terms of accuracy. A benchmark NSL-KDD dataset was used to train the suggested technique. The authors tweaked the test-bed environment and compiled a dataset with 123 input variables. Studies have shown that the suggested method has a 96.5% detection rate.

Martin et al. [17] customized the unsupervised anomaly-IDS for the IoT paradigm. The Conditional Variational AutoEncoder is used in the planned anomaly-IDS (CVAE). The capability of the suggested anomaly-IDS to tolerate missing characteristics for partially finished training data was one of its strongest features. Even though it was an unsupervised approach, the suggested anomaly-IDS utilized the characteristics and the class labels. By utilizing class labels, anomaly-IDS deviations may be quickly and easily identified. Furthermore, the suggested IDS creates a single model from numerous training phases, which might save time in an IoT network. The NSL-KDD benchmark dataset was chosen as a test-bed environment. Experiments conducted in the test-bed environment reveal that the proposed anomaly-IDS can detect 23 different types of attacks.

Gracia et al. in [18] focused on detecting attacks in the Wireless Sensor Networks (WSNs) that serve the IoT smart environment. Various kinds of attacks can target WSNs, which directly impact the IoT smart environment. The suggested WSNs detection technique was developed from the support vector machine algorithm to identify multiple forms of attacks. The suggested WSNs detection technique is separated into two phases: the first is a signature-based IDS that functions as a detection engine for known threats. Intrusion-based criteria were used in the initial detection engine. The identification of abnormalities and unknown attacks is the second phase. The suggested detection method supports combining two detection engines (intrusion-rule based, such as SNORT and support vector machine) to obtain a greater detection accuracy. Midi et al. [19] offer a hybrid IoT-IDS architecture. The suggested knowledge-driven IDS is one of the first IDS in the IoT environment that can function with a wide range of devices and protocols. The main feature of the suggested IDS is that it allows for collaboration in security situations. According to the experimental study, the suggested IDS is efficient for identifying many forms of attacks within the IoT environment.

Prabavathy et al. in [20] suggested a unique fog computing IDS based on the Online Sequential Extreme Learning Machine (OS-ELM). The suggested IDS incorporates fog computing as a security solution within the IoT network. It was broken down into three stages. The first stage is intrusion detection at fog nodes, which employed the OS-ELM algorithm to identify various forms of intrusions. The second phase is the summarizing phase, in which the incursions from the first phase are received, and the next attacker's move is predicted. The NSL-KDD benchmark dataset was utilized to validate the proposed IDS validation approach. The suggested IDS was advertised as having a high detection rate and a quick reaction time.

A considerable number of devices might be linked to the deployed IDS in an IoT-based smart environment. To deal with the enormous number of linked nodes, Amouri et al. [21] suggested a two-stage NIDS, in which the first phase is known as the local detection phase. Exceptional sniffers are used in the local detection phase to capture existing network behavior and build a set of appropriately categorized records. The decision tree method was developed for the detection anomaly in the local detection phase. The second phase of the proposed NIDS is the global detection phase. The time-based profile for the IoT security status was generated using linear regression at the global detection stage. MANET was used to validate the proposed NIDS's validation approach, and the suggested NIDS was able to identify intrusions inside the test-bed environment.

The previously mentioned related works provide valuable efforts for implementing different techniques against the IoT Botnet attacks. However, these detection approaches are either implemented using non-IoT datasets or applied to a binary decision. Evaluating the detection approaches using non-IoT datasets that do not have the current IoT protocol, such as 6LowPAN and Zigbee, could lead to unrealistic results. This work has introduced a detection approach against the IoT Botnet attacks using the fuzzy interpolation reasoning method in response to these issues. Using the interpolation reasoning method instead of the classical reasoning methods avoids the need for complete fuzzy detection rules and overcomes the issue related to the binary decision and lack of knowledge base.

3. Botnet Detection Using Fuzzy-Based IoT

This part presents the complete architecture of the suggested fuzzy-based IoT detection approach along with the main features and implementation requirements.

3.1. Testbed Environment Perpetration

In the IoT smart environment, there are different IoT devices connected, such as computers, switches, camera systems, etc. The lack of standardization makes the IoT environment the desired victim for attackers. Attackers continuously improved their techniques to avoid any detection mechanisms. One of the most dangerous attacks that threatens the IoT environment is the Botnet attacks. The Botnet attack follows the strategy of the synchronized IoT connected devices that include victim devices [22]. Following this strategy, the intruders performed a bi-directional attack against the infected IoT devices using different commands and shells scripts [23]. The major strength of the Botnet attack is that it could be used for several threatening commands. Therefore, the Botnet attacks could be implemented to perform the DDoS attacks, phishing attacks, spamming, and other attacks scenarios. For instance, in 2017, a Mirai-Botnet attack targeted different surveillance cameras; then, it was used to perform DDoS attacks [3,24].

Therefore, there is an urgent need to implement an efficient detection approach against Botnet attacks, especially within the IoT smart environment. In this paper, one realistic and real benchmark IoT Botnet dataset was used. This IoT Botnet dataset was introduced by Koroniotis et al. in [25]. The key strength of the studied IoT Botnet attacks dataset is summarized as follows: it was considered one of the recent IoT benchmark datasets. Moreover, it includes different and recent types of IoT botnet attacks. The captured network traffic reflects the lightweight IoT devices typically implemented within the IoT smart environment. The studied IoT Botnet attacks dataset includes mainly three attacks groups as follows:

- Denial of Service group: this group of attacks includes the denial of service attacks which aim to disrupt the normal service for the legitimate users.
- Information theft group: this group of attacks includes different types of intrusions that aim to steal the personal information of the legitimate users.
- Information gathering: this group of attacks includes the information-gathering attacks, which could be beneficial for the attackers to gather the required information about the desired victims.

The studied Botnet attacks dataset includes different network devices that served a weather station. It also contains a large number of records besides 50 network parameters. It is worth mentioning that not all 50 network parameters were relevant to detecting the IoT Botnet attacks. From another perspective, the existence of irrelevant network parameters could decrease the efficiency of the detection approach. These network parameters were collected and extracted using the CIC-flow meter script.

At the early stage of designing the suggested detection approach, we are concerned about two factors: the simplicity of the suggested detection approach and the effectiveness of the detection rate. Therefore, only 60,000 records were extracted to design and optimize the suggested detection approach for simplicity. On the other hand, there are a large number of network parameters. Koroniotis et al. in [25] and Alkhassabeh et al. in [9] investigated the relevant network parameters using different selection attribute algorithms, and they suggested the top-5 network parameters to detect the IoT Botnet attacks.

To deeply investigate the relevant network parameters that could be affected directly by the Botnet attacks, we performed three ranking algorithms (*ANOVA, MRMR, Chi2*) to minimize the number of input parameters of the suggested detection approach. Furthermore, the intersection operation between these ranking algorithms was performed as shown in Equation (1).

$$(ANOVA \cap MRMR \cap Chi2) \tag{1}$$

Consequently, the input parameters were reduced to having only three effective input parameters to detect the IoT Botnet attacks. These input parameters are the Drate, the State, and Max network parameters. Therefore, the suggested detection approach was designed using only top-3 parameters. These network parameters were chosen according to their relevance to detecting the IoT Botnet attacks. The general architecture of the suggested detection approach within the IoT smart environment is shown in Figure 1.

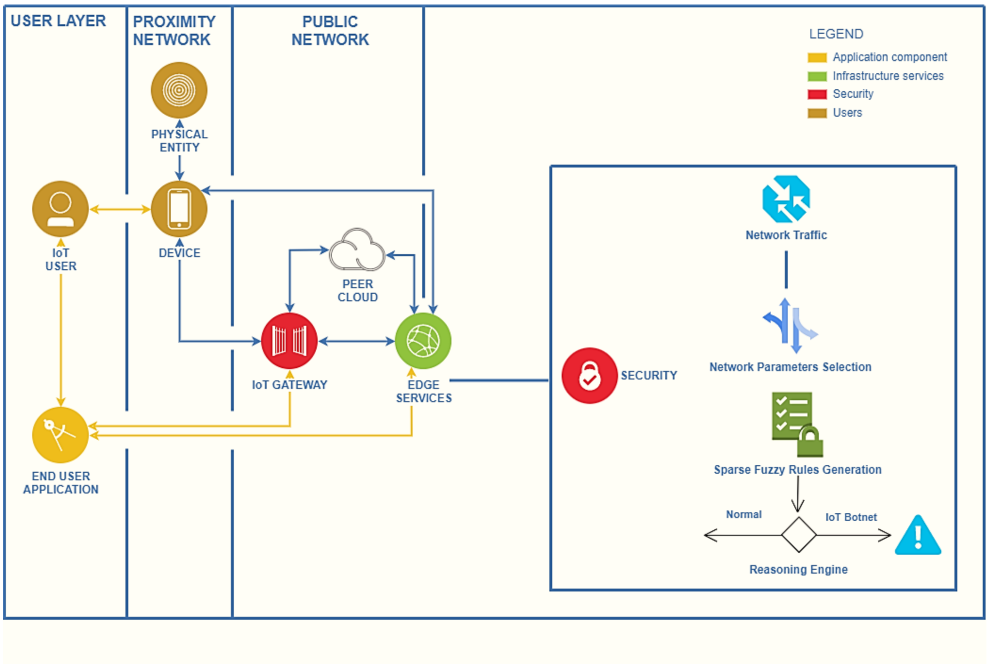

Figure 1. The General Architecture of the Suggested Detection Approach.

The general architecture of the suggested detection approach is started by investigating the network traffic to extract the most relevant network parameters. During this stage, the following procedures were performed:

- The resampling technique is applied for the studied IoT Botnet attacks dataset.
- Checking and removing the any missing observations.
- Searching for the Drate, State, and Max input parameters.
- Eliminating other network parameters.
- Storing the top-3 input parameters for the training and optimization phase.

Subsequently, 60,000 observations were stored for the training and evaluation phase. These observations were selected randomly and represent the real behavior of the IoT Botnet attacks within the IoT smart environment. Unlike other detection methods implemented to detect a specific type of Botnet attack, these observations considered the three groups of IoT Botnet attacks (DoS group, Information gathering group, and Information theft group).

3.2. Designing and Optimization Phase

Generally, the fuzzy inference system plays an essential role in smoothing the boundaries and avoiding binary decisions. There are many challenges still facing adapting a suitable detection approach against different intrusions. One of these challenges is the issue related to the binary decision that is considered a problematic factor for many application areas, especially in intrusion detection [26–28]. Furthermore, generating the required intrusion alerts is also considered a severe demand. In response to these issues, fuzzy rule interpolation was used in this work. The cooperation between the fuzzy system and interpolation techniques offers the required advantages to benefit from the fuzzy system for avoiding the binary decision and adapting the interpolation techniques to avoid issues related to the lack of knowledge base.

Therefore, the sparse fuzzy model identification [29] was used to design the suggested detection approach. The required IoT Botnet attacks observations were forwarded to the sparse fuzzy model identification to generate the required fuzzy sets parameters and sparse detection rules in this stage. The aim behind using the interpolation reasoning methods instead of the classical reasoning methods is that we are concerned about two factors: the simplicity of the suggested detection approach and the effectiveness of the detection rate. Therefore, the interpolation reasoning methods offer the required simple procedure to generate a few sparse detection rules that could detect the IoT Botnet attacks effectively. Furthermore, the interpolation reasoning methods could handle the lack of knowledge-based issues. In the classical reasoning methods such as Mamdani and Sugeno Fuzzy Inference Systems, the complete fuzzy rules are considered an urgent demand to generate the required consequences. There is a lack of expert knowledge in the intrusion detection application area. It could be that some observations appeared and were not covered by any of the fuzzy rules; in this case, the system could not generate the required intrusion alerts.

During the optimization phase, and to extract the required sparse detection rules and optimize the fuzzy sets parameters, the Rule Base Extension using the Default Set of Shapes (RBE-DSS) method was used [29]. The strength point of the RBE-DSS method is that it could generate the required sparse detection rules and optimize the required fuzzy sets parameters. Subsequently, 15 sparse detection rules were generated to detect the IoT Botnet attacks within the studied IoT smart environment. Table 1 shows the optimized sparse Botnet detection rules.

Table 1. The Optimized Sparse Botnet Detection Rules.

Num	Drate	Srate	Max	Alerts
1	Low	Low	Low	Normal
2	Low	Low	High	Botnet Attack
3	Low	Low	Medium	Botnet Attack
4	Low	High	Low	Botnet Attack
5	High	High	Medium	Botnet Attack
6	Low	High	Medium	Botnet Attack
7	Low	Low	Low	Botnet Attack
8	Medium	Low	High	Botnet Attack
9	Low	VLow	VLow	Normal
10	High	High	Medium	Botnet Attack

Consequently, the fuzzy sets were represented by the trapezoidal membership function when adapting the RBS-DSS method for the optimization stage. It is worth mentioning that the input parameters State and Max were divided into four linguistic terms (Very Low, Low, Medium, and High). The Drate input parameter was divided into three linguistic terms (Low, Medium, and High). Figure 2 shows the optimized fuzzy sets parameters of the suggested detection approach.

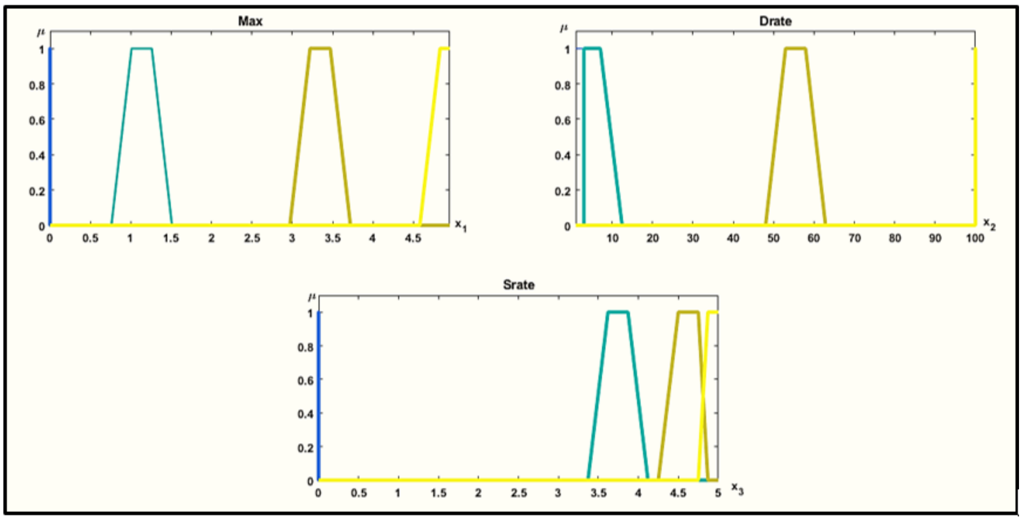

Figure 2. The Optimized Fuzzy Sets Parameters.

4. Experiments and Results

The experiments are described in this part as well as the findings of the recommended detection method. The inference engine of the suggested detection approach was performed using the Fuzzy Interpolation based on Vague Environment (FIVE) method. The FIVE method was introduced by Kovács in [30]. The aim of using the interpolation reasoning (FIVE) method is to simplify rule definition, and the reasoning mechanisms interpolate the missing Botnet attacks detection rules. In the classical reasoning methods, the size of the detection rule base is exponential. For this reason, the suggested Botnet attacks detection approach adopts the FIVE method. It effectively reduces the size of the detection fuzzy rule base. During the optimization phase, the validation process was conducted to check the ability of the suggested detection approach to interpolate the Botnet attacks alerts in case some observations appear and did not overlap by any of the Botnet attacks detection rules. Suppose that we have the following Botnet attack observation, which was not covered by any of the Botnet attack detection rules.

```
NumInputs=3
ObsName=‘‘Sparse Botnet Attack Observation’’
[Observation]
OBS1=’A^*_1’:’Max’,[4.5]![1]
OBS2=’A^*_2’:’Srate’,[90]![1]
OBS3=’A^*_3’:’Drate’,[4.5]![1]
```

Figure 3 shows the output response of the suggested detection approach in the case of the IoT Botnet attack. The output of the suggested detection approach demonstrated its ability to interpolate the required detection alerts even in case of a sparse rule base and lack of knowledge base.

This benefit could help reduce the size of the detection rule base and generate more comprehensive and understandable detection alerts. The testing and validation procedures were performed using 25,000 IoT environment network parameters observations. These network parameters were forwarded to the suggested detection approach as fuzzy singleton observations. Therefore, the testing data were transformed into fuzzy singleton observations during the validation and testing procedures. This step is an important step to evaluate the suggested sparse detection rules. The suggested detection approach had the ability to effectively detect the IoT Botnet attacks and reduce the total number of required sparse detection rules. From another perspective, some of the recent detection approaches that are discussed in Section 2 suffer from a high value of the false positive rate. The suggested detection approach effectively reduced the false positive alert, which could be helpful to save time and resources.

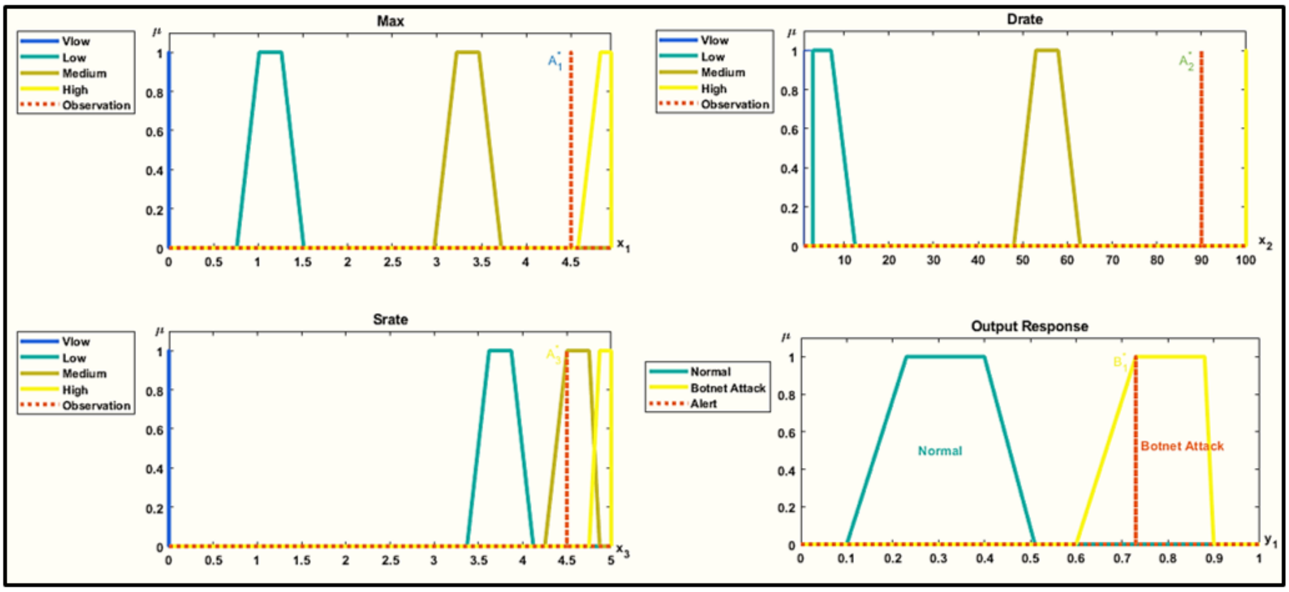

Figure 3. The Output Response of the Suggested Detection Approach.

Typically, standard performance metrics are used to evaluate intrusion detection methods such as detection rate and false-positive rate. Following the typical standard performance metrics could be useful for comparing the obtained results with other literature results that employed the same testbed environment with the same circumstances. The performance metrics of [9,31,32] were used. Table 2 shows the obtained standard performance values.

Table 2. The Performance Metrics of Suggested Detection Approach.

Num	Performance Metrics	Value
1	Sensitivity	0.9880
2	Specificity	0.9872
3	Precision	0.9880
4	Negative Predictive Value	0.9832
5	False Positive Rate	0.0068
6	False Negative Rate	0.0291
7	Computation Time	240 Minutes
8	Accuracy	0.9641

It could be concluded that the suggested detection approach recorded a 96% detection rate and effectively reduced the false positive alerts. The suggested detection approach is characterized by the combination of the fuzzy system and interpolation techniques. Therefore, the issue related to the binary decision and lack of knowledge base was handled. The suggested detection approach offers the required extension of the binary decision to the continuous space where the level of Botnet attack could be calculated. To summarize the results according to the studied IoT Botnet attacks benchmark dataset, the proposed detection method yielded acceptable performance metrics, simultaneously supporting the idea that the interpolation reasoning methods could be a promising approach in the intrusion detection application area.

Difference From Previous Works

There are valuable efforts for implementing different techniques against the IoT Botnet attacks. However, these detection approaches are either implemented using non-IoT datasets or they apply the binary decision. Evaluating the detection approaches using non-IoT datasets that do not have the current IoT protocol, such as 6LowPAN and Zigbee, could have unrealistic results. The major factors that distinguish this method from other typical detection methods are summarized as follows:

- The suggested detection approach uses the concept of the fuzzy system and performs the interpolation technique to reduce the size of fuzzy detection rules.
- Unlike some literature detection methods, the suggested detection approach was designed and optimized using a real IoT Botnet attacks dataset.
- The efficiency of the suggested detection approach is competitive with other detection methods, although using a few sparse detection rules.
- The issues related to the binary decision and lack of knowledge base were handled using the interpolation reasoning methods.
- The suggested detection approach generates the Botnet attacks alert in a more readable and understandable form where the level of IoT Botnet attacks could be calculated.

In summary, the efficiency of the proposed method reaches satisfactory levels for detecting IoT Botnet attacks. In addition, the obtained results were compared with other literature results. Table 3 compares the detection rate results between the proposed model and the previous literature results.

Table 3. Comparison of the Suggested Method with Other Methods.

Reference	Method	Detection Rate
[9]	Fuzzy Reasoning	0.95
[24]	LSTM+CNN	0.94
[28]	Multi-CNN	0.96
This Work	Fuzzy Interpolation based on Vague Environment	0.96

5. Conclusions

The fuzzy interpolation reasoning technique was used in this article to propose a detection method against IoT Botnet attacks. The suggested detection approach was designed and optimized using the sparse fuzzy model identification. The aim of using the interpolation reasoning method instead of the classical reasoning method is to avoid the demand of having complete fuzzy detection rules. Thus, the suggested detection approach is characterized by its ability to reduce the size of the fuzzy rules and interpolate the required IoT Botnet attacks alerts in case of deficiency of expert knowledge. The suggested detection approach was tested and evaluated using a benchmark IoT Botnet attacks dataset. The results demonstrated that the proposed detection technique was successful in detecting IoT Botnet attacks and reducing false positive alerts. From another perspective, the suggested detection approach was able to generate the required Botnet attacks alerts even if some observations appeared and did not overlap with any detection rules.

For future work, it could be worthwhile to investigate other interpolation reasoning methods and other optimization methods to extract the required Botnet attacks detection rules. Furthermore, investigating the hybrid techniques between the interpolation reasoning methods and other machine learning algorithms could be helpful to generate a suitable detection approach for IoT Botnet attacks.

Author Contributions: All authors have contributed equally to the work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gendreau, A.A.; Moorman, M. Survey of intrusion detection systems towards an end to end secure internet of things. In Proceedings of the 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 84–90.
2. Elrawy, M.F.; Awad, A.I.; Hamed, H.F. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 21. [CrossRef]
3. Bezerra, V.H.; da Costa, V.G.T.; Martins, R.A.; Junior, S.B.; Miani, R.S.; Zarpelao, B.B. Providing IoT host-based datasets for intrusion detection research. In *SBSeg 2018*; SBC: Londrina , Brazil, 2018; pp. 15–28.
4. Almseidin, M.; Alzubi, M.; Kovacs, S.; Alkasassbeh, M. Evaluation of machine learning algorithms for intrusion detection system. In Proceedings of the 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 14–16 September 2017; pp. 277–282. [CrossRef]
5. Almseidin, M.; Al-Sawwa, J.; Alkasassbeh, M. Generating a benchmark cyber multi-step attacks dataset for intrusion detection. *J. Intell. Fuzzy Syst.* **2022**, 1–15. [CrossRef]
6. Forestiero, A. Bio-inspired algorithm for outliers detection. *Multimed. Tools Appl.* **2017**, *76*, 25659–25677. [CrossRef]
7. Pajouh, H.H.; Javidan, R.; Khayami, R.; Dehghantanha, A.; Choo, K.K.R. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. *IEEE Trans. Emerg. Top. Comput.* **2016**, *7*, 314–323. [CrossRef]
8. Ghosh, P.; Mitra, R. Proposed GA-BFSS and logistic regression based intrusion detection system. In Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT), Hooghly, India, 7–8 February 2015; pp. 1–6.
9. Al-Kasassbeh, M.; Almseidin, M.; Alrfou, K.; Kovacs, S. Detection of IoT-botnet attacks using fuzzy rule interpolation. *J. Intell. Fuzzy Syst.* **2020**, *39*, 421–431. [CrossRef]
10. Forestiero, A. Metaheuristic algorithm for anomaly detection in Internet of Things leveraging on a neural-driven multiagent system. *Knowl.-Based Syst.* **2021**, *228*, 107241. [CrossRef]
11. Pokhrel, S.; Abbas, R.; Aryal, B. IoT Security: Botnet detection in IoT using Machine learning. *arXiv* **2021**, arXiv:2104.02231.
12. Abu Khurma, R.; Almomani, I.; Aljarah, I. IoT Botnet Detection Using Salp Swarm and Ant Lion Hybrid Optimization Model. *Symmetry* **2021**, *13*, 1377. [CrossRef]
13. Popoola, S.I.; Adebisi, B.; Ande, R.; Hammoudeh, M.; Anoh, K.; Atayero, A.A. smote-drnn: A deep learning algorithm for botnet detection in the internet-of-things networks. *Sensors* **2021**, *21*, 2985. [CrossRef]
14. Ashraf, J.; Keshk, M.; Moustafa, N.; Abdel-Basset, M.; Khurshid, H.; Bakhshi, A.D.; Mostafa, R.R. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. *Sustain. Cities Soc.* **2021**, *72*, 103041. [CrossRef]
15. Arrington, B.; Barnett, L.; Rufus, R.; Esterline, A. Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms. In Proceedings of the 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA, 1–4 August 2016; pp. 1–6. [CrossRef]
16. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Gener. Comput. Syst.* **2017**, *82*, 761–768. [CrossRef]
17. Lopez-Martin, M.; Carro, B.; Sanchez-Esguevillas, A.; Lloret, J. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot. *Sensors* **2017**, *17*, 1967. [CrossRef] [PubMed]
18. Garcia-Font, V.; Garrigues, C.; Rifà-Pous, H. Attack classification schema for smart city WSNs. *Sensors* **2017**, *17*, 771. [CrossRef] [PubMed]
19. Midi, D.; Rullo, A.; Mudgerikar, A.; Bertino, E. Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 656–666.
20. Prabavathy, S.; Sundarakantham, K.; Shalinie, S.M. Design of cognitive fog computing for intrusion detection in internet of things. *J. Commun. Netw.* **2018**, *20*, 291–298. [CrossRef]
21. Amouri, A.; Alaparthy, V.T.; Morgera, S.D. Cross layer-based intrusion detection based on network behavior for IoT. In Proceedings of the 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON), Sand Key, FL, USA, 9–10 April 2018; pp. 1–4. [CrossRef]
22. Silva, S.S.; Silva, R.M.; Pinto, R.C.; Salles, R.M. Botnets: A survey. *Comput. Netw.* **2013**, *57*, 378–403. [CrossRef]
23. Khattak, S.; Ramay, N.R.; Khan, K.R.; Syed, A.A.; Khayam, S.A. A taxonomy of botnet behavior, detection, and defense. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 898–924. [CrossRef]
24. Parra, G.D.L.T.; Rad, P.; Choo, K.K.R.; Beebe, N. Detecting Internet of Things attacks using distributed deep learning. *J. Netw. Comput. Appl.* **2020**, *163*, 102662. [CrossRef]
25. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [CrossRef]
26. Almseidin, M.; Alkasassbeh, M.; Alzubi, M.; Al-Sawwa, J. Cyber-Phishing Website Detection Using Fuzzy Rule Interpolation. *Cryptography* **2022**, *6*, 24. [CrossRef]

27. Altarawneh, G.A.; Hassanat, A.B.; Tarawneh, A.S.; Carfì, D.; Almuhaimeed, A. Fuzzy Win-Win: A Novel Approach to Quantify Win-Win Using Fuzzy Logic. *Mathematics* **2022**, *10*, 884. [CrossRef]
28. Li, Y.; Xu, Y.; Liu, Z.; Hou, H.; Zheng, Y.; Xin, Y.; Zhao, Y.; Cui, L. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement* **2020**, *154*, 107450. [CrossRef]
29. Johanyák, Z.C.; Kovács, S. Sparse fuzzy system generation by rule base extension. In Proceedings of the 2007 11th International Conference on Intelligent Engineering Systems, Budapest, Hungary, 29 June–2 July 2007; pp. 99–104.
30. Kovács, S. New aspects of interpolative reasoning. In Proceedings of the 6th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, Granada, Spain, 8–12 August 1996; pp. 477–482.
31. Obeidat, I.; Hamadneh, N.; Alkasassbeh, M.; Almseidin, M.; AlZubi, M. Intensive Pre-Processing of KDD Cup 99 for Network Intrusion Classification Using Machine Learning Techniques. *arXiv* **2018**, arXiv:1805.10458.
32. Tarawneh, A.S.; Hassanat, A.B.; Alkafaween, E.; Sarayrah, B.; Mnasri, S.; Altarawneh, G.A.; Alrashidi, M.; Alghamdi, M.; Almuhaimeed, A. DeepKnuckle: Deep Learning for Finger Knuckle Print Recognition. *Electronics* **2022**, *11*, 513. [CrossRef]