ISSN (E) : 2616 – 7808 I ISSN (P) : 2414 - 7419

مجلة كلية الكوت الجامعة

K.U.C.J

Vol. 5 Issue 1 2020 5th Year

Determining of Robust Factors for Detecting IoT Attacks

Rawaa Ismael Farhan **Dr. Nidaa Flaih Hassan** **Dr. Abeer Tariq Maolood**

Computer Science Collage / University of Technology

ralrikabi@uowasit.edu.iq nidaaalalousi5@yahoo.com 110032@uotechnology.edu.iq

Abstract

The detection of novel intrusion types is the target of cyber security, therefore best secured network is become very necessary. The Network Intrusion Detection Systems (NIDS) must address the real-time data, since security attacks are expected to be increased substantially in the future with the Internet of Things (IoT).

Intrusion detection approaches in this time, which depends on matching patterns of packet header information have decreased their effectiveness. This paper is focused on anomaly-based intrusion detection system, where NIDS detects normal and malicious behavior by analyzing network traffic, this analysis has the potential to detect novel attacks**.** Robust factors are used for evaluating these attacks by covering previous researches, these factors are: "high accuracy rate", "high detection rate"(DR) and "low false alarm report"(FAR), these factors influence on NIDS performance.

Keywords: Internet of Things (IoT), Intrusion Detection System (IDS), Deep learning (DL), Machine learning (ML).

تحديد العوامل القوية في الكشف عن هجمات إنترنت الأشياء

م.م. رواء اسماعيل فرحان ا.م.د. نداء فليح حسن ا.م.د. عبير طارق مولود

كلية علوم الحاسوب / الجامعة التكنولوجية

ralrikabi@uowasit.edu.iq nidaaalalousi5@yahoo.com 110032@uotechnology.edu.iq

خلاصــة

يعد اكتشــاف أنواع التسـلل الجديدة هدفًا للأمن السـيبراني، حيث بات من الضــروري توفيرأفضـل شـبكة آمنة. ان أنظمة كشـف التسـلل عبرالشـبكة (NIDS) يجب ان تتعامل مع البيانات في الوقت الفعلي، بسـبب توقعات في زياده الهجمات الأمنية بشـكل كبيرفي المسـتقبل باستخدام إنترنت الأشياء (IoT).

أساليب كشف التسلل في هذا الوقت والتي تعتمدعلى مطابقة أنماط معلومات رأس الحزمة قلت فاعليتها. تركزهذه الورقةعلى نظام كشف التسلل القائم على الحالات الشاذة، حيث (NIDS) السلوك العادي والضــارمن خلال تحليل حركة مرورالشبكة، وهذاالتحليل لديه القدرة على اكتشـــاف الهجمات الجديدة. تســتخدم عوامل قوية لتقييم هذه الهجمات من خلال تغطية الأبحاث الســـابقة، وهذه : معدل دقة عالية ومعدل اكتشاف مرتفع وتقريرإنذارخاطئ منخفض، تؤثرهذه العوامل على أداء NIDS.

الكلمات المفتاحية: إنترنت الأشياء ، نظام كشف التسلل ، التعلم العميق ، تعلم الماكنة .

1. Introduction

Internet of Things (IoT) is a revolutional development in Internet and communication, that allows to physical devices to be connected to each other over the Internet [1], Figure 1 depicts the main architecture of it.

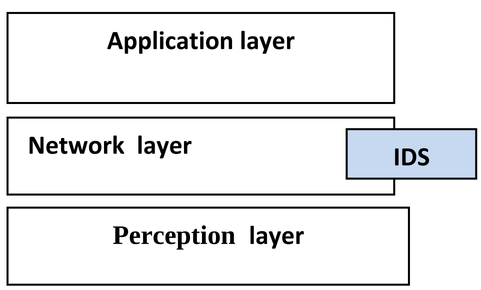

Figure 1. Architecture of IoT [1].

Future of the IoT in the integration with the Artificial intelligence (AI), both are making human life more comfortable, since they made everything smart and there is no need for human intervention [2].

The potential unauthorized access to information and new attacks will increase by 2020, when up to 50 billion devices may be connected according to Gartner. Weaknesses in Internet protocols and the loss of sufficiently robust mathematical analysis methods have led to increased attacks as systems are adopted in IoT [3].

Security is considered the main challenge of IoT, and Real –time data generated from IOT need analysis. Deep learning which improves neural networks is considered the best for analyzing real-time solutions in (IoT), it mimics the human mind for its ability to self-learn from accumulated experiences.

In this paper, many researches are discussed with their challenges, in addition, a research agenda is proposed to address these challenges and highlighted the robust factors in the detection of IoT attacks.

2. Network Intrusion Detection System (NIDS)

Network Intrusion detection systems (NIDS) are the first line of defense in the network, its often suffer from practical testing and evaluation due to the lack of rich dataset [4]. Typically, the traffic of network is picked up in both packet and stream format, traffic of network is typically picked up at the packet level by copying ports on network devices, and its data contains information of payload, stream -based data is contained metadata of network connections only [5].

Firewalls and authentication methods are used to protect and prevent unauthorized access to the systems, but these methods are lost the abilities to monitor the network traffic, where most of the attacks are existing. These attacks may be created by disgruntled employees who have legitimate network access then used the privilege to destruct [6]. Figure 2 depicts the location of Intrusion Detection System in the network after firewall.

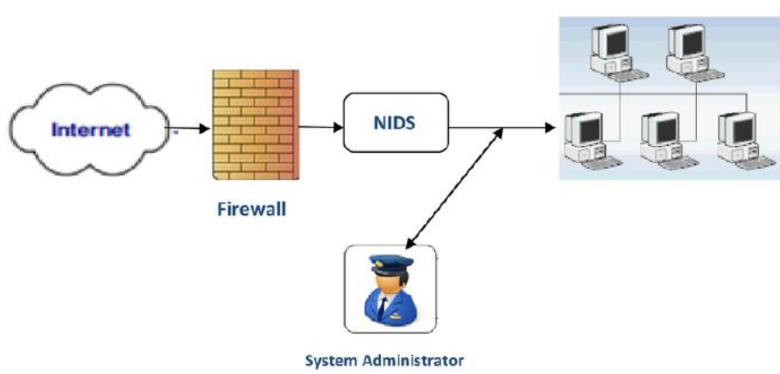

Figure 2. Intrusion Detection System [6].

There are two types of IDSs, these two types are classified according to the detection technique, they are:

1. Anomaly-Based Detection**:** ID Search network traffic to detect abnormal traffic.

2. Misuse Detection or Signature-Based Detection: It is a method that uses unauthorized behavior as known patterns that are called signatures to detect similar attempts [7].

Figure 3 presents a general classification of an Intrusion Detection System According to Implementation method, Architecture and Detection method [8].

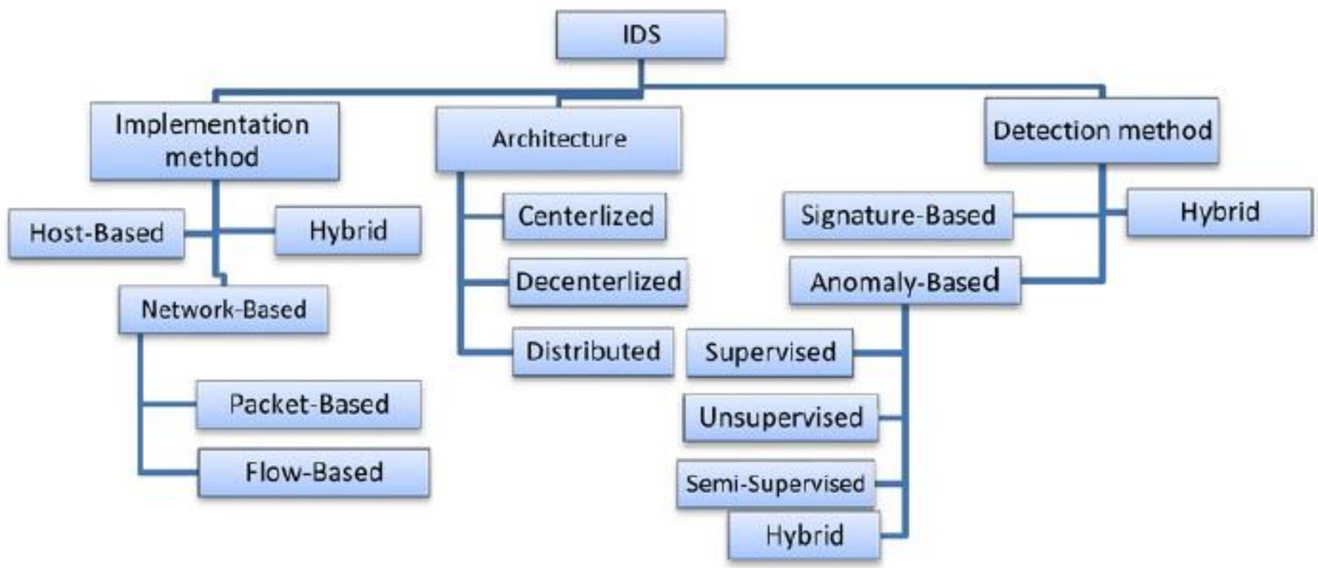

Figure 3. General Classification of Intrusion Detection System [8]

In this paper, anomaly-based NIDS is considered, because it is able to detect new threats which occur in IoT. The NIDS analyzed network traffic and detected new and unknown attacks. The feature set design important to identify network traffic, and it is an ongoing research problem [9].

Restrictions of application systems are required to process data in real- time, not batches. The nature of the stream data shows deviation, favoring algorithms that learn ongoing, by using Numenta Anomaly Benchmark (NAB) which consist of streams with labeled anomalies, benchmark containing real-world data [10].

Training and evaluating anomaly-based NIDS are used Labeled data sets. As in [11,12] datasets for (NIDS) network based intrusion detection are surveid, which presented in details with network data based on packet and flow, thesis researches has presented 15 different properties for evaluating data sets for specific situations, the presentation identified sources for network-based data, like repositories of traffic with traffic generators.

3. Techniques to Design NIDS

In this section, number of machine learning techniques are discussed, these techniques are consider as most common **Machine Learning Techniques (ML)** , such as Decision Tree (DT), Support Vector Machine (SVM), Bayesian Algorithm, K-Nearest Neighbor and Principal Component Analysis (PCA).In addition, **Deep Learning (DL)** are also described such as(Auto Encoder(AE),Variant Auto Encoder(VAE),Deep Belief Networks (DBN), Convolutional neural network (CNN), Recurrent neural network (RNN), Long –Short term Recurrent neural network (LSTM),Bi directional Recurrent neural network (BRNN), Gated Recurrent Units (GRU) and Generative Adversarial Network (GAN)) . Finally, **other NIDS techniques** such as Data mining and Swarm intelligence are also described.

A. Machine Learning Techniques (ML)

Embedded intelligence in the IoT devices and networks are able to be supplemented by ML and DL techniques to manage many security problems. In [13] some of recent ML/DL techniques with IoT are reviewed from security point view. Due to big data challenges facing Intrusion Detection, [14] provided feature selection with high classification efficiency, this selection is educed computational costs. In [15] Hidden Markov Models (HMM) is used, which is one of statistical machine learning (ML) methods, they developed two architectures that can detect and track progress of attacks in real-time, database of HMM templates is developed, which presented diverse performance and complexity. The classifier is applied by using decision tree with "Feature grouping based on linear correlation coefficient" (FGLCC) algorithm and "cuttle fish algorithm" (CFA) is used in [16].

To deal with heterogeneous and large-scale data, [17] proposed hybrid approach for intrusion detection by using dimensionality reduction technique integrated with "information gain" (IG) method and "principal component analysis" (PCA), classifier is ensemble by Applying "Support Vector Machine"(SVM), "Instance-based learning algorithms" (IBK), and "Multilayer Perceptron"(MLP).

B. Deep learning Techniques (DL)

Deep learning is artificial neural networks with multi-layers to produce best accuracy in many domains such as object detection, language translation and speech recognition, in this section recent researches are reviewed focusing on using DL.

As with [18] DL differs from classical ML methods due to the ability to self-learn from data without need to human's knowledge or coded commands, thus it could understand from raw data such as text, image and video because its flexible architectures, while DL is provided with more data, their predictive accuracy is increased. Deep learning models can enhance performance of IDS as presented in [19], also all the IDS associated definitions are provided, with an explanation of different IDS types, where detection module are puted and the used approach. According to [20] a sparse auto-encoder and softmax regression based NIDS was implemented, they used benchmark network intrusion dataset - NSL-KDD to evaluate anomaly detection accuracy.

In [21] SDN has given a potential to make strong secured network and also made a dangerous increasing in attacks chances, with the explanation of potential of using DL for anomaly detection system based on flow. A survey about IoT architecture presented in [22], emerging security vulnerabilities with their relation to the layers of the IoT architecture are also presented.

In [23] declared that deep learning techniques has the ability to handle big data. Big data and obtaining data reflected real challenges to IDS based on machine learning. It showed some IDSs limitations which used old machine methods used to construct, extract and select features. To get rid these challenges, it showed some IDSs with deep learning techniques.

An overview of the recent work of deep learning techniques with network anomaly detection is provided in [24], it also discussed their local experiments showing the feasibility of the deep learning in network traffic analysis.

In [25] understanding how to use deep learning are declared by overview some IDSs which adopted deep learning approaches executed in intrusion detection, with their limitations, advantages and disadvantages.

In [26,27,28], Modelling network traffic used "long short-term memory" (LSTM) recurrent neural networks as supervised learning method, used known normal and abnormal behavior, improved intrusion detection.

In [29], the Paper proposed a hybrid model, this hybrid is composed from Recurrent Neural Network (RNN) with Restricted Boltzmann Machines (RBM). This hybrid regarded malicious traffic detection as a classification task without feature engineering.

In [30] a method is suggested based on CNN to execute intrusion detection, using CNN leads to extract complex features automatically in continually changing environments, which is so necessary in network intrusion detection.

In [31] improved user trust by making the DNN-IDS more communicative, since the black-box nature of DNNs inhibits transparency of the DNN-IDS, which is essential for building trust. The user declared input features which are most relevant in detecting every type of intrusion by training DNN-IDS.

As in [32] described a new IDS called the "hierarchical spatial-temporal features-based intrusion detection system" (HAST-IDS). Firstly, the traffic of network represented spatial features in low-level which learned using deep "convolutional neural networks" (CNNs) then temporal features in high-level is learned using "long short-term memory" (LSTM).

[33] More deep learning approaches have been used for IDS, three models are evaluated on their accuracy and precision, a "vanilla deep neural net" (DNN), "Self-Taught Learning"(STL) approach, and "Recurrent Neural Network" (RNN) based "Long Short Term Memory" (LSTM).

[34] Proposed a new deep learning technique within the youth network for detecting attacks using "Bi-directional Long Short-Term Memory Recurrent Neural Network" (BLSTM RNN).

[35] This paper proposed optimization on structure of DBN’s network, at first " Particle Swarm Optimization" (PSO) is designed used learning factor and adaptive inertia weight. Then the fish swarm behavior provided to develop the PSO and found the optimization solution initially.

[36] A proposed system used Deep Learning technique which applied a combination fusion of Random Forest (RF) Algorithm and Decision Tree (DT) Classifiers, which reduced irrelevant features and detected attacks with a better accuracy.

In [37] It proposed hybrid framework of DNN called "Scale-Hybrid-IDS-AlertNet" (SHIA) used to monitor traffic of network in real time and events in host-level effectively, this SHIA is alert probable cyber-attacks.

C. Other (NIDS) Techniques

Other techniques such as swarm intelligence, data mining techniques and genetic algorithms are used for designing NIDS, the following section is described most recent researches:

In [38] Swarm intelligence has been combined with data mining techniques to configure strong methods for detecting and identifying data flow efficiently. Since, Networks of IoT have been secured using authentication ways and encryption ways, but they are not secured versus attacks of cyber, therefore detection based on anomaly bear the liability to decrease risk of attacks types. [39] The proposed work, used firefly algorithm for feature selection. The resulted features are submitted to the classifier then provided C4.5 and "Bayesian Networks" (BN) for attack classification. Paper [40] showed an intrusion detection model based on Deep Belief Network improved by Genetic Algorithm into multiple iterations of the GA, have faced various types of attacks. This paper [41] suggested a fuzzy aggregation method used the deep belief networks (DBNs) and modified density peak clustering algorithm (MDPCA). MDPCA is used to divide the training set into various subsets to reduce the size and imbalanced samples with similar sets of attributes. Each subset trained on its sub-DBNs classifier. [42] This paper showed a hybrid method for an anomaly network-based IDS by using AdaBoost algorithms and Artificial Bee Colony (ABC), this hybrid method gained a low false positive rate (FPR) and high detection rate (DR).

4. Intrusion Detection System (IDS) and IoT

The implementation of classical IDS technologies on the IoT environment showed obvious complexity, due to the nature of resources constrained in IoT devices and their use of special protocols. Attackers exploit the big IoT potential to develop methods to threaten privacy and security [43].

In [44] presented a complete study of current intrusion detection systems, according to three factors: cost of computation, consumption of energy and privacy. [45] Based on accurate analysis of the existing intrusion detection methods**.** The paper divided into two parts: part one contained algorithm of mining anomaly to detect anomalous data in perception layer, which the second part contained a distributed scheme of intrusion detection of the detected anomalies.

The great dynamic distribution in IoT made an online manner of anomaly detection so difficult, thus in [46] proposed a new IDS, which is used ML algorithms for detection anomaly in IoT , the platform provided "security as a service " for detection, with a simplification to the collaboration between protocols used in IoT.

[47] Presented an online anomaly learning using the reversible-jump MCMC learning, forecasting mechanism, then Network Utility Maximization (NUM) theory is used for structural analysis of it.

[48] Risk Analysis and examined the security threats for each layer, related to this process, suitable procedures and their limitations of IoT protocols are specified.

In paper [49] a new model for intrusion detection is suggested, which is used Principal Component Analysis (PCA) to reduce dataset dimensions from a great number of features to a small number, also online machine learning algorithm is used as a classifier.

According to [50] determined that current data sets (KDD99 and NSLKDD) do not provide acceptable results, because of three main issues, it lost the modern attack patterns, it lost modern scenarios of traffic streams and distributed sets of training and testing is difficult. Therefore, UNSW-NB15 dataset has been generated to address these issues.

In [51] the system uses a structured Self-Organizing Maps (SOM) to classify real-time Ethernet network data. [52] Proposed that "variant-gated recurrent units" are learned packet payload with header features of network automatically, E-GRU and E-BinGRU are new techniques never used for network intrusion detection previously. The E-BinGRU reduces the required size of memory and used bit-wise calculations in most arithmetic operations.

5. NIDS on IoT using Deep Learning

The improvement in CPU work and neural network algorithms made the application of DL more practical. The use of DL for attack detection in the IOT could be a flexible to novel attacks due to of its capability of feature extraction in high-level. [53] showed that centralized detection system is assessed versus the distributed attack detection based IoT/Fog. The experiments proved that distributed attack detection system is better than centralized detection systems using deep learning model. In [54] this paper aims to solve some smart city problems based on a home automated systems, the resulted data from IoT are bulk. It used UCI data set of German credit card, Data set of 12 months taken from Temperature sensor, Images of persons walkways).

According to [55] a new detection framework is presented using simulation for proving its scalability and real-network traffic for proving the concept. The detection options provided "security as a service" and simplifies interoperability between IoT protocols.

In [56] suggested system is created by applying artificial intelligence on a Detect botnet attacks because increasing threats on banking services and financial sectors. The proposed system uses the latest IDS Dataset in 2018 which isa real time dataset (CSE-CIC-IDS2018), created by the Canadian Institute for Cyber Security (CIC) on the environment of AWS (Amazon Web Services). As in [57] show a new deep learning technique within the youth network for detecting attacks using" Bi-directional Long Short-Term Memory Recurrent Neural Network" (BLSTM RNN). In [58] light-weight distributed security solution is presented to improve IoT architecture, analyzing the approaches of ML and DL on the IoT and Cyber Security, and evaluating Networks (LSTM and GRU) for each layer in the architecture of IDS dataset. Table1. Show the Comparative analysis of existing NIDS for IOT explain the approach used on the data set and evaluated according to Accuracy, Detection Rate (DR), False Alarm Rate (FAR).

TABLE (1): Comparative analysis of existing NIDS for IOT

Ref.	Approach	Descriptive Concepts	Dataset	Accuracy	DR	FAR
25	LSTM	Network trained with 8 features and all attacks with the lowest MSE on test data.	DARPA/ KDDCup'99	NA	0.993	0.072
27	RNN	This reference Usedrecurrent neural network	NSL-KDD	NA	DOS 83.49 R2L 0.80 U2R 0.07 Prop 2.16	2.06 24.69 11.50 83.40
50	DT LR NB ANN	Four existing classifiers are used to evaluate the complexity	UNSW-B15	85.56 83.15 82.07 81.34	NA	15.78 18.48 18.56 21.13
23	1.AK16a (ANN) 2.AK16b (Softmax Regression) 3.AK17 (K-means Clustering) 4.ACTYK17 (SVM, DT, ANN) 5.KKSG15	1.use SAE for classifying and clustering approaches. 2. Adopted a feature selection by ANN. 3. SAE extractions and weighted selection are combined. 4. SAE improved the IDS performance than to KKSG15.	"Aegean Wi-Fi Intrusion Dataset " (AWID)	NA	65.178 92.674 92.180 99.918 22.008	0.143 2.500 4.400 0.012 0.021
24	Fully connected	Train+/Test+ Train20/Test+ Train+/Test−	NSL-KDD	DOS 89.4 R2L 90.4 U2R 83.0	NA	NA

	neural network model(FCN)	Train20/Test–		Prob 84.2		
49	(PCA)&k-Nearest	This reference used Principal Component Analysis (PCA) to reduce the dimensions of the datasetand to develop the classifier.Softmax regression and k-nearest applied	KDDCup 99	84.406	99.312	1.116
58	(LSTM and GRU)	Improveits architecture and proposed a light-weighted and multi-layered design of an IoT network	DARPA/KDDCup '99	97.618	NA	0.0257
9	ANN	Backpropagation algorithmis used.	kDDCUP99	0.97	0.9	0.99
17	IG-PCA Ensemble method	Proposed a new hybrid technique for dimensionality reduction that combiningprincipal component analysis (PCA) &information gain (IG),(MLP) ,(SVM)& Instance-based learning algorithms (IBK) approaches .	ISCX 2012 NSL-KDD Kyoto2006+.	1.IG-PCA-SVM 98.82 2.IG-PCA-IBK 98.72 3.IG-PCA-MLP 98.66 4.IG-PCA-ensemble 99.01	0.988 0.986 0.987 0.991	0.011 0.011 0.014 0.010
28	(RNN) & (RBM)	Proposed a hybrid model that combines a recurrent neural network (RNN) with restricted Boltzmann machines (RBM)	ISCX-2012 DARPA1998	98.61 97.82	94.90 95.21	0.07 0.17
29	RNN	Using different models of deep Recurrent Neural Network (BLSTM, LSTM, BRNN, RNN)	NSL-KDD	NA	NA	NA

30	CNN & LSTM	Hierarchical spatial-temporal features-based on intrusion detection system (HAST-IDS) by using (CNNs) to learn the low-level spatial features of network traffic and then learns high-level temporal features using (LSTM) networks	DARPA1998 ISCX2012	41.7 97.2	0.00 0.00	0.00 0.00
31	(MLP)	Binary and multi-class classification was carried out on the dataset	KDD-NSL	94.83	NA	NA
33	BLSTM.	It used Deep Learning Neural Network of multi-layer.	UNSWNB15	0.9571	2.19	0.00
39	Firefly algorithm,(BN) and C4.5	The firefly algorithm to select the features. Then resulted features are submitted to Bayesian Networks (BN)and C4.5	KDDCUP 99	NA	17.24	0.00
15	(FGLCC)&(CFA)	IDS used feature grouping based on "linear correlation coefficient (FGLCC) " &"algorithm and cuttlefish algorithm (CFA)"	KDDCup 99	99.85	99.84	0.19
18	CorrCorr a feature selection method	Features selected with a Principal Component Analysis (PCA) and a Pearson class label correlation	UNSW-NB15 NSL-KDD	91.50	39.60	0.40
26	LSTM	Proposed newmechanism to extract "packet semantic meanings "with LSTM to learn "the temporal relation among fields in the packet header ".	ISCX2012 USTC-TFC2016	99.99 99.99	NA	$7.46X10^{7}$ $1.1 X10^{7}$

35	DBN&PSO& fish algorithm	Optimizing the structure of DBN(Deep BelieveNetwork). Execute a PSO (Particle Swarm Optimization) which depends on learning factor &weight. Then, is used the fish swarm for clustering.	NSL-KDD	80.4 84.0 NA 0 0	Pro p 3.55 DO S 87.2 U2 R 84.0 R2L 80.4	0.77 5.64 0.17 3.02
37	DNN	Hyper parameter selection methods used to select optimal parameters and topologies for DNNsare chosen	NSL-KDD UNSW-NB15 Kyoto WSN-DS CICIDS2017	0.789 0.761 0.885 0.982 0.931	NA	NA
40	DBN & GA	Proposed Deep Belief Network (DBN)with improving on Genetic Algorithm (GA).	NSL-KDD	DoS 99.45 Prob99.37 R2L 97.78 U2R 98.68	99.7 99.4 93.4 98.2	0.8 0.7 7.3 1.8
41	(MDPCA)and deep belief networks (DBNs).	Fuzzy aggregation approach using modified density peak clustering algorithm (MDPCA) and deep belief networks (DBNs).	NSL-KDD UNSW-NB15	82.08	NA	2.62
56	ANN	Detect a classification of botnet attack	IDS2018	0.99975	NA	NA

Conclusion

The DL outperformed traditional machine learning methods in network intrusion detection applications (NIDS), because of its ability to analyze big data with high accuracy which resulting from its potential in self-learn from real-time data. In addition, DL mimics the ability of human mind to learn by accumulated experiences, thus its enable to discover zero-day attacks. However, there are challenges of (NIDS) in IoT, such as globally accessible, restricted resources (Memory, Battery, CPU and Bandwidth), in addition using recent protocols such as (COAP, Zigbee, PRL and 6LoWPAN).

In order to make NIDS on IOT environment more effective, real data sets are recommended to obtain real results that are relevant to the dynamic nature of IoT. Optimization must be made on Deep learning technique by using feature selection methods to select the most relevant features in the large real data sets. This optimization will reduce false alarm rate and increase detection rate and accuracy.

References

[1] Somayya Madakam, R. Ramaswarmy, S. Tripathi, "Internet of things (IOT): A Literature Review ", Journal of computer and communications, 2015, 3, 164-173.

[2] Akash Shukla, Himansho Sharma, Ankita Singh, "Future of Internet of Things: Trends, Challenges & Insight to Artificial Intelligence", International Journal of Advanced Research in Computer: Volume 9, special issue No. 2, April 2018.

[3] Glenn A. Fink, Dimitri V. Z., Thomas E. Caroll, "Security and Privacy Grand Challenges for the Internet of things", IEEE, 2015.

[4] Babatunde, R.S., et al.," development an of intrusion detection system in a computer network", international journal of computers & technology, Vol 12, No. 5.

[5] Prasanta Gogoi, Monowar H. Bhuyan, "Packet and Flow Based Network Intrusion Dataset ", 2012.

[6] Ho, Swee Yenn (George), "Intrusion Detection - Systems for today and tomorrow", SANS Institute 2019, Version 1.2e.

[7] Eric Li, "Intrusion Detection Systems ", ACC 621: IT Assurance & Computer Assisted Auditing,2010.

[8] A. NisIoTi, A. Mylonas, V. Katos,"From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods", IEEE 2018.

[9] Shawq M. Mehibs, Soukaena H. Hashim, "Proposed Network Intrusion Detection System in Cloud Environment Based on Back Propagation Neural Network", Journal of Babylon university/Pure and Applied Sciences / No. (1)/ Vol. (26): 2018.

[10] Subutai Ahmad, Alexander Lavin, Scott Purdy, Zuha Agha," Unsupervised real-time anomaly detection for streaming data", ELSEVIER, Neurocomputing 262 (2017) 134–147.

[11] Markus Ring, Sarah W., Deniz Scheuring, Dieter Landes," A Survey of Network-based Intrusion Detection Data Sets",arXiv: 1903.02460 v1 [Cs. CR] 6 Mar 2019.

[12] Hanan Hindy, David Brosset, Ethan Bayne, "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets", arXiv: 1806.03517 v1 [Cs. CR] 9 Jun 2018.

[13] Mohammed Ali Al-Garadi, et al. , "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security".

[14] Richard Zuech and Taghi M. Khosh goftaar, "A survey on feature selection for intrusion detection", 21st ISSAT International Conference on Reliability and Quality in Design August 6-8, 2015 - Philadelphia, Pennsylvania, U.S.A.

[15] Tawfeeq Shawly, Ali Elghariani, Jason Kobes and Arif Ghafoor, "Architectures for Detecting Real-time Multiple Multi-stage Network Attacks Using Hidden Markov Model "

[16] Sara Mohammadi, Hamid Mirvaziri, Mostafa Ghazizadeh-Ahsaee, Hadis Karimipour " Cyber intrusion detection by combined feature selection algorithm", Journal of Information Security and Applications 44 (2019) 80–88, Elsevier.

[17] Fadi Salo, Ali Bou Nassif, Aleksander Essex, Dimensionality Reduction with IG-PCA and Ensemble Classifier for Network Intrusion Detection, *Computer Networks* (2018), doi:https://doi.org/10.1016/j.comnet.2018.11.010

[18] Florian Gottwalt, Elizabeth Chang, Tharam Dillon, Corr: A Feature Selection Method for Multivariate Correlation Network Anomaly Detection Techniques, Computers & security, doi:https://doi.org/10.1016/j.cose.2019.02.008

[19] Kwangjo Kim, Muhamad Erza, Harry Chaandra, "Network Intrusion Detection using Deep Learning: A Feature Learning Approach", Springer Briefs on Cyber Security Systems and Networks, ISBN 978-981-13-1444-5,2018.

[20] Quamar N., Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam, "A Deep Learning Approach for Network Intrusion Detection System", Conference Paper in Security and Safety, December 2015.

[21] Tang, TA, Mhamdi, L, McLernon, D et al. "Deep Learning Approach for Network Intrusion Detection in Software Defined Networking, International Conference on Wireless Networks and Mobile Communications (WINCOM). 26-29 Oct 2016, Fez, Morocco IEEE.

[22] Mohamed Faisal Elrawy, Ali Ismail Awad and Hesham F. A. Hame, "Intrusion detection systems for IoT-based smart environments: a survey", Journal of Cloud

Computing: Advances, Systems and Applications, Springer ,2018.

[23] Kwangjo Kim, Muhamad Erza Aminanto, "Deep Learning in Intrusion Detection Perspective: Overview and Further Challenges", 2017 IEEE.

[24] Dongh woon Kwon, Hyunjoo Kim, Jinoh Kim, Sang C. Suh, Ikkyun Kim , Kuinam J. Kim, "A survey of deep learning-based network anomaly detection", published online: 27 Sep 2017, Springer.

[25] Kwangjo Kim, Muhamad Erza Aminanto, "Deep Learning in Intrusion Detection Perspective: Overview and Further Challenges", 2017 IEEE.

[26] Ralf C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection", SACJ No. 56, July 2015.

[27] Ren-Hung Hwang, Min-Chun Peng, Van-Linh Nguyen and Yu-Lun Chang, "An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level", Applied Science, MDPI. 2019, doi: 10.3390/app 9163414

[28] Gyuwan Kim, Hayoon Yi, Jangho Lee, Yunheung Paek, Sungroh Yoon, "Lstm-Based System-Call Language Modeling Nd Robust Ensemble Method for Designing Host-Based Intrusion Detection Systems",ar Xiv:1611.01726v1 [Cs.CR] 6 Nov 2016.

[29] Chaopeng Li1, 2, Jinlin Wang1, Xiaozhou Ye1," Using a Recurrent Neural Network and Restricted Boltzmann Machines for Malicious Traffic Detection", Neuro Quantology, May 2018, Volume 16 Issue 5 Page 823-831,
doi: 10.14704/nq.2018.16.5.1391.

[30] Lin Zhang, Meng Li, Xiaoming Wang, Yan Huang," An Improved Network Intrusion Detection Based on Deep Neural", Network IOP Conference Series: Materials Science and Engineering. ,2019 .

[31] Kasun Amarasinghe, Milos Manic, "Improving User Trust on Deep Neural Networks Based Intrusion Detection Systems", Conference Paper November 2018 IEEE.

[32] Wei Wang, Yiqiang Sheng, Jinlin Wang, "HAST-IDS: Learning Hierarchical Spatial-Temporal Features using Deep Neural Networks to Improve Intrusion Detection", IEEE December 2017,
DOI:10.1109/ACCESS.2017.2780250.

[33] Lee, Brian; Amaresh, Sandhya; Green, Clifford; and Engels, Daniel (2018) "Comparative Study of Deep Learning Models for Network Intrusion Detection," SMU Data Science Review: Vol. 1: No. 1, Article 8.

[34] Bipraneel Roy, Dr. Hon Cheung, "A Deep Learning Approach for Intrusion Detection

in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network", 2018 28th international Telecommunication Network Communication Conference (ITANC).

[35] Peng Wei, Yufeng Li, Zhen Zhang, Tao Hu, ZiyongLi, and Diyang Liu " An Optimization Method for Intrusion Detection Classification Model based on Deep Belief Network", DOI 10.1109/ACCESS. 2019.2925828, IEEE.

[36] V. Kanimozhi, Prem Jacob,"UNSW-NB15 Dataset Feature Selection and Network Intrusion Detection using Deep Learning ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-5S2, January 2019.

[37] Vinaya kumar R, Mamoun Alazab, Soman K. p., Prabaharan P., Ameer Al-Nemrat "Deep Learning Approach for Intelligent Intrusion Detection System", DOI: 10.1109/ACCESS.2019.2895334, IEEE.

[38] Sanju Mishra, Rafid Sagban, Ali Yakoob & Niketa Gandhi (2018): Swarm Intelligence in anomaly detection systems: an overview, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2018.1521895.

[39] Selvakumar B., Muneeswaran K.," Firefly algorithm based Feature Selection for Network Intrusion Detection", Computers & Security (2018), doi: https://doi.org/10.1016/j.cose. 2018.11.005.

[40] Ying Zhang, Peisong Li and Xinheng Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network", DOI :10.1109/ACCESS.2019.2903723, IEEE.

[41] Yanqing Yang, Kangfeng Zheng, Chunhua Wu, Xinxin Niu and Yixian Yang, "Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks ",Applied Science, MDPI. 2019, 9, 238; doi:10.3390/app 9020238.

[42] MaziniM., Shirazi B., Mahdavi, I., Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and Ada Boost algorithms, Journal of King Saud University – Computer and Information Sciences (2018), doi: https://doi.org/10.1016/j.jksuci. 2018.03.011.

[43] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani and Sean Carlisto, " A Survey of Intrusion Detection in I internet of Things", Journal of Network and Computer applications, http://dx.doi.org/10.1016/j.jnca. 2017.02.009.

[44] Junaid Arshad, Muhammad A. Azad, Khaled Salah, Wei Jie, RaziIqbal, Mamoun Alazab,

"Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT", arXiv:1812.09160v1 [Cs. CR] 21 Dec 2018.

[45] Rongrong Fu, Kang Feng Zheng, Dongmei Zheng, Yixian Yang, "An Intrusion Detection Scheme Based on Anomaly Mining in Internet of Things".

[46] Sheven Chawla, Geetha priya Thamilarasu,"Security as a Service: Real-time Intrusion Detection in Internet of Things", ACM ISBN 978-1-4503-6406-5/18/04, https:// doi.org/10.1145/3212687. 3212872,2018.

[47] Jun Ping Wang, Shihui Duan, "An Online Anomaly Learning and Forecasting Model for Large-Scale Service of Internet of Thing", 2014 International Conference on Identification, Information and Knowledge in the Internet of Things.

[48] Panag IoT is I., Panag IoT is G., Ioannis D., " Securing the Internet of Things: Challenges, threats and solutions", Internet of Things 5 (2019) 41–70, Elsevier.

[49] Shengchu Zhao, Wei Li, Tanveer Zia and Albert Y. ," A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things", 2017 IEEE. 15th Intl Conf on Dependable, Autonomic and Secure Computing.

[50] Nour Moustafa & Jill Slay (2016): The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set, Information Security Journal: A Global Perspective, DOI:10.1080/19393555.2015.1125974.

[51] Khaled Labib and Rao Vemuri, " NSOM: A Real-Time Network-Based Intrusion Detection System Using Self-Organizing Maps".

[52] Yiran Hao, Yiqiang Sheng, Jinlin Wang, "Variant Gated Recurrent Units with Encoders to Preprocess Packets for Payload-Aware Intrusion Detection", IEEE April 25, 2019..

[53] A.A. Diro, N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things", Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.043

[54] N. Rakesh, "Performance analysis of Anomaly detection of different IoT datasets using cloud micro services".

[55] Geetha priya Thamilarasu and Shiven Chawla, "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things", MDPI, Sensors 2019, 19, 1977; doi:10.3390/s19091977.

[56] V. Kanimozhi and T.P. Jacob, "Artificial Intelligence based Network Intrusion Detection with hyper-parameter

optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing", ICT Express (2019), https:// doi.org/10.1016/j.icte.2019.03.003.

[57] Bipraneel Roy, Dr. Hon Cheung, "A Deep Learning Approach For Intrusion Detection In Internet Of Things Using Bi-Directional Long Short-Term Memory Recurrent Neural Network", 2018 28th International Telecommunication Network Communication Conference (ITANC).

[58] Manoj Kumar Putchala, " Deep Learning Approach For Intrusion Detection System (IDS) in the Internet of Things (IOT) Network Using Gated Recurrent Neural Networks (GRU)", Thesis Submitted to Wright State University 2017.