IOT Routing Attack Detection Using Deep Neural Network

Hossam. T. Yassein
Institute of Graduate Studies and Research, Alexandria University, Egypt.
E-mail: hussamyaseen527@gmail.com

Saleh Mesbah*
Arab Academy for Science, Technology and Maritime Transport, Alexandria, Egypt.
E-mail: mmadbouly@alexu.edu.eg

Magda M. Madbouly
Institute of Graduate Studies and Research, Alexandria University, Egypt.
E-mail: saleh.mesbah@aast.edu

Received May 06, 2021; Accepted August 08, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18SI05/WEB18220

Abstract

The internet of things (IoT) devices becomes omnipresent as IOT resources become all-encompassing. Their success has not gone unnoticed and there are still growing numbers of attacks and assaults on IOT products and services. Cyber-attacks aren't new to IOT, but since IOT is profoundly embedded within our lives and cultures, cyber security becomes a must. There is also a real need to protect IOT, and therefore the risks and assaults on IoT networks must be grasped thoroughly. This thesis aims to categories threat categories as well as evaluates and describes intruders and assaults that IoT devices and services face. The objective of this thesis has been aimed a deep-learning-based machine learning addition to analyzing and characterizing intruders and attacks in IOT devices and services, this study is an attempt to identify category of threat. A deep learning machine method for the revelation of routing attacks for IoT was provided as the purpose of this thesis. The Cooja IoT simulator was utilized in our research for the development of high-reliance attack results. For detecting deep learning attacks for IoT path attacks, we provide a highly scalable solution. They have high precision and high precision Kiru and Mirai.ng technique for the revelation of routing attacks for IoT. Consequently, the Cooja IoT emulator was utilized for high resolution attack data generation. We propose a highly scalable, deep-learning-based attack revelation techniqueology for the revelation of IoT routing attacks which are Kiru, and Mirai with high accuracy and precision. The application of deep learning for cyber-security in IoT requires the availability of substantial IoT attack data and we believe that the IoT attack dataset produced in this work can be utilized for further research. The results analysis offers a deep Neural Network model to robustly classify routing attacks with a 99.9 percent accuracy assessment

scoring for Kiru and Mirai attacks, which forms a robust model for preventing most attacks from impacting subsequent layers in the sensors or actuators. The Cooja network simulator based on the Contiki OS is utilized to demonstrate in real-time simulation the functioning of this routing and compression protocol. The results show that the utilize of the Deep learning technique in IoT security is a promising solution to the challenges facing security.

Keywords

Deep Learning, Machine Learning, Internet of Things, Cyber-physical Systems, Cyber Security, Routing Attack.

Introduction

Considering their ad-hoc and resource-constrained nature, IoT systems are an ideal target for cyber-attacks. As a result, continual monitoring and analysis are required for IoT system security. Due to the massive quantity of network and sensory data created by IoT devices and systems, Big Data and machine learning (ML) approaches are extremely useful in continuous monitoring and analysis for IoT system security (Geluvaraj *et al*, 2019), (Apruzzese *et al*, 2018), (Xin *et al*, 2018). In several industries for instance the telecommunications, transportation, processing, water and poor control, healthcare, education, financial services, government and even entertainment, the Internet of Things (IoT) innovations have been commonly utilized. The innovations of the SDN (software-defined networking) and the CRN (Kakalou *et al*, 2017) the cloud computing and the mobile edge caching and fog computing (Abbas *et al*, 2018) have been further advanced in ICT. The that susceptibility to cyber assaults that are characterized as some sort of offensive activity by one or more computers to threaten the computer information system, network infrastructure or personal computer is following these innovations.

Despite artificial neural networks (ANNs) have been around for decades, G. Hinton et al. developed the notion of deep belief networks in 2006. Following that, this technology's state-of-the-art performance was seen in a variety of AI disciplines, including image recognition, image retrieval, search engines and information retrieval, and natural language processing. On top of conventional ANNs, DL methods have been created. Feed-forward Neural Networks (FNNs), also known as Multilayer Perceptron - MLPs, have been used to train systems for decades, however they become harder to train as the number of layers increases (Gamage *et al*, 2020).

Another issue that causes overfitted models is the small quantity of the training data. Furthermore, because to limitations in processing capability at the time, efficient deeper

FNNs could not be implemented. Hardware improvements in general, as well as the creation of Graphics Processing Units (GPUs) and hardware accelerators in particular, have helped to overcome these computational restrictions. Aside from the structural features and importance of depth in DL designs, as well as hardware developments, DL approaches have benefitted from advances in effective deep network training algorithms, including certain (Mohammadi *et al*, 2018):

- Rectified Linear Units (ReLUs) are used as an activation function.
- Introducing dropout prevention techniques.
- Weights of the network are randomly initialised.
- Addressing residual learning networks' deterioration of training accuracy.
- Introducing and improving Long Short-Term Memory networks to solve vanishing gradient and expanding gradient problems.

The purpose of this paper is to utilize Deep Learning to cyber security, and to develop and construct a system for attack detection in distributed architectures of IoT applications, such as smart cities. To demonstrate the usefulness of deep models over shallow models, the assessment procedure used performance measures such as accuracy, revelation rate, false alarm rate, and so on.

Distributed attack disclosure has been demonstrated to be more successful than centralized algorithms in identifying cyber-attacks due to the exchange of parameters that may avoid local minima in training. It has also been demonstrated that our deep model outperforms traditional machine learning methods, such as SoftMax for the internet. The remainder of this work is structured as follows: Work relating to Section 2. Section 3: Definition of the Issue Engineering and selection are featured in Section 4. Model architecture in Section 5. Section 6 will be noted as experimental, while section 7 will be highlighted as conclusion.

Related Work

In 2007, (Traian *et al*, 2007) utilizing Self Organizing Maps (SOM) algorithm to identify routing attacks. In 2010, (Rolf, 2010) concentrated on legal concerns and legislative strategies to decide whether IoT systems met the standards for privacy and protection. (Roman *et al*, 2013) addressed protection and privacy in the sense of distributed IoT. These authors have identified many problems that need to be tackled and the benefits of the centralized approach to IoT about protection and privacy concerns. Survey in 2013, (Rodrigo *et al*, 2013), analyzed the emerging flaws and risks in IoT applications,

including assaults on malware and protection problems. In same period (Shahid *et al*, 2013) study, node IDs and rankings for detecting abnormalities are tested to match assigned values. Upon discovery of a hostile node, an alert is triggered. However, rule-based identification is not ancient for dynamic networks and unexplained threats as it needs certain laws that render it challenging to control management. Therefore, because rules are built from pre-determined device settings and existing threats, new rules need to be introduced to manage different forms of attack. In 2015, (Jorge *et al*, 2015) underlined the reliability of IoT connectivity after analyzing IoT connectivity applications protection problems and solutions. In 2017, (Zarpelão *et al*, 2017) completed an IoT-systems intrusion prevention study. Well in the same period, (Ibrar *et al*, 2017) narrowly considered the ML data privacy and security safety approaches in the IoT context. Their research also identified several obstacles in potential directions for the application of ML in IoT systems (i.e. overhead processing and connectivity, data recovery approaches and partial state observation). Applications of data analysis and safety machine learning approaches to facilitate intrusion detection. The easiest approach to build and maintain the longevity of stable IoT networks is to defend yourself from disruptive threats before they occur. Identifying and detecting hostile threats, if necessary, rises to attention at this stage in order to defend the IoT networks from attacks. There are several alternate methods to predicting attacks; a rule-based approach (or signature-based) and a statistical (or behavioral) technique. Signature related approaches struggle to route attacks which have slightly altered their existence. The object tracking approaches are great at predicting precision in previously unexplored threats than signature-based solutions. There are so many reports that utilize the rule-based technique to routing protocol threat exposure for IoT. The Period from 2017-2018, many analysts performed IoT protection surveys to offer concrete advice on potential IoT device protection a vulnerability and a blueprint for possible works. Furthermore, several of the recent IoT protection studies did not rely directly on IoT protection applications for the ML/DL. Surveys (Sfar *et al*, 2017), (Djamel *et al*, 2018) for instance, examined extant literature and confidential for instance, examined extant literature and confidential problems in IoT frameworks in terms of confidentiality, authorization, access management, network protection and device protection.

In this section we show few examples for papers been published using deep learning for IOT Routing revelation. In year 2020, Deep Learning for Revelation of Routing Attacks in the Internet of Things (Charles *et al*, 2020) where most of data preprocessing techniques possessed, Also model detect the routing attacks using deep learning approach, with good accuracy on 3 Different datasets than ours (Decreased Rank Model, Hello

Flood Model, Version Number Model) with (94.9%, 99.5%, 95.2%) accuracy respectively. However our model could detect the 2 different attacks without being trained on, and keeping accuracies +97%.

Problem Definition

The scale of Internet-connected systems has increased considerably, and these systems are being exposed to cyber-attacks more than ever. In addition, attack detections in IoT are radically different from the existing mechanisms because of the special service requirements of IoT which cannot be satisfied by the centralized cloud:

- Low latency.
- Resource limitations.
- Distribution.
- Scalability and mobility.
- This means that neither cloud nor standalone attack detection solutions solve the security problems of IoT.

The complexity and dynamics of cyber-attacks require protecting mechanisms to be responsive, adaptive, and large-scale.

Machine Learning, or more specifically Deep Learning (DL), methods have been proposed widely to address these issues. By incorporating deep learning into IOT, DL-IOT is highly capable of solving complex, dynamic, and especially high-dimensional cyber defense problems.

Thus, It proposed that with a highly scalable deep learning-based attack recognition technique for realistic IoT scenarios**.**

To achieve a better accuracy with highly scalable secure attack, defend with processed data for 3 major attacks, Namely, Hide and Seek, Kiru and Mirai to solve the security routing attack problem of IoT.

Furthermore, there can be double-sided communication between devices, such communication is initially carried out on a network, which is connected on all networks, and each device is known to be a node in this topology (Furkan *et al*, 2018). One of these nodes could be hostile as the key threat. This ensures that all machines that serve as recipients of and senders in the form of communication will send dangerous signals to

other nodes from such a malicious node and form unsuitable acts as signals are sent to actuators.

A malicious node in the network, particularly when attached to the Root Node and begins to send malicious signals to the specific node in the network, is a problem called routing attack. (Sebastian *et al*, 2020). The relation of the node number 22 to the root node, which can influence the entire network, has been shown in Figure 1.

Although that a malicious node sends such dangerous node 22 signals with a specific pattern in network topology, these patterns are not detectable by original rule-based devices in real-time especially if signals are not easily encoded in the rules. Machine Learning (ML) algorithms are very common here. ML algorithm based on data recognition, where the case is to be found, is sadly a major challenge to achieve such data transfer and not to be shared publicly either.

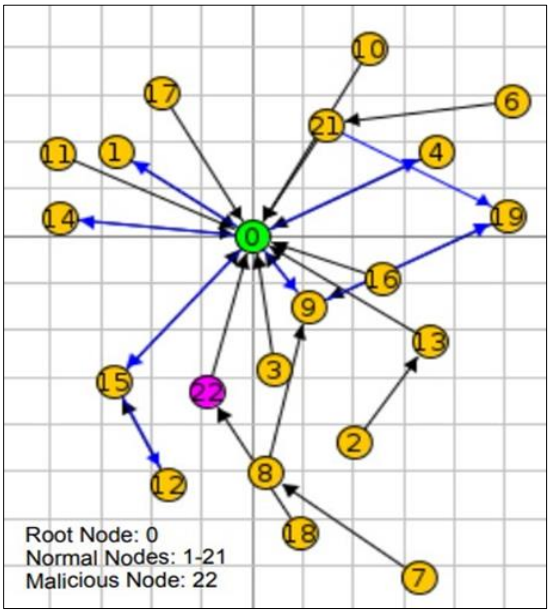

Figure 1 Malicious Node in network topology (Furkan et al, 2018)

Internet of Things

The Internet of Things (IoT) is a network of connected sensors, actuators, embedded, and wearable devices. This network is projected to include billions of devices, making homes, institutions, cities, and many other locations smarter (Evans, 2011). IoT network parts are projected to be low-cost, small-form-factor devices with minimal resources in order to reach populations in the billions.

Routing Attacks

Denial of Service (DoS) and Distributed DoS (DDoS) attack aimed at misusing resources and causing disruptions, delays, losses, and degradation of IoT services. DoS attacks obviously pose a danger to IoT availability and dependability. Attacks, for example, must be prevented, detected, or mitigated autonomously for a highly reliable and available Internet of Service (Bada *et al*, 2020).

- **RPL Attacks**

D/DoS attacks target the IoT Network Layer as illustrated in Figure 2. Such attacks a utilize the vulnerabilities of the RPL protocol design (Anhtuan *et al*, 2016), Rank is a very crucial parameter of the RPL protocol which represents a node's position within the Destination Oriented Directed Acyclic Graph (DODAG). This position is a relative distance of a node from the DODAG root. Malicious nodes may utilize rank in various ways to apply D/DoS attacks.

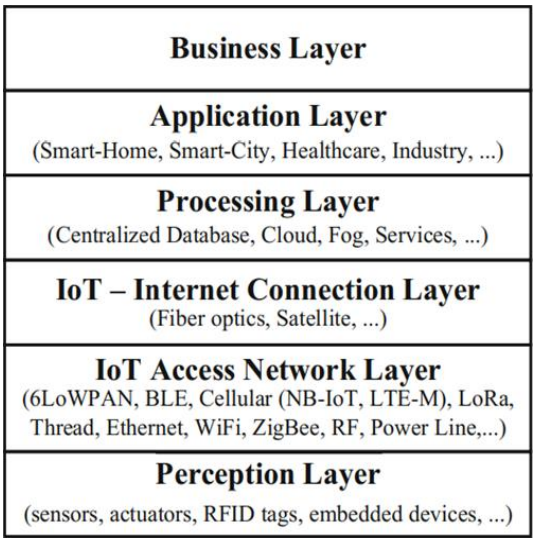

Figure 2 Generic IoT Architecture

Attacker node selects the neighbor with worst rank as a preferred parent instead of choosing the one with the best rank. Thus an inefficient DODAG is established which cautilizes delays and a number of control messages (Roman *et al*, 2013).

- **Attacks not specific to RPL**

A malicious node can apply the neighbor attack by re-transmitting the routing control messages it hears (Granjal *et al*, 2015). These behavior cautilizes neighbor nodes to think that the source of the control message is close to them and take actions accordingly.

Dataset Problem

As been discussed before, lackage of Network topology and signal transmission data, forms a big challenge for recognizeing malicious node pattern of transmission across the net- work with Machine learning and Deep learning algorithms. Proposed solution is to create a virtual topology where malicious node is being embedded, and start simulating the nodes signals and monitoring all data resulted from such simulation across the network and saving it, to be as training dataset for our model.

Dataset are saved in.pcap file formats, transformation done on data to be Comma-Separated-Values (CSV) tabular format Utilizing Wireshark, enabling dataset to be fed as input to the Deep Learning model. as illustrated in Figure 4.

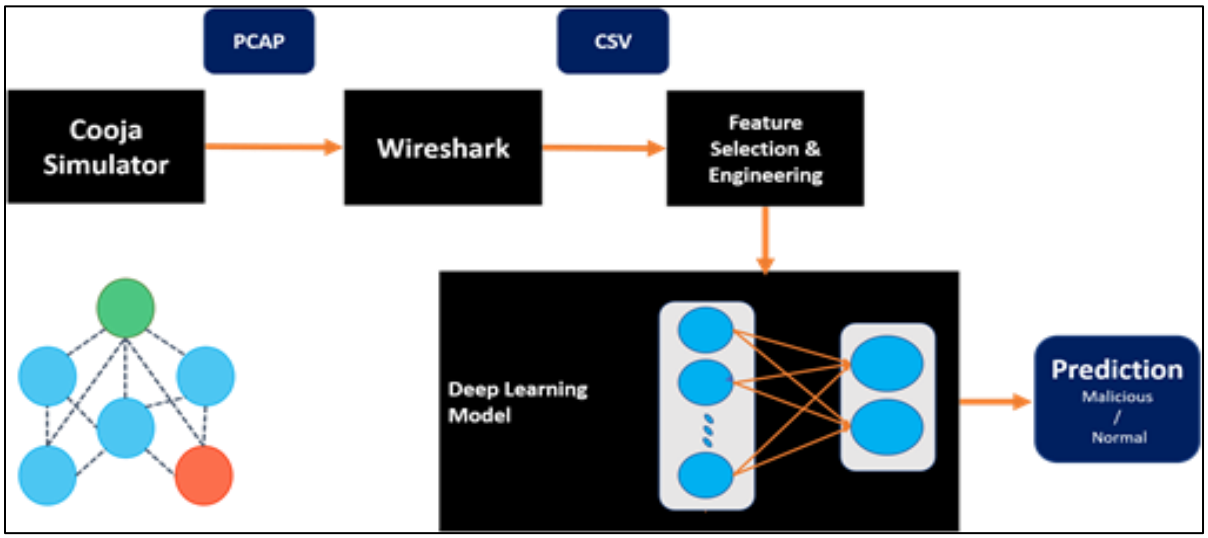

Figure 3 End-to-End Pipeline

Feature Engineering and Selection

Pre-processing techniques have been done with reference (Farid *et al*, 2008), (Udaya *et al*, 2015), (Buczak *et al*, 2016).

Encoding Process

- Create an encoding for source and destination ip ad- dresses.
- Create a protocol encoding. create info encoding.
- Calculate the transmission duration and utilize it to set the packet monitor duration's.
- Get all packets in each second and utilize it to get source/ destination packet counts.

- Calculate the transmission and receiving total durations.
- Utilize the all above to create ready features data file.
- Utilize the infected ip to label all the resulting data.

Normalization Process

Applying quantile transform and min-max scaling to the 3 datasets with feature names expressed in Table (1).

Table 1 Extracting Features as been done through topology (Furkan et al, 2018)

#	Feature Name	Feature Description
1	Protocol	Type of Protocol
2	Length	Packet Length
3	Info	Packet Information
4	TR	Transmission Rate
5	RR	Reception Rate
6	TAT	Transmission Average Time
7	RAT	Reception Average Time
8	TPC	Transmitted Packet Count
9	RPC	Received Packet Count
10	TTT	Total Transmission Time
11	TRT	Total Reception Time
12	SC	Source IP Count Per 1000 ms
13	DC	Destination IP Count Per 1000 ms
14	Label	Normal / Malicious Label

The tables 2,3,4 respectively represent a snapshot from features per data set after being extracted.

Table 2 Out of Hide and Seek attack

protocol	length	info	transmission_rate_(per_1000_ms)	reception_rate_(per_1000_ms)	tr_/_rr	Sources_count_per_sec	Destinations_count_per_sec	trans_total_duration_per_sec	rcv_total_duration_per_sec	trans_average_per_sec	rcv_average_per_sec	label	
0	0.600097	0.555347	0.611595	0.555783	0.490453	0.454571	0.516366	0.49021	0.455109	0.489188	0.55871	0.467416	1
1	0.478714	0.555347	0.459918	0.555783	0	0.454571	0.57967	0	0.455109	0.550817	0.55871	0.467416	1
2	0.495293	0.555347	0.470972	0.555783	0	0.454571	0.57967	0	0.455109	0.586793	0.55871	0.467416	1
….	…	…	…	…	…	…	…	…	…	…	…	…	…
196816	0.456442	0.314054	0.431271	0.261475	0	0	0.422018	0	0	0.447706	0	0.546919	0

Table 3 Out of Kiru attack

protocol	length rcv_average_per_sec	info	transmission_rate_(per_1000_ms)	reception_rate_(per_1000_ms)	tr_/_rr	Sources_count_per_sec	Destinations_count_per_sec	trans_total_duration_per_sec	rcv_total_duration_per_sec	trans_average_per_sec	rcv_average_per_sec	label	
0	0.498793	0.543 28	0.538237	0.406774	0.567 08	0.332 243	0.406774	0.567077	0.332243	0.555 5541	0.40 8116	0.5 267 63	0
1	0	0.5 50 62	0.390 132	0.459 503	0.4 84 25	0.504 828	0.459503	0.486 565	0.473613	0.51 6856	0.53 735 4	0.5 408 92	1
2	0.498793	0.5 50 62	0.4796 4	0.459 503	0.4 84 25	0.504 828	0.459503	0.486 565	0.473613	0.51 6856	0.53 735 4	0.5 408 92	1
…	…	…	…	…	…	…	…	…	…	…	…	…	…
75 58	0.498793	0.5 05 31	0.431233	0.584 534	0.4 39 54	0.572 894	0.584534	0.439538	0.603944	0.47 4889	0.49 891 4	0.5 364 45	1

Table 4 Out of Mira attack

protocol	length rcv_average_per_sec	info	transmission_rate_(per_1000_ms)	reception_rate_(per_1000_ms)	tr_/_rr	Sources_count_per_sec	Destinations_count_per_sec	trans_total_duration_per_sec	rcv_total_duration_per_sec	trans_average_per_sec	rcv_average_per_sec	label	
0	0	0.797 75	0.316 27	0.310 73	0.755 01	0.28 737	0.31073	0.7550 1	0.26838	0.30 444	0.2 844 1	0.3 01 43	1
1	0.496 14	0.311 56	0.417 02	0.312 38	0.767 91	0.28 737	0.31238	0.7679 1	0.34148	0.56 615	0.7 238 1	0.4 44 26	0
2	0	0.797 75	0.324 83	0.312 38	0.767 91	0.28 737	0.31238	0.7679 1	0.34148	0.56 615	0.7 238 1	0.4 44 26	0
…	…	…	…	…	…	…	…	…	…	…	…	…	
11 50 4	0.496 14	0.501 33	0.578 75	0.363 29	0	0.50 157	0.50109	0	0.40754	0.65 451	0.4 079 3	0.6 55 22	1

Now, that all the ready data for modeling step where we can define the deep learning model.

In the following steps, the entire implementation process can be outlined:

1. Network traffic record (utilizing Wire shark)
2. Feature extraction and selection (utilizing Python 3.7)
3. Application of the machine learning methods (utilizing Python 3.7)
4. Evaluation of the results.

Model Architecture

Attacks aiming at squandering resources and causing IoT service interruptions, delays, losses, and deterioration. DoS attacks are clearly a threat to the availability and dependability of IoT devices. For a highly dependable and available Internet of Service, attacks, for illustration, must be prevented, detected, or mitigated autonomously.

The data and predicted results are used to establish the weights of the internal layers of NN. And the best weights are found. Another word is the validation set, which aids in the learning process of fine-tuning function parameters to get optimal weights.

Eventually, the test set (Kiru & Mirai routing assaults data) is used to evaluate the training process' performance. The dataset is split into the training set and the testing set before the learning process begins, and the validation dataset is segregated from the training set. Epochs are used as learning time while creating the neural network algorithm. The training set is entirely transmitted through the network in one epoch.

The goal of Deep Neural Network (DNN) training methods is to find the 'optimal' collection of weight values for the issue at hand.

Deep Neural Network model with 5 hidden Layers, output single neuron applying sigmoid activation to map output within [0, 1] range, as expected, determining the optimal set of weights is often a trade-off between minimizing network error, computation time, and maintaining the network's ability to generalize.

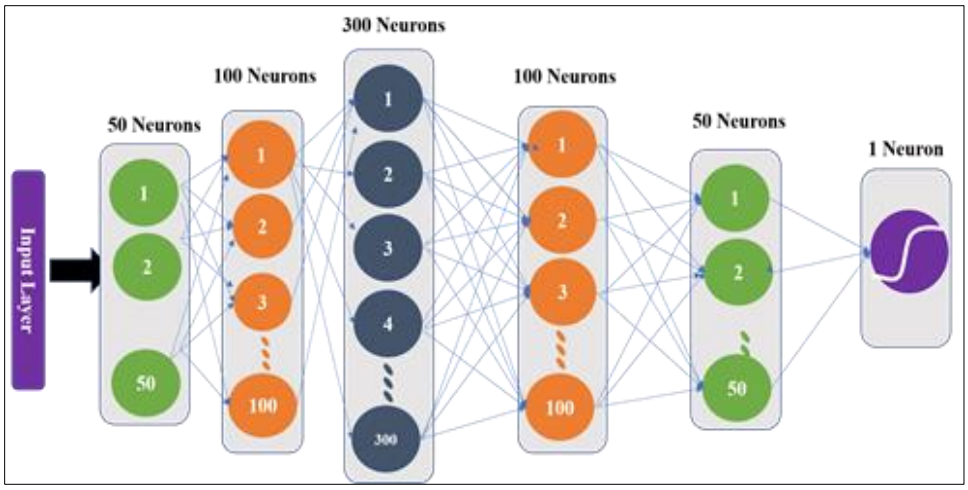

Figure 4 Deep Neural Network Architecture

After each layer we add such regularization techniques, to make model training becomes more stable across the Neural- Network and prevent it from overfitting.

Regularization Techniques added after to prevent model from overfitting.

- Batch Normalization (Sergey *et al*, 2015).
- Drop-out with 10% probability (Ibrar *et al*, 2017)

After each layer we add such regularization techniques, as **Batch-normalization** prevents each layer from producing a new distribution and model learning becomes more stable across the Neural-Network.

$$\mu\mathcal{B} = \frac{1}{m}\sum_{i=1}^{m} xi \qquad (1)$$

$$\sigma_{\mathcal{B}}^2 = \frac{1}{m}\sum_{i=1}^{m}(xi - \mu\mathcal{B})^2 \qquad (2)$$

$$\hat{x}_i = \frac{x_i - \mu\mathcal{B}}{\sqrt{\sigma_{\mathcal{B}}^2 + \epsilon}} \qquad (3)$$

$$y_i = \gamma_{\hat{x}}\hat{i}_i + \beta = BN_{\gamma,\beta}(x_i) \qquad (4)$$

Where *Y* and β are learnable parameters used to make the suitable shifting and scaling for each layers' distribution.

On the Other hand **Drop-out** Technique aims to provide more randomness within the neural network, where it force the Neural Network to robust such randomness and generalize to unseen data, as it coerce the model to capture maximum features as much as possible across each layer.

Experimental

In this section we provide analysis on the model through training on Routing attack datasets which contain a malicious node with Specific IP has been discussed through section1.

This dataset was as part of the Avast AIC laboratory with the funding of Avast Software (Zarpelão *et al*, 2017). It is labeled dataset with malicious and benign IoT network traffic. The dataset consist of 3 different (PCAP) files that contain the monitoring packets about different routing attacks. Also, as a middle step, we have converted the (PCAP) files into (CSV) files using wire shark as illustrated in Figure 4.

Three different datasets for each attack.

- Hide & Seek attack
- Kiru attack
- Mirai attack

Training done on **Hide & seek** Dataset, while testing done on Both Kiru & Mirai.

Where Hide & seek validation set reached 99.9% accuracy with 10 Epochs training.

Table 5 Training & Evaluation metrics

-	Kiru	Mirai
Accuracy	98.9%	98.28%
Precision	99.9%	97.38%
Recall	98.9%	99.8%

Conclusion

This paper proved that its additionally rendered and even prepossessed the data sets. Indeed, the main task was to build and analyze the datasets of the assailant. Our provided this attempt in this study. Our also built a deeper neural network and trained them to build three attack recognition models utilizing generated routing attack data sets. Its additionally rendered and even preprocessed the data sets. Indeed, the main task was to build and analyze the datasets of the assailment. Our provided this attempt in this study. Our also built a deeper neural network and trained them to build three attack recognition models utilizing generated routing attack data sets. The platform efficiency is equivalent to approximately 99%.

This paper it proved that Deep Neural Network is successfully able to classifies the malicious signals across different and unseen attacks for instance Kiru and Mirai: (1) Adaptive sub-gradient optimizer (Adaptive Gradient Algorithm (Adagrad)); (2) Batch Normalization; and Drop-out with 10 % probability.

References

Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. *IEEE Internet of Things Journal*, *5*(1), 450-465.

Le, A., Loo, J., Chai, K.K., & Aiash, M. (2016). A specification-based IDS for detecting attacks on RPL-based network topology. *Information*, *7*(2), 25. https://doi.org/10.3390/info7020025

Buczak, A.L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, *18*(2), 1153-1176.

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. *In IEEE International Conference on Cyber Conflict (CyCon)*, 371-390.

Bada, M., & Nurse, J.R. (2020). The social and psychological impact of cyberattacks. *In Emerging cyber threats and cognitive vulnerabilities*, Academic Press, 73-92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

Zarpelão, B.B., Miani, R.S., Kawakani, C.T., & De Alvarenga, S.C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25-37.

Wheelus, C., & Zhu, X. (2020). Iot network security: Threats, risks, and a data-driven defense framework. *IoT*, *1*(2), 259-285. https://doi.org/10.3390/iot1020016

Kouicem, D.E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Nait-Abdesselam, F., Bensaou, B., & Taleb, T. (2008). Detecting and avoiding wormhole attacks in wireless ad hoc networks. *IEEE Communications Magazine*, *46*(4), 127-133.

Yavuz, F.Y., Ünal, D., & Gül, E. (2018). Deep learning for detection of routing attacks in the internet of things. *International Journal of Computational Intelligence Systems*, *12*(1), 39-58.

Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, *169*, 102767.

Geluvaraj, B., Satwik, P.M., & Kumar, T.A. (2019) The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. *In*

*International Conference on Computer Networks and Communication Technologie*s. Springer. Singapore, 739-747.

Yaqoob, I., Ahmed, E., UR Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444-458. https://doi.org/10.1016/j.comnet.2017.09.003.

Granjal, J., Monteiro, E., & Silva, J.S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312.

Kakalou, I., Psannis, K.E., Krawiec, P., & Badea, R. (2017) Cognitive radio network and network service chaining toward 5G: Challenges and requirements. *IEEE Communications Magazine*, *55*(11), 145-151.

Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, *20*(4), 2923-2960.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Sebastian, G., Agustin, P., & Maria, J.E. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746.

Sergey, I., & Christian, S. (2015). Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. *In Proceedings of the 32nd International Conference on International Conference on Machine Learning*, (ICML'15), 448–456.

Sfar, A.R., Natalizio E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118–137.

Shahid, R., Linus, W., & Thiemo, V. (2013). SVELTE: Real- time intrusion detection in the internet of things. *Ad Hoc Networks*, *11*(8), 2661–2674.

Traian, A., Seungchan, O., & Salim, H. (2007). Analyzing Attacks in Wireless Ad Hoc Network with Self-Organizing Maps. *Fifth Annual Conference on Communication Networks and Services Research (CNSR '07)*, 14-17, 166-175. http://doi.org/10.1109/CNSR.2007.15.

Dhamodharan, U.S.R.K., & Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, *2015*. https://doi.org/10.1155/2015/841267.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018) Machine learning and deep learning methods for Cybersecurity. *IEEE Access*, 6, 35365-35381.

Mohammadi, M., Saeedi, R., Mansouri, M., Banisaffar, M., Mahimani, A., Shahri, M.A., & Yadgari, M. (2019). Evaluation of effective indicators on promotion of webometric rank of golestan university of medical sciences website. *Webology*, *16*(2), 242-256.