ISSN: 2249-7196
IJMRR/July 2023/ Volume 13/Issue 3/01-7
Mrs. CH. Harshini/ International Journal of Management Research & Review

A MACHINE LEARNING BASED CLASSIFICATION AND PREDICTION TECHNIQUE FOR DDOS ATTACKS

Mrs. CH. Harshini[1], Dokuri Devika Parameswari[2], E. Harshitha[3], Farah Tazeen[4], Gorla Maneesha[5]

[1]Assistant professor, [2345]UG Scholar

Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, India

Chikkaharshini@gmail.com[1], devikaddp@gmail.com[2], eppalapallyharshitha@gmail.com[3], farahtazeen03@gmail.com[4], gorlamaneesha@gmail.com[5].

ABSTRAT

The recent proliferation of Internet of Things (IoT) is paving the way for the emergence of smart cities, where billions of IoT devices are interconnected to provide novel pervasive services and automate our daily life tasks (e.g., smart healthcare, smart home). However, as the number of insecure IoT devices continues to grow at a rapid rate, the impact of Distributed Denial-of- Service (DDoS) attacks is growing rapidly. With the advent of IoT botnets such as Mirai, the view towards IoT has changed from enabler of smart cities into a powerful amplifying tool for cyberattacks. This motivates the development of new techniques to provide flexibility and efficiency of decision making on the attack collaboration in a software defined networks (SDN) context. The new emerging technologies, such as SDN and blockchain, give rise to new opportunities for secure, low-cost, flexible and efficient DDoS attacks collaboration for the IoT environment. In this paper, we propose Co-IoT, a blockchain-based framework for collaborative DDoS attack mitigation; it uses smart contracts (i.e., Ethereum's smart contracts) in order to facilitate the attack collaboration among SDN- based domains and transfer attack information's in a secure, efficient and decentralized manner. Co- IoT's implementation is deployed on the Ethereum official test network Ropsten [1]. The experimental results confirm that Co-IoT achieves flexibility, efficiency, security, cost effectiveness making it a promising scheme to mitigate DDoS attacks in large scale

INTRODUCTION

In the fast-progressing environment of automated and connected devices, the whole world can be considered as a large network of devices connected and communicating with each other. The Internet of

Things (IoT) refers to this ubiquitous computing environment where sensors and actuators will be associated with living and non-living 'things' and all these will be part of the Internet; not just the computers and smartphones. However, as the network gets bigger, the challenges are also escalating. The security issues related to IoT have large impacts on the future of this domain posting questions over the security of devices being used. Meanwhile, distributed denial of service (DDoS) attacks was already been significant in the area of cyber security. When the things got connected over the Internet the DDoS attacks have increased magnificently since they have more devices to compromise and create the attacks. The resource constrained devices being deployed in the IoT scenario has even made it easier for an attacker to crack. It ranges from high-end computing systems to the basic microprocessors with low memory and computational capacity. In this variant environment, the security solutions are also to be proposed at various levels. The capabilities of devices at different levels of IoT varies, hence, implementing security mechanisms at the different level will have different dimensions and properties. In this work, we are proposing a defensive framework against distributed denial of service (DDoS) attacks and denial of service (DoS) attacks in general. We have targeted to the flooding attacks for now. The remaining sections are arranged as follows. Section II will give a glimpse of the recent statistics and the motivation towards addressing this problem. Then we will look into the related works specific to defending DDoS and DoS attacks in IoT scenario.

LITERATURE SURVEY

On networking of Internet of Things: Explorations and challenges

AUTHOR:

H. Ma, L. Liu, A. Zhou, and D. ZhaoAABSTRACT:

Internet of Things (IoT), as the trend of future networks, begins to be used in many aspects of daily life. It is of great significance to recognize the networking problem behind developing IoT. In this paper, we first analyze and point out the key problem of IoT from the perspective of networking: how to interconnect large-scale heterogeneous network elements and exchange data efficiently. Combining our on-going works, we present some research progresses on three main aspects: 1) the basic model of IoT architecture; 2) the internetworking model; and 3) the sensor-networking mode. Finally, we discuss two remaining challenges in this area

TITLE:

Risks of automation: A cautionary total-systemper- spective of our cyberfuture, AUTHORS :

P. G. NeumannABSTRACT:

M A N Y C O MP UT ER -R E L ATE D R I S K

S discussed in past Inside Risks columns are still present today. These risks (and new ones) are likely to intensify even further as sys- tems provide extensive automated or semi-automated operation. Signifi- cantly greater total-system trustworthi- ness will be required, encompassing better hardware, system software, and

applications that are able to tolerate human limitations and environmental factors. Risks will continue to result from inadequate reliability, security, and privacy, as well as gullibility and general inability of users to cope with complex technology. We repeatedly discover unexpected risks resulting from lashing subsystems together (for example, see Beurdouche 2), because of unexpected system behavior. Many advances in research, system develop- ment, and user friendliness are urgent- lyneeded

EXISTING SYSTEM

Blockchain technology (e.g., Bitcoin [10] and Ethereum [11]) is considered as a new technology to secure and store information in a decentralized manner without any trusted tier; it has proven its success and effectiveness in multiple application domains (e.g., Healthcare [12], financial field [13]) to achieve high level of security and transparency. One such application domain is the IoT [14] due to its decentralized structure and the resource-constraints of its devices. Using blockchain technology, which ensures trust between nodes in a trustless environment, can be an efficient approach to facilitate the future underlying infrastructure for IoT. Security and privacy for IoT have been an active research topic for decades and several DDoS collaboration mitigation schemes have beenproposed. In the following, we present the most prominent schemes as well as their security issues

PROPOSED SYSTEM

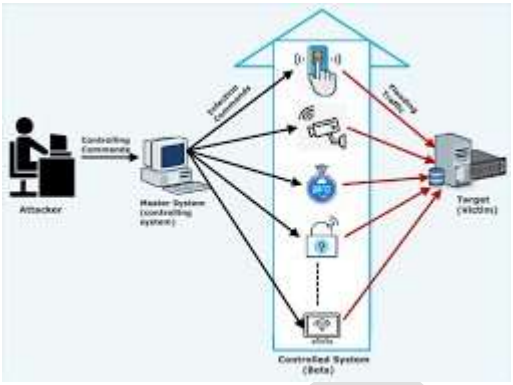
We implemented Co-IoT using both private (Ganache simulator [28]) and public blockchain (Ethereum official test network Ropsten). Once the collaboration contract is deployed, it can be self-executed without any human intervention. The process of deployment is elaborated using truffle framework [29] (see Fig. 4). First, we have coded the contract using the high-level language programming solidity [30]. Then, we compiled the contract into Ethereum Virtual Machine (EVM) byte code; once the collaboration contract gets compiled, it generates EVM byte code as well as Application Binary Interface (ABI). Afterwards, we deployed the collaboration contract to the blockchain. Initially, we have deployed the collaboration contract using Ganache, a private blockchain simulator to test Ethereum's smart contract in a fast way. Then, we have deployed the smart contract on Ethereum official test network Ropsten. Fig. 5 shows the smart contract lifecycle. Once deployed, the smart contract can be invoked using its address and the ABI definition. If needed, the contract can be deleted

PROPOSED SYSTEM ADVANTAGES:

1. High Accuracy

2. High Efficiency

SYSTEM ARCHITECTURE:

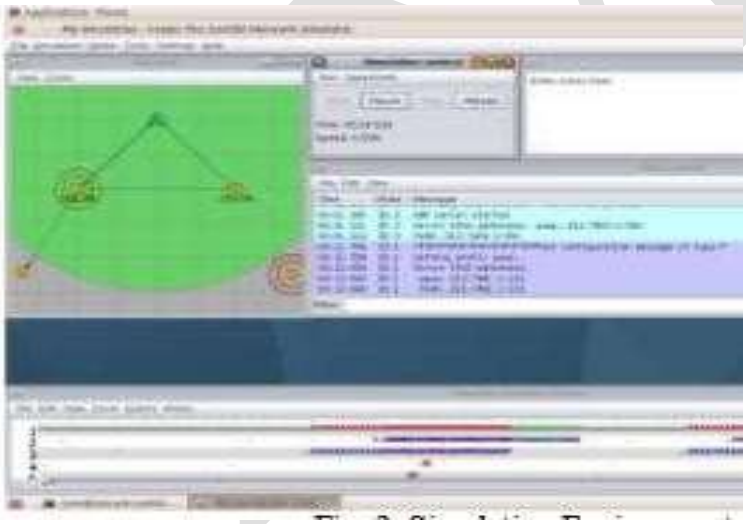


IMPLEMENTATION

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations suchas

Login, Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results in Line Chart, View Prediction Of DDOS Attack Type, Find View Prediction DDOS Attack Type Ratio, Download Predicted Datasets, View DDOS Attack Type Ratio Results, View All Remote Users.



View and Authorize Users

In this module, the admin can view the list ofusers who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

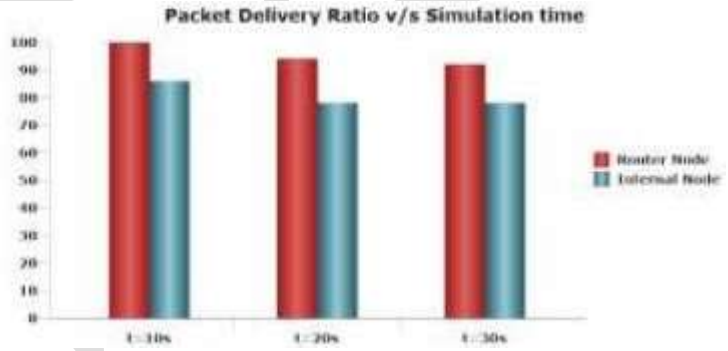
In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using

authorized user name and password. Once Login is successful user will do some operations like PREDICT DDOS ATTACK TYPE, VIEWYOUR PROFILE.

WORKING METHODOLOGY

The proposed framework is simulated in Cooja and fig. 3 shows the simulation environment. Sky motes are used for border router and RPL is used for DODAG formation. UDP clients and servers are connected inside the internal network to represent different internal devices. Testing of the framework against flooding DDoS attacks has been performed. Packet Delivery Ratio, Response Time, True Positives and False Negatives are considered as the testing parameters based on comparison with the existing approaches. It helps us to compare the results with the existing approaches as similar information about those approaches is published.

In specific cases, we have got 100% delivery rate for border router and 86% for the internal node. However, we expect some more reduction in the delivery ratio if we go for real- time hardware implementation, which is planned as a future work. Fig. 4 and 5 shows results of our proposed solution in terms of efficiency in successful communication. We obtained a better packet delivery ratio to the internal nodes and failed communications are comparatively lesser inour work. Further, the complexity of our proposed algorithm is lesser compared to the existing approaches that we have mentioned in the related works. It helps to achieve the improvements in the communication parameters.



CONCLUSION

In this paper, we proposed a complete systematic approach for detection of the DDOS attack. First, we selected the UNSW-nb15 dataset from the GitHub repository that contains information about the DDOS attacks. This dataset was provided by the Australian Centre for Cyber Security(ACCS) [29], [30]. Then, Python and jupyter notebook were used to work on data wrangling. Secondly, we divided the dataset into two classes i.e. the dependent class and the independent class. Moreover, we normalized the dataset for the algorithm. After data normalization, we applied the proposed, supervised, machine learning approach. The model generated prediction and classification outcomes from the supervised algorithm. Then, we used Random Forest and XG Boost classification algorithms. In the first classification, we observed that both the Random Forest Precision (PR) and Recall (RE) are approximately 89% accurate. Furthermore, we noted approximately 89% average Accuracy (AC) for the proposed model that is enough good and extremely awesome. Note that the average Accuracy illustrates the F1 score as 89%. For the second classification, we noted that both the XG Boost Precision (PR) and Recall (RE) are approximately 90% accurate. We noted approximately 90% average Accuracy (AC) of the suggested model that is wonderful and extremely brilliant. Again, the average Accuracy illustrates the F1 score as 90%. By comparing the proposal to existing research works, the defect determination accuracy of the existing research
[4] which was 85% and 79% were also significantly improved.

Looking to the future, for functional applications, it is important to provide a more user-friendly, faster alternative to deep learning calculations, and produce better results with a shorter burning time. It is important to work on unsupervised learning toward supervised learning for unlabeled and labeled datasets. Moreover, we will investigate how non-supervised learning algorithms will affect the DDOS attacks detection,in particular, we non-labeled datasets are takeninto account.

REFERENCES

[1] N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, ``Adversarial machine blearning applied to intrusion and malware scenarios: A systematic review," *IEEE Access*, vol. 8, pp. 35403_35419, 2020.

[2] G. Karatas, O. Demir, and O. K. Sahingoz,
``Increasing the performance of machine learning- based IDSs on an imbalanced and up-to-date dataset," *IEEE Access*, vol. 8, pp. 32150_32162, 2020.

[3] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li,
``BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, vol. 8, pp. 29575_29585, 2020.

[4] H. Jiang, Z. He, G. Ye, and H. Zhang,
``Network intrusion detection based on PSO- xgboost model," *IEEE Access*, vol. 8, pp. 58392_58401, 2020.

[5] A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty, and V. S. Kiran,
``Similarity based feature transformation for network anomaly detection," *IEEE Access*, vol. 8, pp. 39184_39196, 2020.

[6] L. D'hooge, T. Wauters, B. Volckaert, and F. De Turck, ``Classi_cation hardness for supervised

learners on 20 years of intrusion detection data," *IEEE Access*, vol. 7, pp. 167455_167469, 2019.

[7] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, ``An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, pp. 82512_82521, 2019.

[8] Y. Yang, K. Zheng, B. Wu, Y. Yang, and X. Wang, ``Network intrusion detection based on supervised adversarial variational auto-encoder with regularization," *IEEE Access*, vol. 8, pp. 42169_42184, 2020.

[9] C. Liu, Y. Liu, Y. Yan, and J. Wang, ``An intrusion detection model with hierarchical attention mechanism," *IEEE Access*, vol. 8, pp. 67542_67554, 2020.

[10] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, ``Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450_42471, 2019.