ANALYSIS ON DDOS ATTACKS IN IOT NETWORK

T Ramya, Research Scholar, Anurag Universtiy, Hyderabad India : 2904ramya@gmail.com

Abstract.
IoT plays a vital role and will change our living styles, standards, as well as business models. The IoT permits billions of gadgets, people groups, and administrations to associate with others.There is a drastic increase in the past decade in the use of these Iot devices. Due to lack of resource constraints like low computational power, less storage capacity, limited battery power, and dispersed network architecture these devices are highly vulnerable to different types of cyber attack.There is very limited possibility to implement any kind of IDPS or Firewalls in these networks.Distributed Denail of Service attack aims to attack a node in a IoT network ,so that the entire network is collapsed. This paper like to focus on the challenges that are faced by an IoT network in terms of DDoS attack This paper gives a detailed description of the types of DDoS attacks in IoT Network.

Keywords. *DDoS attacks, IoT network, Vulnerabilities*

Literature Survey

Wanderson L Costa [1] carried out experiments based on two datasets BoT-IoT2 and UNSW-IoT which are formatted in real world monitoring data. The fog computer was executed in local machine and cloud computer using Azure virtual machine. The results of the experiments highlight the importance of the features selection for the accuracy, execution time and volume of data. For example, using the most appropriate selection technique, the performance of the KNN and SVM classifiers increases by 8% and 7%, respectively. Additionally, the LR technique using the 80 extracted features (no selection) has an unacceptable accuracy, while using the Extra-Tree technique, it achieves more than 93% of accuracy. Regarding the training time, its importance increases in contexts that a recurrent training is necessary to update the ML model to the high dynamics of the SE, such as smart campi and smart cities. Thus, the ML model will be trained in a very short time period to keep the detection of DDoS attacks effectively. The same reasoning can be applied to thedetection time.

The performance of the proposed intelligent system (including the combination of selection and ML techniques), considering the cases of True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) for a DDoS detection, was based on the following evaluation metrics: -Accuracy (in percentage): Rate of correct classification, regardless the class, according to the Equation 1. It isimportant to note that the Accuracy was measured for the Traffic Segmentation and the DDoS detection.Recall (in percentage): Efficiency of the classifier to detect the correct class, i.e., the rate of TP in relation to total positive cases (TP+FN).Training Time (in seconds): time required to train the DDoS detector (ML model) with the selected input features.Detection Time (in seconds): time spent by the DDoS detector to define whether a case is a DDoS attack or not.Volume of Data (in Megabits): the size of the data generated (processed data) to be exchanged between Fog and Cloud. The results of the experiments highlight the importance of the features selection for the accuracy, execution time and volume of data. For example, using the most appropriate selection technique, the performance of the KNN and SVM classifiers increases by 8% and 7%, respectively. Additionally, the LR technique using the 80 extracted features (no selection) has an unacceptable accuracy, while using the Extra-Tree technique, it achieves more than 93% of accuracy. Regarding the training time, its importance increases in contexts that a recurrent training is necessary to update the ML model to the high dynamics of the SE, such as smart campi and smart cities. Thus, the ML model will be trained in a very short time period to keep the detection of DDoSattacks effectively. The same reasoning can be applied to the detection time.

Inference

Nowadays, new paradigms have emerged, such as Smart Environments (heterogeneous IoT and Personal devices). A critical challenge in smart environments lies in the detection of network DDoS attacks, resulting from security vulnerabilities. Their early detection helps to avoid the QoS degradation and possible financial losses.

This article described an Intelligent System for detecting DDoS in ESs. The proposed system is based on ML techniques to perform the traffic segmentation and DDoS detection, while a features selection approach is applied to reduce the amount of data exchanged between Fog and Cloud and to improve the accuracy of the detection. Results from performance evaluation based on real traffic as workload indicate a 99% of accuracy (in average) to detect DDoS attacks, while the training time was 10 seconds (in average). As future work, authors intend to investigate new security solutions for other threats to SEs, such as SideChannel, OS Service Scan, Keylogging andData Exfiltration.

Sehrish Batool[2] Multimodular Statistical Approach towards DDoS Detection (MMSA) consists of multiple phases that work together to detect and mitigate specifically TCP SYN flood attacks. Weighted moving average and standard deviation have been used for detection along with entropy. Standard deviation and moving average have been used to determine the level one threshold. If the packet_ count is greater than zn , an alarm will be triggered, and the algorithm will move towards the second phase of detection. For entropy calculation, we have used the destination IP of the sending device, and it will be calculated in a fixed window size of 50. ,e threshold value for entropy is 1. ,e algorithm for the proposed method is given in Algorithm 1. Basic TCP parameters like packet counter per second, source, and destination IP to measure the entropy and threshold values have been used to ensure speed and minimum computation time.

MMSA has been implemented on a VMware with 8 GB RAM, Ubuntu 16.04 LTS OS. Mininet [48] emulator has been used for SDN simulation, and POX controller has coupled to a network containing two switches. Forty-three hosts are connected to the switches. Netdata is a real-time traffic monitoring tool that is installedon a computer with 4 GB RAM and core i3.

MMSA method was tested and analyzed several times. Results illustrate that the algorithm can accomplish efficiently in different attack scenarios against TCP SYN flood attacks. ,e suggested method provides lightweight code for DDoS attack detection and mitigation scheme in SDN architecture. ,Three phases ensure theminimal false positive rate and high accuracy, and it does not block the whole network traffic. It is aimed to tryto extend our method to other attacks for future work, for example, ICMP and spoofing attack

Inference

This paper has proposed a lightweight statistical approach towards TCP SYN flood DDoS attack detection andmitigation in the SDN environment. The objective of this technique was to design and propose a lightweight and practical method for the diagnosis and diminution of TCP SYN flood attacks in the SDN. ,is technique hasthree modular approaches to notice and mitigate DDoS attacks. ,e method used multiple phases to accurately detect the attack. ,e limitation of the statistical approach is its dependency on selected parameters.

MA Lawal[3] In this paper In order to evaluate the k-NN classifier of our proposed framework. A total of 241173 instances wereextracted randomly from the CICDDoS 2019 dataset. Authors selected 23 features using the feature selection by employing the ranker search method and information gain, which removes redundant and irrelevant features. These features selected represent the best features that will give good performance in terms of classification. The k-NN classifier is evaluated against Decision

Tree (DT) and Naïve Bayes (NB) classifiers using the 10-fold cross- validation. The evaluations are in terms of accuracy, false-positive rate, precision, recall and F1 Score of binary classification (normal and attack). In addition, the effect of distance measurement techniques namely Euclidean, Manhattan, and Chebychev distance measurement techniques are investigated on the CICDDoS 2019 dataset in terms of accuracy.

The k-NN achieved the best results in terms of accuracy with 99.99% while DT and NB recorded 99.88% and 95.55 %, respectively. The k-NN recorded 100% in terms of precision, recall and F1 score. The DT recorded 99% in terms of precision, recall and F1 score. While the NB recorded 96.10%, 95.60% and 95.70% in terms of precision, recall and F1 score, respectively. In addition, figure 5 shows the false positives rate of the classifiers with k-NN recording zero. The results show that the k-NN classifier has achieved superior results than DT and NB classifiers, which will translate to good performance in detecting DDoS attacks.

The Euclidean and Manhattan distance measurement techniques recorded similar accuracy results with 99.99% while the Chebychev distance measurement techniques obtained a lower accuracy with 79.75%. Although, these distance measurement techniques belong to the same family, which is the power distance [28]. The Euclidean and Manhattan distance measurement techniques are suitable for distance calculation between two distances in any vector dimension provided the data is numerical. While the Chebychev distance measurement technique is suitable for the distance between two points if they are different in one dimension.

Inference

The combination of 5G and fog computing facilitates the efficient deployment of security solutions for IoT networks. The 5G enables connecting many devices and provides communication with high speed and low latencies while the fog provides the resources (storage and computation) essential for security solutions suchas anomaly mitigation. In this paper, a DDoS attack mitigation framework using fog computing is proposed to ensure fast and accurate detection. The framework employs an anomaly-based mitigation method that utilizesa k-NN classification algorithm alongside a database. The database stores signatures of previously detected attacks, which will offer a faster detection when the attack is executed again. Authors evaluated the proposed k-NN classifier for the framework using the CICDDoS 2019 dataset. The results demonstrate that the k-NN classifier will be able to detect DDoS attacks with high accuracy. In the future, authors intend to implement the framework on available fog computing platforms to further evaluate our approach.

In this paper[4] The heterogeneous nature of an IoT network makes parametric anomaly detection approaches for DDoS detection less effective since they assume probabilistic models for nominal and anomalous conditions. In practice, it is difficult to know/estimate the anomalous and even the nominal probability distributions. Hence, parametric anomaly-based IDSs, as well as many conventional signature-based IDSs are not feasible in addressing stealthy DDoS attacks through IoT. Recently, an online and non-parametric detector called the Online Discrepancy Test (ODIT) was proposed for detecting persistent and abrupt anomalies [32]. Thanks to its nonparametric operation, ODIT does not need to know baseline or anomalous distributions beforehand, hence can address the challenge (C3) stated in Section I-A. ODIT is a sequential method which accumulates evidence in time, and makes a decision at each time based on the accumulated evidence so far, instead of making a hard decision based on a single data point. This sequential nature of ODIT is tailored for timely detection, thus it is able to address the challenge (C4). Moreover, ODIT can handle monitoring large numberof devices together, which addresses the challenge (C2).

Results show that the proposed ODIT-based IDS significantly outperforms the deep autoencoder-based

IDS proposed in the N-BaIoT paper ,and by extension Isolation Forest ,SVM and LOF , which are shown to be outperformed by the autoencoder method.proposed model with an IDS based on cooperative CUSUM [35], which knows the exact parameters of the nominal model and the anomalous model. CUSUM knows exactly the mean and standard deviation of the Gaussian distribution, as well as the probability of being active for each device. Note that due to rounding to the nearest nonnegative integer value, the real probability distribution of number of packets deviates from the generative bimodal Gaussian. Hence, the proposed ODIT detector even sometimes outperforms CUSUM, which exactly knows the generative Gaussian model. The results for Average Detection Delay vs False Positive Rate are shown in Fig. 14. Authors see that the cooperative ODIT-based IDS, proposed in Section IV-B, performs better than the clairvoyant CUSUM detector, which exactly knows the generative probabilistic model, for false alarm rates less than 0.1. It significantly outperforms the information metric method proposed in [20], which monitors the aggregate traffic at each node. In Fig. 14, it is seen that the cooperation among nodes facilitates earlier detection by our algorithm (ODIT vs. Cooperative ODIT).

[5] In this paper the authors performed experiments in a controlled laboratory environment using recent literature datasets. The proposed system was executed in a Raspberry PI 3 model B environment using the QEMU [18] platform, an emulator that simulates various types of CPUs such as x86, PowerPC, ARM, and Sparc. In this work, the datasets CIC-DoS [19], CICIDS2017 [20] and customized [16] were used since they include modern threats and DoS techniques. System performance was evaluated using the Precision (PR), and F-Measure (F1) metrics present in the literature. PR measures the ability to avoid false positive. F1 is a harmonic average between PR and Recall (Re), which measures system sensitivity.

The experimental setup consists of a network traffic processor, a virtual switch containing a packet sampler, and the Smart Detection-IoT system. TcpReplay [22] software was used to process PCAP files whosetraffic was forwarded to the Open vSwitch (OVS) [23], where packets were sampled at a rate of 20% using a built-in sFlow agent OVS. These samples were received and analyzed by the Smart DetectionIoT system, configured with Tmax

= 50. Several previous tests were performed to choose the most balanced parameters to be used. In scenarios where the sample rate is too low, and the Tmax is too large, for example, traffic samples are discarded before processing by the classifier. On the other hand, if Tmax is too small, the F AR increases because the classifier has little data to analyze.

the Smart Detection-IoT system, a solution that uses machine learning to classify IoT network traffic and detect denial of service attacks by only analyzing the IP/TCP header of network traffic samples, thus not compromising data privacy. The intention is to detect the attack as close as possible to the threat, allowing actions to be taken as quickly as possible to mitigate them. The Smart Detection-IoT system performance was assessed under three classification algorithms, and competitive results were observed when the proposed system is compared to other approaches from the recent literature. The system was tested with three datasets: CIC-DOS, CICIDS2017, and a customized containing several DoS/DDoS attacks, such as UDP flood, TCP flood, HTTP flood, and HTTP slow. Based on the experimental results, the Smart Detection-IoT approach delivers enhanced P REC, F A_R and D_r. For instance, in the CIC-DoS and customized datasets, the proposed system acquired DR and PREC higher than 96%with F A_R less than 6%.

CONCLUSION

These days, new standards have arisen, like Smart Environment (heterogeneous IoT and personal devices). A basic test in shrewd conditions lies in the recognition of organization DDoS attacks, coming about because of safety weaknesses. Their initial identification assists with keeping away from the QoS

degradation and conceivable monetary misfortunes

REFERENCES

(Use the Microsoft Word template style: *Heading 1*) or (Use Times New Roman Font: 12 pt, Bold, ALL CAPS, Centered)

References should be numbered using Arabic numerals followed by a period (.) as shown below and should follow the formatin the below examples.

1. [1] Features-Aware DDoS Detection in Heterogeneous Smart Environments based on Fog and Cloud Computing WL Costa,ALC Portela… - International Journal of …, 2021 - search.proquest.com
2. [2] Lightweight Statistical Approach towards TCP SYN Flood DDoS Attack Detection and Mitigation in SDN Environment Sehrish Batool, Farrukh Zeeshan Khan , Syed Qaiser Ali Shah,Muneer Ahmed, Roobaea Alroobaea , Abdullah
M. Baqasah,4 Ihsan Ali.
3. [3] A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing MA Lawal, RA Shaikh, SR Hassan .
4. [4] Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks Keval Doshi ,Yasin Yilmaz and Suleyman Uludag
5. [5] Smart Detection-IoT: A DDoS Sensor System for Internet of Things Federico A. F. Silveira,[1] Agostinho de Medeiros BritoJunior,[1] Genoveva Vargas-Solar,[2] and Luiz F. Silver
6. [6] AL-Hawawreh M, Moustafa N, Sitnikova E.(2018) "Identification of malicious activities in industrial internet of things based on deep learning models." Journal of Information Security Applications 41: 1–11.
7. [7] Zarpelão BB, Miani RS, Kawakani CT, Cláudio Toshio, De Sean Carlisto.(2017) "A survey of intrusion detection in Internet of Things." Journal of Network and Computer Applications 84: 25–37.
8. [8] Rauf A, Shaikh RA, Shah A. "Security and privacy for IoT and fog computing paradigm.(2018)" In: 15th Learning and Technology Conference (L&T).IEEE. Jeddah, Saudi Arabia : 96–101.
9. [9] Yaseen Q, Albalas F, Jararwah Y, Al-Ayyoub M.(2018) "Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks." Transactions on Emerging Telecommunication Technology 2018 29(4): 1–13.
10. [10] Kasinathan P, Pastrone C, Spirito MA, Vinkovits M.(2013) "Denial-of-Service detection in 6LoWPAN based Internet of Things." In: International Conference on Wireless and Mobile Computing, Networking and Communications. IEEE: 600–607.
11. [11] Da Silva Cardoso AM, Lopes RF, Teles AS, Magalhaes Fernando B V .(2018) "Real-time DDoS detection based on complex event processing for IoT." In: Proceedings - ACM/IEEE International Conference on Internet of Things Design and Implementation, IoTDI : 273–274.
12. [12] Vipindev Adat, Gupta BB.(2017) "A DDoS attack mitigation framework for internet of things."International Conferenceon Communication and Signal Processing:2036–2041.
13. [13] Lee T-H, Wen C-H, Chang L-H, Chiang H S, Ming C H.(2014) "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN." In: Advanced Technologies, Embedded and Multimedia for Human-centric Computing :1257–1268.
14. [14] Gai F, Zhang J, Zhu P, Xinwen Jiang B.(2017) "Multidimensional Trust-Based Anomaly Detection System in Internet of Things." In: Wireless Algorithms, Systems, and Applications. WASA 2017. Lecture Notes in Computer Science. Springer, Cham :302–313.
15. [15] Sonar K, Upadhyay H.(2016) "An Approach to Secure Internet of Things Against DDoS." In: International Conference on ICT for Sustainable Development. Advances in Intelligent Systems and Computing. Singapore: Springer.
16. [16] Sedjelmaci H, Senouci SM, Al-Bahri M.(2016) "A lightweight anomaly detection technique for lowresource IoT devices: A game-theoretic methodology." In: 2016 IEEE International Conference on Communications, ICC 2016. IEEE :1–6.
17. [17] Fix, E. and Hodges JL.(1951) "Discriminatory analysis. Nonparametric discrimination; consistency properties". TechnicalReport 4, USAF School of Aviation Medicine Randolph Field, TX, USA.
18. [18] Prasath VBS, Haneen Arafat Abu Alfeilat ABAH, Lasassmeh O, Lasassmeh O, Ahmad S. Tarawneh,

Mahmoud B Alhasanat, Hamzeh S. Eyal Salman.(2017) "Distance and Similarity Measures Effect on the Performance of K-Nearest Neighbor Classifier -- A Review." arXiv preprints 1708.04321:1–39.
19. [19] Nguyen HV and Choi Y.(2009)"Proactive detection of DDoS attacks utilizing k-NN classifier in an antiDDos framework." International Journal of Computer, Electrical Automation, Control and InformationEngineering 39(3): 640–645.
20. [20] Li W, Yi P, Wu Y, Pan L, Li J.(2014)"A new intrusion detection system based on KNN classification algorithm in wirelesssensor network." Journal of Electrical and Computer Engineering.

Where to Find Further Information

We warmly invite you to visit our online platform, Scitation, where you can find further help/advice and publishingpolicies for AIP Conference Proceedings:

- For authors: https://aip.scitation.org/apc/authors/preppapers
- For conference organizers: https://aip.scitation.org/apc/organizers/abstracts

Summary: Points to Consider when Preparing Your Paper

1- Articles should use 8.5 x 11 single column template.
2- Use Times New Roman font, the point size will vary by section.
3- DO NOT alter the margins of our templates. They are carefully designed for AIP's production process: Altering them can cause significant delays. Paper size should be 8 ½ x 11 with margins set at:Top – 1 inch, Left – 1 inch, Bottom – 1.18 inch, Right – 1 inch.
4- DO NOT display the title in ALL CAPS (initial cap only)
5- DO NOT include any headers, footers, or page numbers in your document. They will be added to your article PDF by AIP Publishing, *so please do not amend this template to add them to your paper.*
6- Line spacing should be 1.0 throughout the entire article, no double spacing.
7- Make sure all author affiliation associations are correct. This means author vs. affiliation and author vs. email address. If there is only one affiliation for all authors, association is not needed. Author names should be listed in First name Surname format.
8- Use clear, legible graphics and diagrams. Readers of your paper will be grateful. If they cannot read it, they are unlikely to cite it.
9- DO NOT use copyrighted material without permission. Papers using copyrighted material without appropriate permission and acknowledgment will be excluded from the proceedings.
10- No 1-page papers please. 1-page, abstract-only contributions are not acceptable and will be excluded fromthe proceedings.
11- Prepare and format references with care. References should be numbered using Arabic numerals followed bya period (.).
12- Embed all fonts into your article PDF. The importance of font embedding is discussed in the section Font Embedding (above). PDFs supplied without embedded fonts are often completely unusable for printing or publication purposes. In such cases, we must return those PDFs to the proceedings editors for font embedding. Failure to embed fonts can cause unnecessary inconvenience to your proceedings editor(s) and publication delays for other authors. Failure to provide a replacement paper in a timely fashion may result in an article being removed from the proceedings.
13- Check your article PDF file! It is not uncommon for errors to appear in PDFs generated from Microsoft Word
– corrupted math, figures reflowing, etc. It is essential to very carefully check your article PDF file before sending it to the proceedings editor(s).
14- Avoid large PDF files (10 MB maximum, ideally). For the benefit of your readers, we recommend keeping your article PDF file below 10 MB. This is a recommendation, not a requirement.

