International Journal of Engineering & Technology, 7 (2.7) (2018) 797-802

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Anomaly based Intrusion Detection by Heuristics to Predict Intrusion Scope of IOT Network Transactions

Ravinder Korani[1*], Dr. P. Chandra Sekhar Reddy[2]

[1]B. Tech, M. Tech, (Ph.D.), Associate Professor, ECE Department, Shadan College of Engineering and Technology, JNTU, Hyderabad, India.
[2]B. Tech, M. E, M. Tech, Ph.D. Professor &Co-ordination, ECE Department, JNTU, Hyderabad, India.
**E-mail: koraniphd814@gmail.com*

Abstract

Conventional intrusion detection mechanisms face serious limitations in identifying heterogeneous and distributed type of intrusions over the IoT environment. This is due to inadequate resources and open deployment environment of IoT. Accordingly, ensuring data security and privacy are tough challenges in the practical context. This manuscript discusses various aspects of networking security and related challenges along with the concepts of system architecture. Further, endeavored to define a machine learning model that outlines two heuristics called Intrusion Scope Heuristic (*ish*), and benign scope heuristic (*bsh*), which further uses in predictive analysis to identify the IOT network transaction is prone to intrusion or benign. The experimental study revealed the significance of the proposal with maximal detection accuracy, and minimal miss rate.

Keywords: *IOT, IDS, Intrusion, Intrusion Scope Heuristic, Benign Scope Heuristic, open deployment.*

1. Introduction

Securing both data and network infrastructure is witnessing wide attraction from researchers due to increasing attacks observed over the internet. The internet communication is efficient and plays a prominent role in individual's daily life and work. Due to its omnipresence, the Internet is vulnerable to attacks from heterogeneous and distributed intruders globally. The study in [1] depicts that hackers intrude internet once in every 20 seconds and the quanta of economic losses caused by these attacks in the US alone summed up to 10 billion USD every year. The authors observed that the information theft is increasing at a rate of 250%. Further, almost 98% of popular companies witnessed attacks on their networks. Accordingly, designing effective intrusion defending strategies are the most vital tasks ahead of both academicians and industry experts. Network intrusion detection mechanism is an important technology in this aspect [2], [3].

The practical applications of IoT are increasing rapidly across industries including transmission industry, railways, infrastructure, residential and consumer applications. The IoT devices are being installed as sensors, wireless communication modules, processors in these industries. During 1999, MIT university researchers put forward the idea of the Internet of Things on the basis of RFID. Further, they proposed the idea of product e-code. This EPC mechanism is capable of monitoring the products on the real-time basis and equips users with more comprehensive and optimal supply-chain management. Accordingly, adapting the automated identification technology can largely assist users in their regular operations [4]. IoT devices operate over computer networks, wireless sensor networks, and conventional mobile communication networks and because of the inbuilt attack proneness of these networks, IoT devices are constantly exposed to the security and privacy problems associated with the networks.

Diverse types of attacks are observed over these networks, of which prominent types include targeting integrity, confidentiality of networks and unauthorized access to information and resources. Conventional intrusion detection strategies like encrypting and authenticating are observed to be passive and regardless of upgrades, they face constant intrusions.

Intrusion detection mechanism is a novel technology developed over the recent few years. It is observed to be efficient in handling network security and implementing effective strategies for overcoming limitations in conventional mechanisms [5].

The study in [6] presented the intrusion detection approach [6]. The study concluded that an efficient detection strategy must consider network packet data, insights from the collected data, attack detection capability, ability to transfer information to the system management alert mechanism, should offer suitable defending measures. Accordingly, the model must comprise of basic functions including data gathering, analysis, identification, and alarms.

2. Related Work

Amid the growth in real-time security intrusions in IoT environment, selected intrusion detection approaches should be dynamic. Further, the mechanisms should be less complex and must be executed with minimum resources and time while ensuring adequate precision rates.

Most of the intrusion detecting and defending approaches rely on statistical methods to identify malicious activities. Some of the statistical models engaged include HMM-model [7], NBs algorithm [8], cluster analysis [9], distance measuring [10] and Signal processing [11]. Typically, these detection mechanisms are classified as supervised and unsupervised learning [12]. The general

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

behavior of the network is built through labeled corpus in the supervised approach [13]. On the contrary, the unsupervised anomaly detecting models presume that such general behaviors occur frequently and accordingly, do not engage any training phase [14].
The study in [15] put forward an unsupervised intrusion detection system on the basis of subspace clustering and outlier detection. The experimental evaluation of the study depicted the model outperformed over benchmark models against new and unknown attacks.
An attribute selection filter approach is presented in [16] that use PCA analysis and Fisher Dimension Reduction to remove noises. Though the model was efficient in filtering out noises, it resulted in high FPR ratio.
The authors in [17] put forward an unsupervised NIDS through Optimum-path forest approach and K- Means clustering model. The study attempted to model malicious and benign behaviors.
A two-phase IDS was put forward by [18]. The model initially detects misuse and in the next phase, it attempts to lower FPR and FNR rates through KNN-algorithm.
The study in [19] put forward a multi-classification IDS approach comprising of SVMs and BRICH hierarchical clustering approach to obtain important features from KDD99 corpus. The approach depicted superior performance over DoS and Probe type of intrusions. However, the model had poor efficiency over U2R and R2L attacks.
The study in [20] relied on multivariate correlation analysis to increase precision rates in network traffic characterization. The authors in [21] developed a two-layer classifier to identify U2R and R2L intrusion types. The model was relatively simple due to optimized attribute reduction. The study in [22] put forward an ensemble model driven multiple filter attribute selection strategies. The model identifies DDoS intrusion type in cloud environments and opted for four filter mechanisms to obtain the best selection. The model was developed over NSL-KDD corpus. An intrusion classification for cloud services were put forward in [23]. The author proposed a cloud-based IDS.
The study in [24] put forward a mutual information-based detection system, which identifies optimal attributes for classifiers on the basis of attribute selection approach. The model has been simulated over three popular corpuses- KDD Cup 99, Kyoto 2006+, and NSL-KDD.
In addition to communication networks, IDS concept has been extended to the industrial environment [25]. Multiple mechanisms have been designed to handle security challenges in industrial control systems. The study in [26] designed an automatic mechanism to construct a hybrid intrusion detection system, which learns temporal state-based metrics for power systems. The model was incorporated to precisely identify disturbances, regular control functions, and cyber-attacks. The study in [27] designed an anomaly for the industrial environment along with a multi-model-based detection system on the basis of HMM model to differentiate intrusions and benign faults.
Network attacks are a potential hurdle restricting incorporation of IoT devices in different industries. The study in [28] depicted that multiple approaches can be used to defend cyber-attacks in IoT environment. The author in [29] suggested a hierarchical authentication framework for managing anonymous information communication over IoT networks.
The study in [30] emphasized on the prominence of ghost attacks over ZigBee based IoT devices and in [31], an automated model-based security mechanism was suggested. This mechanism is utilized to predict, identify and counter cyber-attacks automatically with almost no manual intervention. The study in [32] cross verifies information transform at each node in the IoT network and thereby defending against insider's attacks.
However, the aforesaid contemporary models are specific to defend the intrusion through the signatures depicted from past network transactions of intrusion prone and benign, which limits their performance to defend zero-day intrusions. Another critical limit is the dimensionality of the features, which is the crux of process complexity. In regard to this, the depicted model of this manuscript enables to reduce the dimensionality of the features and allows to defend the zero-day intrusions.

3. Heuristics to Scale Intrusion Scope

The proposed intrusion detection strategy is of two phases and they are learning and prediction (rightly label the unlabeled records). The learning phase depicts two metrics called Intrusion Scope Heuristic and Benign Scope Heuristic. The knowledge obtained from the labeled data used in learning phase of the model is used to depict the two heuristics proposed.
The records that are used in learning phase are labeled as either intrude or benign, and each record is sequence of values representing the set of attributes in fixed sequence. The first move of the learning phase partitions the given records in to two sets, such that the records labeled as intrude is one set IR and the records labeled as benign as other set BR. Further, frames the bigram sequences of the field attributes that representing the values in static order of the respective records as feature identities. This phase depicts $n-1$ feature identities from n attributes of the respective set of records used in learning phase. Later the process of finding bigram sequences as feature identities, the values in records of sets BR, IR representing for each of these bigram sequences will be considered as feature sets BRF, IRF in respective order. Further phase depicts the optimal features of the both the benign and intrude record sets BR, IR, which is done by the floating search technique for feature optimization called Sequential Forward Search [33]. Further phase of the learning process depicts the impact weight of each optimal feature of benign and intruded record sets, which is done by bi-graph projected between optimal features and records of the respective labels benign and intrudes.
Further phase uses the impact weights of the features of corresponding labels "benign", and "intrude" to assess the Benign Scope Heuristic $esbs$, and Intrusion Scope Heuristic $esms$ in respective order. These heuristics further uses to rightly label the unlabelled records given.

3.1. The Features Projection

Let the set $IR = \{ir_1, ir_2, ..., ir_{|IR|}\}$ contains the records that are labeled as intrude, $|IR|$ represents the total number of records in set IR. Each of the record $\{ir \exists ir \in IR\}$ is sequence of values representing fixed number of different attributes in static order. Let the size of each record $\{ir \exists ir \in IR\}$ is n. Let the set $IRF = \{bsi_1, bsi_2, ...bsi_{|IRF|}\}$ contains the unique bigram sequences of the values as features, such that each of these bigram sequence exists in at least one record of the set IR.
Similarly, the set $BR = \{br_1, br_2, ..., br_{|BR|}\}$ denotes the set of records labelled as benign. Each of the record $\{br \exists br \in BR\}$ is sequence of values representing fixed number of different attributes in static order. Let the size of each record $\{br \exists br \in BR\}$ is n. Let the set $BRF = \{bsb_1, bsb_2, ...bsb_{|BRF|}\}$ contains the unique bigram sequences of the values as features, such that each of these bigram sequence exists in at least one record of the set BR.

3.2. Feature Optimization

The floating search technique called sequential forward search [33] is adopted to depict the optimal features in regard to both labels intrude, and benign. This method trains by a fitness state that defines optimum features, and the criteria that defines the tawdriness of the features, and the same will be in use to select

optimum features. The fitness of a feature in regard to the proposal can define as "a bigram sequence bs that exists with high coverage support in records IR labeled as intrude, and the same bigram sequence bs , which exists with least coverage support in records BR labeled as benign, or if does not exists in BR , then that feature is optimum in regard to the label intrude. Vice versa, a bigram sequence bs exists with coverage support in records BR labeled as benign, and does not exists or exists with least coverage support in records IR labeled as intrude is the optimal feature in regard to the label benign.

Upon completion of this forward sequence search, the feature sets $IRF, and\ BRF$ retains optimum features and discards the features with tawdriness.

3.3. Intrusion and Benign Scope Heuristics

This section explores the process of depicting heuristics for intrusion scope, and benign scope. The projection weight of each optimal feature respective to labels intrude and benign will be assessed initially. The record level projection weight of each feature denotes the correlation of that feature with the other optimal features in regard to each record of respective label. The following explores the process of assessing the record level projection weight of each optimal feature in regard to corresponding label.

Initial step of the process depicts the coverage support of each pair of bigram sequences depicted as optimal features, which is as follows

For each feature $\{bsi_i \exists bsi_i \in IRF \wedge i = 1,2,... \mid IRF \mid\}$ Begin

//that exists in features set IRF of size $\mid IRF \mid$

For each feature $\{bsi_j \exists bsi_j \in IRF \wedge j = i+1, i+2,... \mid IRF \mid\}$ Begin

//that exists in features set IRF of size $\mid IRF \mid$

$$cr_{bsi_i \leftrightarrow bsi_j} = \frac{\sum_{k=1}^{|IR|} \{1 \exists bsi_i \in ir_k \wedge bsi_j \in ir_k \wedge ir_k \in IR\}}{\mid IR \mid}$$

// ratio $cr_{bsi_i \leftrightarrow bsi_j}$ is of number of records contain both the bigram sequences bsi_i, bsi_j against total number of records $\mid IR \mid$

End

End

Similarly, the correlation of each pair of bigram sequences in regard to label benign will be assessed as follows:

For each feature $\{bsb_i \exists bsb_i \in BRF \wedge i = 1,2,... \mid BRF \mid\}$ Begin

//that exists in features set BRF of size $\mid BRF \mid$

For each feature $\{bsb_j \exists bsb_j \in BRF \wedge j = i+1, i+2,... \mid BRF \mid\}$ Begin //that exists in features set BRF of size $\mid BRF \mid$

$$cr_{bsb_i \leftrightarrow bsb_j} = \frac{\sum_{k=1}^{|BR|} \{1 \exists bsb_i \in br_k \wedge bsb_j \in br_k \wedge br_k \in BR\}}{\mid BR \mid}$$

// ratio $cr_{bsb_i \leftrightarrow bsb_j}$ is of number of records contain both the bigram sequences bsb_i, bsb_j against total number of records $\mid BR \mid$

End

End

Further phase of the process depicts the record level projection weights of each bigram sequence that depicted as optimal feature of the labels intrude or benign, which is as follows:

For each record $\{ir_k \exists ir_k \in IR \wedge k = 1,2,...,\mid IR \mid\}$ Begin

For each feature $\{bsi_i \exists bsi_i \in IRF \wedge i = 1,2,... \mid IRF \mid\}$

Begin //that exists in features set IRF of size $\mid IRF \mid$

$w_{bsi_i \to ir_k} = 0$ // aggregate of the correlation weights is initialized to 0.

For each feature $\{bsi_j \exists bsi_j \in IRF \wedge j = i+1, i+2,... \mid IRF \mid\}$ Begin //that exists in features set IRF of size $\mid IRF \mid$

$$w_{bsi_i \to ir_k} += \{cr_{bsi_i \leftrightarrow bsi_j} \exists bsi_i \in ir_k \wedge bsi_j \in ir_k\}$$

End

$$rpw_{bsi_i \to ir_k} = \frac{w_{bsi_i \to ir_k}}{ir_k^n}$$ // record level projection weight $rpw_{bsi_i \to ir_k}$ of a bigram sequence bsi_i against a record ir_k , which is the ratio of aggregate of the correlation weights $w_{bsi_i \to ir_k}$ between bsi_i and other bigram sequences exists in corresponding record, and ir_k^n denotes the number of optimal bigram sequences exists in corresponding record.

End

End

Similarly, the record level projection weight of each bigram sequence, which is optimal feature of the records labeled as benign will be assessed as follows:

For each record $\{br_k \exists br_k \in BR \wedge k = 1,2,...,\mid BR \mid\}$ Begin

For each feature $\{bsb_i \exists bsb_i \in BRF \wedge i = 1,2,... \mid BRF \mid\}$

Begin //that exists in features set BRF of size $\mid BRF \mid$

$w_{bsb_i \to br_k} = 0$ // aggregate of the correlation weights is initialized to 0.

For each feature $\{bsb_j \exists bsb_j \in BRF \wedge j = i+1, i+2,... \mid BRF \mid\}$ Begin //that exists in features set BRF of size $\mid BRF \mid$

$$w_{bsb_i \to br_k} += \{cr_{bsb_i \leftrightarrow bsb_j} \exists bsb_i \in br_k \wedge bsb_j \in br_k\}$$

End

$$rpw_{bsb_i \to br_k} = \frac{w_{bsb_i \to br_k}}{br_k^n}$$ // record level projection weight $rpw_{bsb_i \to br_k}$ of a bigram sequence bsb_i against a record br_k , which is the ratio of aggregate of correlation weights $w_{bsb_i \to br_k}$ between bsb_i and other bigram sequences exists in corresponding record, and br_k^n denotes the number of optimal bigram sequences exists in corresponding record.

End

End

Further phase of the process estimates the projection weight of the records, which is the ratio of record level projection weights of all bigrams sequences exists in corresponding record. The following equation depicts the projection weight of each record.

For each record $\{ir_k \exists ir_k \in IR \wedge k = 1,2,...,\mid IR \mid\}$ Begin

$$pw_{ir_k} = \frac{\sum_{i=1}^{|IRF|} \{pw_{bsi_i \to ir_k} \exists bsi_i \in IRF \wedge bsi_i \subset ir_k\}}{\mid ir_k \mid -1}$$ // depicting the projection weight of the record ir_k , which is the ratio of aggregate record level projection weights of all bigrams sequences exists in corresponding record

End

Similarly, the projection weight of each record related to benign label will be assessed as follows:

For each record $\{br_k \exists br_k \in BR \wedge k = 1,2,...,|BR|\}$ Begin

$$pw_{br_k} = \frac{\sum_{i=1}^{|BRF|} \left\{ pw_{bsb_i \to br_k} \exists bsb_i \in BRF \wedge bsb_i \subset br_k \right\}}{|br_k| - 1}$$ // depicting the projection weight of the record br_k, which is the ratio of aggregate record level projection weights of all bigrams sequences exists in corresponding record

End

Further phase of the proposal assesses the feature projection weight corresponding to respective labels benign and intrude, which is as follows:

For each bigram sequence $\{bsi \exists bsi \in IRF\}$ Begin //which is optimal feature of the label intrude

$$pw_{bsi} = \frac{\sum_{k=1}^{|IR|} \left\{ pw_{ir_k} \exists bsi \subset ir_k \right\}}{\sum_{k=1}^{|IR|} \left\{ pw_{ir_k} \right\}}$$ // ratio of aggregate projection weights of the records those contains the given bigram feature bsi against the aggregate projection weights of all records.

End

For each bigram sequence $\{bsb \exists bsb \in BRF\}$ Begin //which is optimal feature of the label benign

$$pw_{bsb} = \frac{\sum_{k=1}^{|BR|} \left\{ pw_{br_k} \exists bsb \subset br_k \right\}}{\sum_{k=1}^{|BR|} \left\{ pw_{br_k} \right\}}$$ // ratio of aggregate projection weights of the records those contains the given bigram feature bsb against the aggregate projection weights of all records.

End

The final phase of the depicted model assesses the heuristics for intrusion scope, and benign scope as follows. In regard to this, the ratio projection weights observed for all records of the corresponding labels intrude, and benign will be assessed in respective order that is as follows:

$$ish = \frac{\sum_{k=1}^{|IR|} pw_{ir_k}}{|IR|}$$ // intrusion scope heuristic ish is depicted, which is the average of projection weights observed for records labeled as intrude.

$$bsh = \frac{\sum_{k=1}^{|BR|} pw_{br_k}}{|BR|}$$ // benign scope heuristic bsh is depicted, which is the average of projection weights observed for records labeled as benign.

In order to depict the down side and up side of the heuristics depicted for labels intrude, and benign, the root mean square distance of the projection weights of the records will be assessed in respective order of the aforesaid labels, which is as follows:

$$d_{ish} = \frac{\sum_{k=1}^{|IR|} \sqrt{\left(ish - pw_{ir_k}\right)^2}}{|IR|}$$ // root mean square distance of the projection weights of the records labeled as intrude.

$$d_{bsh} = \frac{\sum_{k=1}^{|BR|} \sqrt{\left(bsh - pw_{br_k}\right)^2}}{|BR|}$$ // root mean square distance of the projection weights of the records labeled as intrude.

The minimal, and maximal levels of the intrusion and benign scope will be assessed as follows

$$\left.\begin{aligned} \min_{ish} &= ish - d_{ish} \\ \max_{ish} &= ish + d_{ish} \end{aligned}\right\}$$ // minimal and maximal intrusion scope depicted from the projection weights of the records.

$$\left.\begin{aligned} \min_{bsh} &= bsh - d_{bsh} \\ \max_{bsh} &= bsh + d_{bsh} \end{aligned}\right\}$$ // minimal and maximal benign scope depicted from the projection weights of the records.

3.4. Predicting the label of the given record

The heuristics and their respective minimal and maximal levels depicted for labels intrusion and benign will be used further to estimate the given unlabeled record is prone intrusion scope or benign scope. The process involved to label the given record is as follows:

Let the record r to be labeled either as intrude or benign, let $rf = \{bs_1, bs_2, ..., bs_n\}$ be the set of bigram sequences of count n depicted from the given record r. The following is the equation that used to depict the projection weight of the record r towards intrusion scope.

$$pw_{r \to IR} = \frac{\sum_{i=1}^{|rf|} \left\{ pw_{bs_i} \exists bs_i \in rf \wedge bs_i \in IRF \right\}}{\sum_{j=1}^{|IRF|} \left\{ bsi_j \exists bsi_j \in IRF \right\}}$$

// the projection weight $pw_{r \to IR}$ of the record r towards intrusion scope is estimated, which is the ratio of aggregate projection weight of the bigram sequences found from record r and that are exists in optimal bigram features IRF of the intrusion scope against the total of the projection weights of all optimal bigram sequences IRF of the intrusion scope.

Similarly, the projection weight of the record r towards benign scope will be assessed as follows:

$$pw_{r \to BR} = \frac{\sum_{i=1}^{|rf|} \left\{ pw_{bs_i} \exists bs_i \in rf \wedge bs_i \in BRF \right\}}{\sum_{j=1}^{|BRF|} \left\{ bsb_j \exists bsb_j \in BRF \right\}}$$

// the projection weight $pw_{r \to BR}$ of the record r towards benign scope is estimated, which is the ratio of aggregate projection weight of the bigram sequences found from record r and that are exists in optimal bigram features BRF of the benign scope against the total of the projection weights of all optimal bigram sequences BRF of the benign scope.

Further, the given record will be labeled either as intrude or as benign by correlating the depicted projection weight of the record r for intrusion scope $pw_{r \to IR}$ with Intrusion Scope Heuristic, and projection weight $pw_{r \to BR}$ of the record r for the benign scope with Benign Scope Heuristic. The label prediction process is as follows:

$$\left.\begin{aligned} &\left(pw_{r \to IR} \geq \max_{ish}\right) or \\ &\left(pw_{r \to IR} \geq ish \wedge pw_{r \to BR} \leq bsh\right) or \\ &\left(pw_{r \to BR} \leq \min(bsh)\right) \end{aligned}\right\}$$ // if the given condition is true, then the given record predicted as intrude

$$\left.\begin{aligned} &\left(pw_{r \to BR} \geq \max(bsh)\right) or \\ &\left((pw_{r \to BR} \geq bsh) and (pw_{r \to IR} \leq \min(ish))\right) \end{aligned}\right\}$$ // if the given condition is true, then the given record predicted as benign

If the both conditions failed, then the record will be denoted as suspicious and push forward to administrative decision.

4. Experimental Study

The experimental study was done on the dataset called IoT Sentinel [34]. This dataset contains approx. million records those labeled as intrude and benign. Among these 190000 (intrude: 100000, and benign: 90000) records were considered for experimental study. In order to estimate the performance of the proposal, 75% of intrude and benign records of the chosen dataset were used in learning phase. The rest 25% of the records were unlabeled and used to perform predictive analysis. The results obtained from experimental study were listed in Table 1, which are evincing the significance of the proposed Heuristics towards intrusion detection. The detailed prediction statistics were explored in Table 2.

Table 1: The Inputs and Outcomes of the Learning Phase

Malicious Request Sequence	75000
Benign Request Sequence	67500
ish	0.575
d_{ish}	0.106
$\min(ish)$	0.476
$\max(ish)$	0.683
bsh	0.645
d_{bsh}	0.179
$\min(bsh)$	0.477
$\max(bsh)$	0.811

Table 2: The inputs and outcomes of the label prediction phase

Positives (intruded)	25000
Negatives (benign)	22500
True Positives	24688
True Negatives	19853
False Positives	2647
False Negative	312
precision	0.903
Negative Predictive Value	0.985
Accuracy	0.938
Sensitivity	0.988
Specificity	0.882

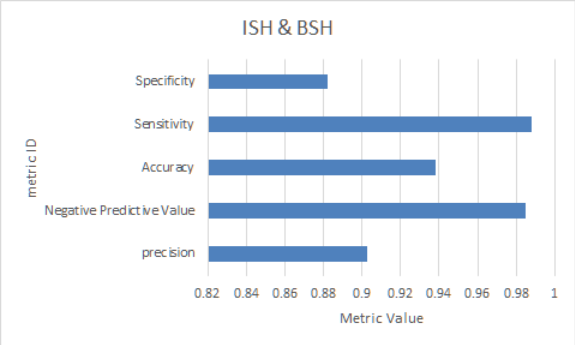


Figure 1: The metric values observed from experimental study.

The 47500 (intruded: 25000, and benign: 22500) records were used in prediction phase of the proposed model. The results obtained from the predictive analysis indicating that the truly predicted records are 44541. Among these 24688 are truly labeled as intruded, and 19853 are truly labeled as benign. Hence the true positive rate that defined by the metric called sensitivity is 0.988 (the ratio of true positives against actual positives), and the true negative rate that denotes by the metric called specificity, which is 0.882 (the ratio of true negatives against actual negatives). The total number of falsely predicted records is2959. Among these 2647 are falsely labeled as positive (intrude), and 312 records are falsely labeled as negative (benign). Hence the positive predictive value that denoted by the metric called precision is 0.903 (the ratio of true positives against the sum of true positives and false positives), and negative predictive value is 0.985 (the ratio of true negatives against the sum of true negatives and false negatives). The overall predictive accuracy is 0.938, which is the ratio of sum of true positives and true negatives against total number of records used in predictive analysis. These statistics revealing that the proposed heuristics to scale the intrusion and benign scope of the IOT network transactions are noteworthy to discriminate the IOT network traffic as intruded and benign with 94% accuracy. The depicted sensitivity of the proposal (sensitivity: 99%) indicating that the miss rate is very less. However, the fall out (false positives are high) is marginally high since the specificity is around 88%. These metric values are visualized in Figure 1.

5. Conclusion

This manuscript proposed a model to defend intrusion in IOT networks. The depicted model is a machine learning strategy that learns from training data and define Intrusion Scope Heuristic (ish), and Benign Scope Heuristic (bsh). The proposed heuristics allows to predict the given IOT network transaction is prone to intrusion or benign. The learning phase of the model depicts bigram sequences of the network transactions as features from the training records that are labelled intrude and benign respectively. Further, the respective feature sets dimensionality is reduced by retaining the optimum features and discarding the features with tawdriness. The optimum feature selection is done by using floating search technique called sequential forward selection [35]. Then the projection weights of these optimal features and respective records that labelled as intrude, and benign will be depicted in respective order. Afterwards, the proposed model uses these projection weights to define intrusion scope heuristic, and benign scope heuristic. Further, the proposal performs predictive analysis to depict the scope of the network transaction is prone to intrusion or benign. The experimental study reveals that the proposed model is significant as it evinces the 94% detection accuracy, and minimal miss rate. However, the fallout of the benign record prediction is considerably high, but it can be tolerable to achieve maximum defence of the intrusion in sensitive IOT networks. The possible future research can extend this model to work with trigram and n-gram features. On other dimension of research, the depicted heuristics can be used as fitness metrics in evolutionary computation techniques such as genetic algorithm, and cuckoo search.

References

[1] Kun, Z.,Meng, X.: (2009) Research and prevention measures of computer network security. Fujian 10, 102–103.
[2] United States General Accounting Office: (1996) Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84 Defense Information Security, Washington DC.
[3] United States General Accounting Office: (1996) Opportunities for improved OMB over sight of agency practices. GAO/AIMD Information Security, Washington DC.
[4] Conti, J.P.:(2006) The Internet of things. Commun. Eng. 4(6), 20–25.
[5] Zhou, J.: (2009) Wireless sensor network intrusion detection model research. In: CIE 16th Information Theory Academic Conference Proceedings, pp. 799–804. Electronic Industry Press, Beijing.
[6] Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on software engineering, (2), 222-232.
[7] Ariu, D., Tronci, R., & Giacinto, G. (2011). HMMPayl: An intrusion detection system based on Hidden Markov Models. computers & security, 30(4), 221-241.
[8] Koc, L., Mazzuchi, T. A., & Sarkani, S. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass

classifier. Expert Systems with Applications, 39(18), 13492-13500.
[9] Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based systems, 78, 13-21.
[10] Weller-Fahy, D. J., Borghetti, B. J., & Sodemann, A. A. (2015). A survey of distance and similarity measures used within network intrusion anomaly detection. IEEE Communications Surveys & Tutorials, 17(1), 70-91.
[11] Thottan, M., & Ji, C. (2003). Anomaly detection in IP networks. IEEE Transactions on signal processing, 51(8), 2191-2204.
[12] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: methods, systems and tools. IEEE communications surveys & tutorials, 16(1), 303-336.
[13] Theiler, J. P., & Cai, D. M. (2003, September). Resampling approach for anomaly detection in multispectral images. In Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery IX (Vol. 5093, pp. 230-241). International Society for Optics and Photonics.
[14] Chandola, V., Banerjee, A., & Kumar, V. (2012). Anomaly detection for discrete sequences: A survey. IEEE Transactions on Knowledge and Data Engineering, 24(5), 823-839.
[15] Casas, P., Mazel, J., & Owezarski, P. (2012). Unsupervised network intrusion detection systems: Detecting the unknown without knowledge. Computer Communications, 35(7), 772-783.
[16] De la Hoz, E., De La Hoz, E., Ortiz, A., Ortega, J., & Prieto, B. (2015). PCA filtering and probabilistic SOM for network intrusion detection. Neurocomputing, 164, 71-81.
[17] Bostani, H., & Sheikhan, M. (2017). Modification of supervised OPF-based intrusion detection systems using unsupervised learning and social network concept. Pattern Recognition, 62, 56-72.
[18] Guo, C., Ping, Y., Liu, N., & Luo, S. S. (2016). A two-level hybrid approach for intrusion detection. Neurocomputing, 214, 391-400.
[19] Horng, S. J., Su, M. Y., Chen, Y. H., Kao, T. W., Chen, R. J., Lai, J. L., & Perkasa, C. D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert systems with Applications, 38(1), 306-313.
[20] Tan, Z., Jamdagni, A., He, X., Nanda, P., & Liu, R. P. (2014). A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE transactions on parallel and distributed systems, 25(2), 447-456.
[21] Pajouh, H. H., Dastghaibyfard, G., & Hashemi, S. (2017). Two-tier network anomaly detection model: a machine learning approach. Journal of Intelligent Information Systems, 48(1), 61-74.
[22] Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications, 67, 147-165.
[23] Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications, 74, 98-120.
[24] Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. IEEE transactions on computers, 65(10), 2986-2998.
[25] Daryabar, F., Dehghantanha, A., Udzir, N. I., & bin Shamsuddin, S. (2012, June). Towards secure model for SCADA systems. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on (pp. 60-64). IEEE.
[26] Pan, S., Morris, T., & Adhikari, U. (2015). Developing a hybrid intrusion detection system using data mining for power systems. IEEE Transactions on Smart Grid, 6(6), 3104-3113.
[27] Zhou, C., Huang, S., Xiong, N., Yang, S. H., Li, H., Qin, Y., & Li, X. (2015). Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 45(10), 1345-1360.
[28] Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. Journal of Network and Computer Applications, 49, 112-127.
[29] Ning, H., Liu, H., & Yang, L. T. (2015). Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Transactions on Parallel and Distributed Systems, 26(3), 657-667.
[30] Cao, X., Shila, D. M., Cheng, Y., Yang, Z., Zhou, Y., & Chen, J. (2016). Ghost-in-ZigBee: Energy depletion attack on ZigBee-Based wireless networks. IEEE Internet of Things Journal, 3(5), 816-829.
[31] Chen, Q., Abdelwahed, S., & Erradi, A. (2014). A model-based validated autonomic approach to self-protect computing systems. IEEE Internet of Things Journal, 1(5), 446-460.
[32] Teixeira, F. A., Machado, G. V., Fonseca, P. M., Pereira, F. M. Q., Wong, H. C., Nogueira, J. M. S., & Oliveira, L. B. (2015). Defending Internet of Things against Exploits. IEEE Latin America Transactions, 13(4), 1112-1119.
[33] Jović, A., Brkić, K., & Bogunović, N. (2015, May). A review of feature selection methods with applications. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on (pp. 1200-1205). IEEE.
[34] Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017, June). IoT Sentinel: Automated device-type identification for security enforcement in IoT. In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on (pp. 2177-2184). IEEE.
[35] Somol, P., Pudil, P., Novovičová, J., & Paclık, P. (1999). Adaptive floating search methods in feature selection. Pattern recognition letters, 20(11-13), 1157-1163.