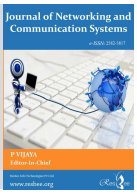
Vol.4 No.2 April 2021

Journal of Networking and Communication Systems

Received 19 December, Revised 17 February, Accepted 18 March



Deep Learning based optimization for Detection of Attacks in IoT

A.V.Krishna Prasad
Associate Professor, IT Department
Maturi Venkata Subba Rao Engineering College
Hyderabad, Telangana, India.
krishnaprasad_cse@mvsrec.edu.in

Abstract: Internet of Things (IoT) is an intelligent network which links smart objects to the Internet. A great amount of IoT devices are linking to the Internet, so far a lot of of these devices are apprehensive, exposing them to a number of security threats. Most IoT devices are resource constrained hence making it difficult to secure them using existing security techniques. Numerous researchers have developed intrusion detection model implemented at IoT gateways. In this work, to defend cyberspace a novel detection technique with a novel concept was introduced which helps the deep learning model. Here, the process includes two stages such as classification as well as feature extraction. Initially, the feature extraction is performed, from the subjected input data the extraction of features is carried out with the aid of the well-known Principal Component Analysis (PCA). Then, the extracted features are fed to the classification stage; here the Convolutional Neural network (CNN) model is exploited. The presence of attacks is classified by the classifiers, the attacks such as R2L, denial of service (DoS), U2R as well as a probe. For this, a novel optimization approach is called Hybrid Whale Optimization Algorithm (WOA)-Bat Algorithm (BA). This optimization is mainly exploited to choose optimally the hidden neurons. The developed algorithm performance is analyzed with the existing techniques regarding both the positive as well as negative metrics, and the analysis revealed the superiority of the proposed model.

Keywords: Classifiers, Detection,Deep Learning, Feature Extraction,PCA,Optimization Algorithm

Nomenclature

Abbreviations	Descriptions
DDoS	Distributed Denial of Service
ML	Machine Learning
ReLu	Rectified Linear Unit
IoT	Internet of Things
MPL	Max Pooling Layer
IDS	Intrusion Detection Systems
MLP	Multilayer Perceptron
CL	Convolution Layer
MIoT	Multiple IoT Scenario
BNL	Batch Normalization Layer

1. Introduction

Generally, IoT networks comprise numerous portable devices namely actuators as well as sensors and powerful devices namely control units, these devices are linked and swap the information ubiquitously. The information transforms amid the power restricted IoT devices as well as long-distance devices commonly pass via multiple nodes, to form a multi-hop mesh network. For multiple security threats, the multi-hop networks are susceptible namely reply packet attack, tamper packet attack, and discard packet attack, etc. Attackers control numerous attacks, and the malicious nodes execute. Therefore, it is important in IoT to detect malicious nodes [1].

To detect attacks, the IDS are renowned equipment in digital and linked systems. Generally, there are 2 detection models for IDS such as on the basis of ML as well as on the basis of the predefined set of misuse rules. In the previous technique, both the unknown as well as known attack rules are created by humans. The last model uses a detection technique on the basis of a pre-defined ML technique of normal

https://doi.org/10.46253/jnacs.v4i2.a5

behavior. To detect the malicious activities or novel kinds of attacks is used by the technique, which has never been exhibited earlier [2].

To identify as well as to protect the IoT devices, the occurrence of threats inspires the advancements of novel methods. Several studies possess advanced models, which aid to enhance the IoT devices security namely modeling lightweight authentication strategies, developing IDS so on. In some work is aspired to prevent DoS attacks on IoT devices [3].

The main objective of the DoS attack is to deluge devices in the network with false service requests, therefore disorder the network device's normal operation. DoS is an attack, which targets strenuous network devices' computational resources. Multiple agents initiate the DoS attack in a network and from several positions is called a DDoS attack. In a single IoT environment, anomaly detection has extensively experimented with and numerous outcomes include security, privacy as well as detection of fault is established. Nevertheless, no analysis on anomalies and their probable recognization in an IoT was carried out.

To detect the attacks, numerous techniques or models are there at risk till now, but the conventional models frequently do not fulfill the particular requirements of IoT such as scalability, distribution, resource restrictions, and minimum latency. Furthermore, several control operations are performed amid a several set of devices in IoT that frequently aids intelligent processing and decision making in addition to autonomous way via the communication associations devices as well as sensors. In addition, better performance and reliability besides ubiquity for the IoT model were performed. Nevertheless, the IoT is effective regarding the evaluation of high cost, minimum latency, and storage which is an implication in the calculation. ML approaches and optimization techniques are widely exploited in the state-of-the-art for attack detection. In numerous engineering issues, optimization techniques identify speedy applications [9], [10].

The main contribution of the developed model is to propose a hybrid optimization algorithm named Hybrid WOA-BA, which is used to choose the hidden neurons of the deep learning approach and also enhances the accuracy rate of classification procedure, which may be highly accurate in the detection of attacks. In classification outcome, to obtain high accuracy a novel optimization Hybrid WOA-BA algorithm is used it also exploits to find the optimal hidden neurons. Finally, the performance analysis of the developed model is evaluated with the existing techniques regarding the positive as well as negative metrics.

2. Literature Review

In 2020, Jerry John Kponyo et al [1],worked on the IoT that was an intelligent network which links smart objects to the Internet. In this work, a host-based and lightweight detection as well as defense model in order to identify DoS attacks in IoT devices. Moreover, on the basis of heuristics to handle the ICMP, SYN, as well as UDP flood attacks, an anomaly DoS detection scheme, was developed via the ML application.

In 2020, Bohan Li et al [2], developed a new technique for malicious detection nodes on the basis of the online learning model. Initially, the credibility of each path in the network was calculated, on the basis of the gathered packets. Subsequently, using the online learning approach, path reputation was modeled. At last, each node trust was calculated in the IoT environment as well as the malicious node was detected using the clustering approach. While the network was small, in order to create the design in better performance, some processing in the network topology was performed on the basis of the basic online learning detection approach and obtains an improved online learning detection approach.

In 2020, Fal Sadikin et al [3], developed a new hybrid IDS which integrates ML-based anomaly detection as well as rule-based IDS. Here, to present a precise detection model a rule base technique was exploited for known attacks. Nevertheless, in order to define precise as well as accurate rules need human effort as well as it was tiresome as well as error-prone. Moreover, the IDS was implemented which wrapped several kinds of detection models in order to detect the known attacks. In addition, a secure, as well as effective model was developed for large-scale IDS data collection. Hence, a trust reporting model was provided, which can work in the strict resource models obligatory using the present IoT systems.

In 2020, Quoc-Dung Ngo et al [4], worked on static IoT malware detection, initially the evolution, definition, and security threats were introduced in IoT malware. Subsequently, conventional IoT malware detection models were summarized as well as analyzed and compared. At last, the techniques of conventional models were performed on the basis of a similar IoT malware dataset.

In 2021, Francesco Cauteruccio et al [5], investigated an initial attempt of anomalies in a MIoT. Initially, a novel methods model was developed, which can create furthermore examinations in this paper simpler, coherent as well as uniform. Subsequently, the inverse problem, and the forward problem, as defined in the anomaly detection context in a MIoT was described. The explanations of these issues permit

the examination of anomalies based upon the internode distance, degree centrality as well as IoT network size.

3. Adopted Attack Detection Model in IoT

The modernization in technologies in hardware possess enabled a huge number of IoT device which linked to the Internet. Nevertheless, this huge IoT device link creates the network degraded by developing novel as well as various attacks which may cause human life loss and also millions of dollars. In reality, remarkable smart things are involved in the IoT ecosystem which is distributed over the geographical area. The interlinked frequently creates the network difficult with malevolent adversaries who could weaken the accessible resources as well as initiate several attacks such as a probe, U2R, R2L, and DoS.

In this paper, these attacks are detected using a novel scheme is proposed which integrates the idea of optimization in order to assure accurate attack detection in the network. The adopted approach working model is presented in this paper such as two stages such as classification as feature extraction. Moreover, to extract the distributed features such as duration flag, protocol, service, destination bytes as well as source bytes, the PCA process is exploited. Then the extracted features are fed to the classification process using the CNN technique. Using a novel optimization model, the hidden neuron of CNN is optimally chosen, to enhance the accuracy rate of classification. Fig 1 demonstrates the block diagram of the proposed technique for the attack detection in IoT

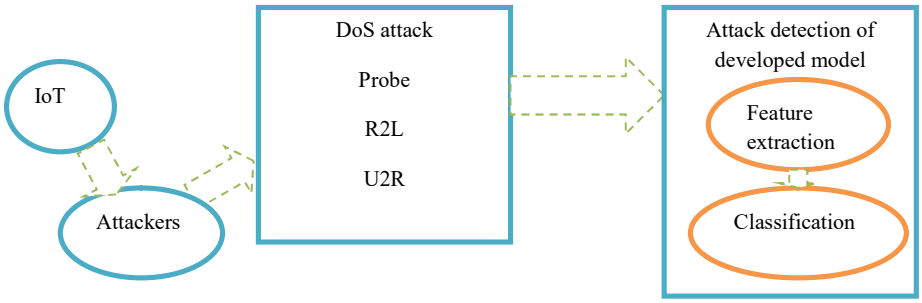


Fig. 1 *Block diagram of the adopted model for attack detection in IoT*

3.1 Proposed Model for Feature Extraction and Classification

From the input, the deep features can be extracted using the CNN. Nevertheless, the PCA possesses its own benefits while it is used on the input. The PCA benefits such as minimum requirements for the memory as well as capacity, minimum noise sensitivity, maximized effectuality, which occurred in lesser dimensions. Moreover, the PCA is exploited for data compression when assuring that no information is misplaced and it handles more than 2 parameters such as simple to recognize the variables, insensible to original data scales, integrates the correlated parameters to a single variable, enhances visualization, minimizes over fitting as well as simple to evade correlated features. Moreover, to extract the deep features the CNN model is performed from the PCA-based features. Initially, the feature extraction is the initial phase for the adopted detection technique, whereas the features such as flag, duration service, protocol, source bytes, destination bytes, and few other features are done by exploiting the PCA principles.

3.2 PCA Model

From input data I^D, the features F are extracted using PCA [6] process. Initially, in order to find the correlation matrix eigenvectors are carried out and the eigenvectors that possess maximum eigenvalues are considered. It is indicated as IN input vector transformation with the same length L in IN -dimensional vector $\mathrm{v}=[\mathrm{v}_{\mathbf{1}},\mathrm{v}_{\mathbf{2}},.....\mathrm{v}_{\mathrm{I}}]^{\mathrm{T}}$ into a vector l as stated in eq. (1).

$$\mathrm{l}=\mathrm{A}\left(\mathrm{v}-\mathrm{me}_{\mathrm{V}}\right) \tag{1}$$

Each v row consists of L values. Eq. (2) indicates formulation of me_a vector represents the mean vector.

$$\mathrm{me}_{\mathrm{V}}=\mathrm{MA}\{\mathrm{v}\}=\frac{\mathbf{1}}{\mathrm{L}}\sum_{\mathrm{f}}^{\mathrm{L}}\mathrm{v}_{\mathrm{f}} \tag{2}$$

From the covariance matrix CV_{V}, matrix A is ascertained. A row of A matrix consists of eigenvectors of CV_{V} which are arranged based on the equivalent Eigenvalues in descending order. Eq. (3) is obtained by the CV_{V} using the relation. The covariance matrix size is $\mathrm{IN}\times\mathrm{IN}$ as v is IN-dimensional. Eq. (4) indicates the covariance amid $\mathrm{v}_{\mathrm{d}},\mathrm{v}_{\mathrm{d}'}$. Using the relation, the module number for preservation is ascertained, that is

stated in Eq. (5), L indicates the count of retained principal components, VA indicates the Eigenvalues, TO indicates the total count of Eigenvalues.

$$CV_v = MA\left\{(v - me_v)(v - me_v)^T\right\} = \frac{1}{L}\sum_{f=1}^{L} v_f v_f^T - me_v me_v^T \quad (3)$$

$$CV_v(d, d') = MA\left\{(v_d - me_d)(v_{d'} - me_{d'})\right\} \quad (4)$$

$$\frac{\sum_{d=1}^{TO} VA_d}{\sum_{f=1}^{L} VA_f} = \alpha \quad \text{where } 0 < \alpha <= 1 \quad (5)$$

At last, the extracted features $F = f_1, f_2 .... f_n$, (whereas n represents the total number of features) from the input data are subjected to the classification procedure. This work exploits the CNN, for the classification process.

3.3. CNN Model

Here, the extracted features F are fed to the CNN [7] approach, whereas it classifies if there exists an attack or not. Specifically, this work mostly concentrates on the attacks such as Probe, DoS, R2L, U2R. The explanation of aforesaid attacks is stated as below:

Probe: Satan-Probing of the network for well-known weakness.

R2L: Illegal access of local user account through vulnerability, and etc

U2R: Admin level is accessed by enabling the roolkit.

DoS: Through User Data Packets (UDP) packets, system rebooting or crash occurs.

The exploited CNN classifiers classify if the network suffers from any of these attacks.

The used DBN classifier classifies whether the network suffers from any of these attacks. The CNN model is designed based on the input layer, MPL, CL, BNL, ReLu, fully connected layer, and the output layer. The convolutional kernels parameters are adjusted during the training process on the basis of the optimal values attained at the time of the optimization procedure. Generally, the stochastic gradient solver is exploited by the CNN to tune the hyperparameters. The parameter choice is application-dependent. Nevertheless, the convergence rate and CNN accuracy are decided by the suitable hyperparameters choice in the classification task. The training needs a large amount of time if the primary learning rate is less. The hyperparameter is decided by the change by the learning rate, which is needed each time the technique is updated on the basis of the error.

Likewise, the regularization term is added by the regularization parameter to the cost function. It is exploited to avoid the technique from overfitting. The gradient decay factor is used to decide the factor therefore the learning rate alters each epoch.

The CNN exploits a large number of hyperparameters rather than a conventional MLP.

For the input image, the features are extracted by the convolution layer at each offset. By the proposed model, the layers hyperparameters are optimized. In the input image, output features maps are sensitive to the position of the features. To address the sensitivity, one solution that is exploited and attains the local translation variance is to carry out pooling. Subsequent to that the nonlinearity is used to the feature maps attained from the convolutional layers, pooling is used. The ReLu is exploited for the nonlinear activation function which maps to the feature space by the extracted features. Here, four kinds of pooling are present such as max pooling, average pooling, global max pooling, and, global average pooling. In this paper, max pooling is exploited, since it retains the mainly well-known features of the featuremaps, hence sharp features are retained.

3.4. Hybrid WOA-BAT optimization Model

The WOA approach was developed in [8] by replicating the hunting humpback behavior of whales by starting chasing the prey as well as replicating the bubble net scheme. The WOA approach comprises two important stages such as spiral and prey updating called as exploitation stage. Here, the prey is arbitrarily searched. This paper uses the WOA approach primarily initiates with a random set solution for *V = (W, B)*, weights, and bias for the MLP. In each iteration, on the basis of arbitrary selection, the search agent or optimal solution is attained.

The subsequent for mulations eq. (6) and (7) states the hunting behavior of the prey.

$$\vec{X}(t+1) = \vec{X}^*(t) - \vec{A}\vec{D}\, z \quad (6)$$

$$\vec{D} = |\vec{C}\vec{X}^*(t) - \vec{X}(t)| \quad (7)$$

$\vec{X}^*(t)$ indicates the whale's optimal earlier location and $\vec{X}(t+1)$ indicates the current whale location. $\vec{D}$ indicates the distance vector and $\vec{C}$ and $\vec{A}$ indicates the co-efficient vectors calculated as (8).

$$\vec{C} = 2r \; ; \; \vec{A} = 2ar + a \tag{8}$$

The spiral updating model is performed of bats and it is integrated with particular enhancements in order to speed up the convergence. An arbitrary value of p is created by exploiting if there is a fifty percent of probability to select amid either the replicating the encircling model or the spiral mechanism in order to update the location.

If $p > 0.5$ then the current iteration is updated as given in (9).

$$\vec{X}(t+1) = \vec{D}e^{bk}\cos(2\pi k) + \vec{X}(t) \tag{9}$$

Let $k = b = 1$, therefore (9) minimizes to (10).

$$\vec{X}(t+1) = 2.7 * \vec{D} + \vec{X}(t) \tag{10}$$

If $p < 0.5$, subsequently the current iteration is updated as given in (11)–(13).

$$f_i = f_{min} + (f_{max} - f_{min}) \tag{11}$$

$$v_i^{t+1} = v_i^t + \left(x_i^t - x_*\right) f_i \tag{12}$$

$$x_i^{t+1} = \left(x_i^t - v_i^{t+1}\right) \tag{13}$$

where v_i is the bat velocity as well as x_i is the bat position. The wave frequency is the upper and lower bound represented as (100,-100).The bats' new location is updated based on the novel velocity as while the bat identifies the food/prey, the rate loudness is inversely proportional to the rate of emission.

4. Result and Discussion

In this section, the developed detection technique was illustrated. Here, the proposed model illustrates the traffic compositions, intrusion beside the extensive adaptable as well as reproducible. Moreover, the datasets consist of two classes as normal and attack. The performance analysis of the proposed model and conventional models was demonstrated with respect to two cases such as two-class and multi-class scenarios. Also, the analysis was estimated with certain positive as well as negative metrics.

Fig 2 demonstrates the outcomes in two-class cases. Here, it is seen that the accuracy of the developed technique is 12% better than the PSO models. Fig 3 demonstrates the analysis of the proposed model in the multi-class scenario. Here, it is seen that the developed technique is efficient in order to detect the attacks in the network. Moreover, the proposed method's accuracy is very effective over the conventional models. Therefore, the overall analysis exhibits that the superiority of the adopted technique in order to detect the attacks in IoT.

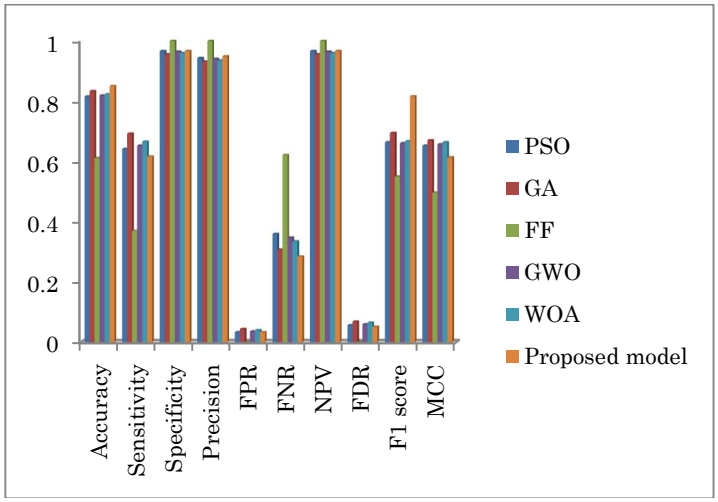


Fig. 2*Performance analysis of the developed and existing models in 2 class scenario*

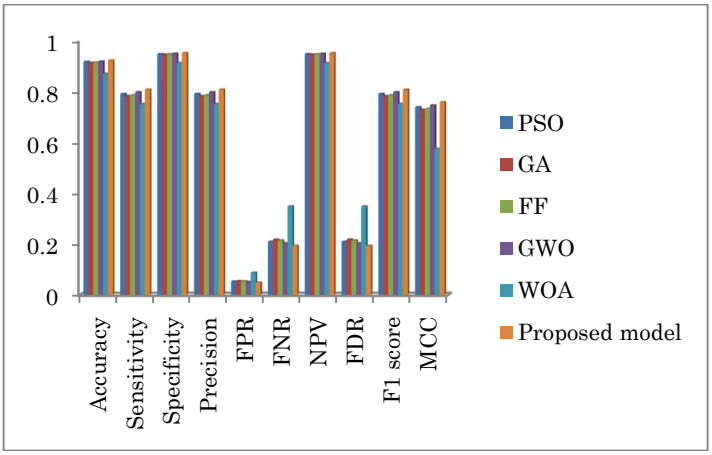


Fig. 3*Performance analysis of the developed and existing models in multi-class scenario*

5. Conclusion

In this work, a novel attack detection technique was exploited to detect the R2L, probe, DoS, and U2R in IoT. Here, the process was performed in two states as classification and feature extraction. In order to extract the feature, the PCA process was exploited from the input data. Subsequently, these features were fed to the deep learning classifier; here the classified outcomes were obtained. Furthermore, the adopted technique was aspired to process the optimization idea to attain the superior as well as accurate classification outcome. Therefore, a novel optimization method called the Hybrid WOA-BA algorithm was developed to choose the optimal hidden neurons. At last, the developed technique was estimated with the existing techniques regarding the positive as well as negative metrics. From the analysis, it was seen that the adopted model performs better and obtained highly precise classification results over the conventional techniques, and also it was exhibited in the detection of attacks.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Jerry John KponyoJustice Owusu AgyemangJoshua Ofori Boateng,"Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices", Internet of Things, vol.12, 6 November 2020.

[2] Bohan LiRenjun YeKen Cai,"A detection mechanism on malicious nodes in IoT", Computer Communications, vol. 151, pp 51-59, 30 December 2019.

[3] Fal SadikinTon van DeursenSandeep Kumar,"A ZigBee Intrusion Detection System for IoT using Secure and Efficient Data Collection", vol. 12, Internet of Things,20 October 2020.

[4] Quoc-Dung NgoHuy-Trung NguyenDoan-Hieu Nguyen,"A survey of IoT malware and detection methods based on static features", vol. 6, no.4, pp. 280-286, ICT Express,15 May 2020.

[5] Francesco CauteruccioLuca CinelliGiancarlo Fortino,"A framework for anomaly detection and classification in Multiple IoT scenarios", Future Generation Computer Systems,vol. 114, pp.322-335, 14 August 2020.

[6] A.Vinay, C. AkshayKumar, Gaurav R.Shenoy, K. N. BalasubramanayaMurthy and S.Natarajan, " ORB-PCA Based Feature Extraction Technique for Face Recognition, Procedia Computer Science, vol. 58, pp. 614-621, 2015.

[7] Sisi LiuIckjai Lee,"Sequence encoding incorporated CNN model for Email document sentiment classification", Applied Soft Computing,13 January 2021.

[8] Sameena PathanP. C. SiddalingaswamyTanweer Ali," Automated Detection of Covid-19 from Chest X-ray scans using an optimized CNN architecture", Applied Soft Computing,24 February 2021.

[9] Dr.Sivaram Rajeyyagari,"Automatic Speaker Diarization using Deep LSTM in Audio Lecturing of e-Khool Platform", Journal of Networking and Communication Systems, vol.3, no. 4, October 2020.

[10] Amit Sarkar,Senthil Murugan T,"Adaptive Cuckoo Search and Squirrel Search Algorithm for Optimal Cluster Head Selection in WSN", Journal of Networking and Communication Systems, vol.2, no. 3, July 2019.