Snort for Intrusion Detection in Internet of Things Network: A Study Using Machine Learning Approach

Lekhika Chettri, Chanda Pradhan, Ankur Konwar and Sabina Sherpa
Department of Computer Applications, Sikkim University, Sikkim, India

Abstract

The extending vogue of network attacks impacts the availability, confidentiality, and integrity of critical information in all types of network. Some typical network like Internet of things (IoT) can can have fatal consequences as a result of network attacks. With the growth in the usage of Internet of Things devices in the existing network, their vulnerability to a vast range of cyber attacks becomes a prime concern. The, Intrusion Detection Systems (IDS) have been used since long as a defense to identify the attacks and secure the network from intrusions. However, the existing IDS may be less effective in handling the rising attacks and threats in IoT network and machine learning based IDS can provide a more efficient solution. Snort has been used since more than 2 decades for detecting network attacks in various applications. Thus, in this work we study machine learning algorithms to explore their suitability for use in snort in attack detection for IoT traffic. ***We also propose a model that integrates the snort with machine learning algorithms for attack detection in IoT network traffic.***

Keywords: Snort, Machine Learning, Intrusion Detection System, IoT Traffic, Security, Attacks.

1. INTRODUCTION

The use of IoT devices has been rapidly increasing over the past few years, like mobile phones, wrist health bands, internet-connected ACs, microwave oven, etc. While IoT devices bring effective communication between devices, still concerning factor is its security. IDS can be used in IoT to protect the network from malicious traffic [2][3]. However, even with decades of development, existing Intrusion Detection Systems are not able to overcome the obstacles in improving the false alarm rate, detection accuracy, and detecting unknown attacks. To solve the problems, many researchers have focused on developing IDSs that capitalize on machine learning methods. The essential differences between normal data and abnormal data can be automatically discovered with high accuracy by machine learning methods. So, adopting the traditional intrusion detection system would not be a good idea. It would be prominent if a smart solution is adapted where intrusion detection systems are integrated with a machine learning-based solution.

Furthermore, IoT has various issues associated with it like, data heterogeneity, resource constraint devices, close proximity to human body and their day to day human life. Considering the fact, IoT devices are small, integrated and resource constraint a host based IDS may not be feasible to use. Instead a network based IDS may help provide a solution. Thus, we choose snort as it is a Network based Intrusion Detection System (NIDS).

2. RELATED WORK

In this section, we briefly discuss a few work that are related to handling attacks in network traffic using machine learning approach using intrusion detection system. The survey highlighted a key concern that a very limited work has been done in exploring or handling security issues of IoT network using particularly IoT traffic. Also, in Table 1, a summary of related work has been tabulated based on algorithms used, network type, and IDS type etc.

The findings of Timčenko et.al [6] shows that it focuses on the problem of providing security measures and anomaly detection which has considered several different categories of machine learning classification algorithms with a goal to estimate the proper choice for network anomaly detection in IoT. The comparison of frequently used machine learning classifiers from the group of Support Vector Machine (SVM) and a range of ensemble algorithms are discussed where the analysis is based on a range of testing procedures in Weka and [6] proved the strong classification capabilities of ensemble algorithm and on the other side support vector machine algorithm has shown to lack the fast enough performance. Amudha et.al [7] presented a summary of intrusion detection and KDDCup’99 dataset while analyzing the classification techniques used in intrusion detection. It is discussed that most of the classification techniques commonly used for classifying intrusion detection datasets directly apply standard methods to the publicly available intrusion detection datasets which do not perform well and has stated that the classification accuracy of the existing algorithms or techniques has to be improved as it is very difficult to detect new attacks, moreover classifier is a challenge to build an efficient intrusion detection system. Chakrabarti et.al [10] categorizes two tools namely, Snort and EagleX and describes that though latter has built-in intrusion detection system but still Snort is better equipped to handle attacks which also adds the power of preventing attacks by looking at the application-layer information within the packet. According to [10] the outcome of the progress with Snort shows that it is in fact a useful tool, especially when considering the speed with which rules can be released to protect against newly discovered attacks. Lin and Chih-Jen [14] Attempted to explicate the implementation of a pre-processor plug-in for anomaly detection approach using the machine learning technique and integrating it into the Snort. It further demonstrated that the plug-in can be efficient pre-processor plug-in for Snort that successfully detects anomalies before the intrusion detection system.

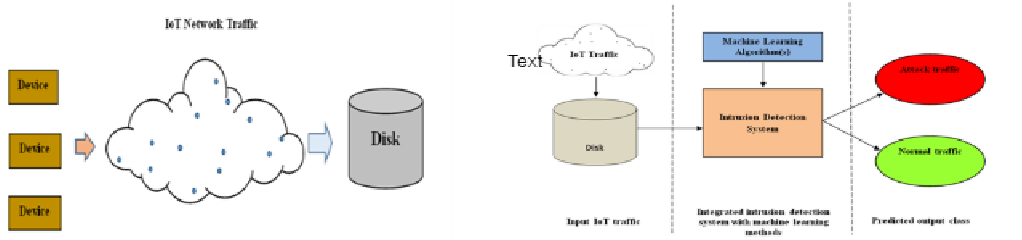
Sl. No	**Title of Paper, Author(s), Year**	**Algorithm used**	**IDS type**	**Network**	**Nature of IDS**	**IoT Traffic**
1.	Machine Learning based Network Anomaly Detection for IoT environments, Valentina Timčenko, SlavkoGajin,2018[6]	SVM	NIDS	IoT	Anomaly	Yes
2.	Classification Techniques for Intrusion Detection An Overview, P.Amudha, S.Karthik, S.Sivakumari, 2013 [7]	Naive Bayes, Decision Tree, SVM	NIDS	Computer Network	Anomaly	No
3.	Survey on Intrusion Detection System using Machine Learning Techniques, Sharmila Kishor Wagh, Vinod K. Pachghare, Satish R. Kolhe, 2013[8]	Fuzzy logic	NIDS	Computer Network	Anomaly	No
4.	A Machine Learning Approach to Anomaly Detection, Philip K. Chan, Matthew V. Mahoney, Muhammad H. Arshad, 2003[9]	LARAD,CLAD	HIDS	Computer Network	Anomaly	No
5.	Study of Snort-Based IDS, S Chakrabarti, M Chakraborty, I Mukhopadhyay, 2010[10]	-	NIDS, HIDS	Wireless Network	Signature	No
6.	Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey, Hongyu Liu, Bo Lang, 2019[11]	KNN, Naïve Bayes,SVM, Decision Trees, ANN, Logistic Regression, K-means	NIDS	Computer Network	Anomaly, Misuse	No
7.	Intrusion detection with the K nearest neighbour algorithm, William Giffen, 2017[12]	KNN	NIDS	Wireless Network	Misuse	No

8.	adsvm: pre-processor plug-in using support vector machine algorithm for Snort, Annie George, Prabaharan Poornachandran, M.RamachandraKaimal, 2012[14]	SVM	NIDS	Computer Network	Anomaly	No
9.	Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System, Syed Ali, Raza Shah, BijuIssac, 2018[16]	SVM, Fuzzy Logic	NIDS	Computer Network	Anomaly	No
10.	Intrusion Detection System using Support Vector Machine, JayshreeJha, LeenaRagha, 2013[18]	SVM,KNN	NIDS	Computer Network	Anomaly	No
11.	Pattern Matching Algorithms For Intrusion Detection Systems,Stanimir Bogomilov Belchev, 2012[19]	Single-Keyword Pattern Matching Algorithm and Multiple-Keyword Pattern Matching Algorithm:	NIDS	Wireless Network	Signature	No
12.	Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems, Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, Wei-Hsuan Tai, 2012[20]	-	NIDS	Computer Network	Signature	No
13.	Intrusion Detection: Support Vector Machines and Neural Networks, SrinivasMukkamala, Guadalupe Janoski, Andrew Sung, 2002[21]	Neural Network and Support Vector Machines	NIDS	Computer Network	Signature	No
14.	A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms, L.Dhanabal1, Dr. S.P. Shantharajah, 2015[22]	Support Vector Machine and Naïve Bayes Algorithms	NIDS	Wireless Network	Anomaly	No
15.	Analysis of Machine Learning in Intrusion Detection Systems. The Machine Learning Approach to	Support Vector Machine	NIDS	Wireless Network	Anomaly	No

	Detecting Cyber Intrusions, Brian Asta [23]					

3. PROPOSED MODEL

In this section we have proposed a potential model that can be used by Snort IDS to detect intrusion in IoT network suing machine learning models. The proposed model is broadly divided into three parts that includes: 1) input IoT traffic, 2) snort IDS integrated with machine learning models, and 3) predictions of output class. The Figure 1 highlights the block diagram of the proposed model.



(a) Storing IoT Traffic

(b) Proposed IDS model for IoT attack Detection

Figure 1: Proposed Model for Implementing Machine Learning Models in Snort IDS

Figure 1(a) shows collection of IoT traffic from various IoT devices. The traffic is then stored before it is passed through the proposed model. The dataset received from the input traffic is then inspected by the integrated intrusion detection system as shown in Figure 1(b).

4. EXPERIMENTAL ESSESMENT

In this experimental set-up an intrusion detection system software i.e., Snort is explored for implementing machine learning techniques to outcome the proposed model. At first Snort is installed in Ubuntu operating system. Snort performs protocol analysis, content searching and matching. It performs real-time traffic analysis and packet logging on IP networks.

Secondly, we have considered Support Vector Machine (SVM) [13] algorithm using the libsvm library for classification. The (SVM) pre-processor plug-in is installed and implemented with pre-installed Snort. The task of plug-in is to detect unknown malicious traffic by importing the machine learning algorithm. The pre-processor sends decoded packets to the plug-in while operating parallel with Snort's detection engine to classify the benign and malicious traffic by using the algorithm. A dataset split of 80% and 20% was used for training and testing purpose.

4.1 Machine Learning Model used

Support Vector Machine (SVM) is considered as the one of the efficient supervised classification models. It has been widely used in anomaly detection problems [1]. SVM can solve linear and non-linear problems and work well for many practical problems. The algorithm creates a line or a hyper plane that separates data into classes. SVM uses a portion of the data to train system, finding several support vectors that represent the training data. The basic input and output data format is as follows

(xi ,yi), …… ,(xn, yn), x € Rm , y € {+1 , -1}1

Where (xi , yi), …… ,(xn, yn) is the set, *m* is the input vector, *y* belongs to the classes of the input data as +1 or -1 as binary classification is the basic. The hyperplane can be represented as

(w.x) + b = 02

The hyperplane equation can be written

(w.x) + b ≥ + 1 for yi = +13

(w.x) + b ≤ - 1 for yi = -14

for the two class labels +1 or -1 such that to find the weight, w and the b values

4.2 Results and discussion

The proposed model was experimented for KDD-Cup99 dataset as it is a well known benchmark data set in the research of Intrusion Detection techniques [4][5]. An accuracy of 79% was recorded with SVM plug-in in snort. The execution of the model is carried out in the following steps:

Step 1: For experiment purpose, the dataset was stored in disk (storage device). Some specific featured and class label for machine learning algorithm were only considered for experimentation. The packet header fields like timestamp, checksum and derived features which include binary values such as source ip and destination ip were selected.

Step 2: The snort IDS is integrated with pre-processor plug-in module SVM, to detect anomalies. The extracted dataset from Step 1 is sent to integrated IDS for determining whether it is a benign or attack traffic. The steps or the execution is further highlighted in detail in Figure 2.

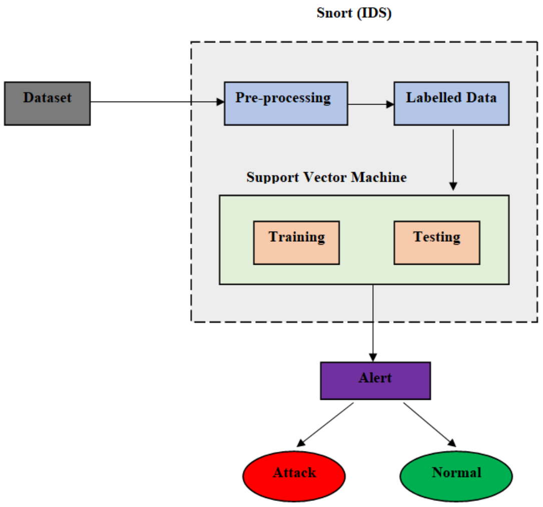


Figure 2: Execution of proposed model on the given network traffic

CONCLUSION

IoT is touching every aspect of life, it has become necessary to address the security issues of the network traffic that are entering into the IoT devices. In case of IoT using the traditional IDS would not be sufficient considering a huge dimension of heterogeneity in IoT traffic. Thus, we integrate machine learning techniques into the existing IDS system i.e., Snort, to enhance the performance of the IDS in detecting intrusions for an IoT network. Among the variety of machine learning techniques, the Support Vector Machine (SVM) is amongst a good machine learning algorithms to classify abnormal behavior thus we choose SVMM for experimentation. Snort uses the in-built algorithm for detection while we have implemented a pre-processor plug-in, the supervised machine learning algorithm SVM in Snort. The accuracy achieved shows a potential usage of snort in IoT traffic but as the accuracy is not so promising it may not be directly used for attack detection in an IoT network.

REFERENCES

[1] Gauthama Raman, M.R., Somu, N., Jagarapu, S. et al. An efficient intrusion detection technique based on support vector machine and improved binary gravitational search algorithm. Artif Intell Rev 53, 3255–3286 (2020)

[2] Meera A.J., Kantipudi M.V.V.P., Aluvalu R. (2021) Intrusion Detection System for the IoT: A Comprehensive Review. In: Abraham A., Jabbar M., Tiwari S., Jesus I. (eds) Proceedings of the 11th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2019). SoCPaR 2019. Advances in Intelligent Systems and Computing, vol 1182. Springer, Cham. https://doi.org/10.1007/978-3-030-49345-5_25

[3] Elrawy, M., Awad, A. & Hamed, H. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comp 7, 21 (2018)

[4] Aggarwal, Preeti, and Sudhir Kumar Sharma. "Analysis of KDD dataset attributes-class wise for intrusion detection." Procedia Computer Science 57 (2015): 842-851.

[5] Kumar S., Sunanda, Arora S. (2020) A Statistical Analysis on KDD Cup'99 Dataset for the Network Intrusion Detection System. In: M. Thampi S. et al. (eds) Applied Soft Computing and Communication Networks. ACN 2019.

[6] Timčenko, Valentina, and SlavkoGajin. "Machine learning based network anomaly detection for IoT environments." (2018): 196-201.

[7] Amudha, P., S. Karthik, and S. Sivakumari. "Classification techniques for intrusion detection-an overview." *International Journal of Computer Applications* 76, no. 16 (2013).

[8] Wagh, SharmilaKishor, Vinod K. Pachghare, and Satish R. Kolhe. "Survey on intrusion detection system using machine learning techniques." *International Journal of Computer Applications* 78, no. 16 (2013).

[9] Chan, Philip K., Matthew V. Mahoney, and Muhammad H. Arshad. *A machine learning approach to anomaly detection*. 2003.

[10] Chakrabarti, S., MohuyaChakraborty, and IndraneelMukhopadhyay. "Study of snort-based IDS." In *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*, pp. 43-47. 2010.

[11] Liu, Hongyu, and Bo Lang. "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey." *Applied Sciences* 9, no. 20 (2019): 4396.

[12] Sæbø, William Giffen. "Intrusion detection with the K nearest neighbour algorithm." Master's thesis, 2017.

[13] Lin, Chih-Jen. "Formulations of support vector machines: a note from an optimization point of view." *Neural Computation* 13, no. 2 (2001): 307-317.

[14] George, Annie, Prabaharan Poornachandran, and M. RamachandraKaimal. "adsvm: Pre-processor plug-in using support vector machine algorithm for Snort." In *Proceedings of the First International Conference on Security of Internet of Things*, pp. 179-184. 2012.

[15] Gupta, S., Kumar, P. and Abraham, A., 2013. A profile based network intrusion detection and prevention system for securing cloud environment. *International Journal of Distributed Sensor Networks*, *9*(3), p.364575.

[16] Shah, Syed Ali Raza, and BijuIssac. "Performance comparison of intrusion detection systems and application of machine learning to Snort system." *Future Generation Computer Systems* 80 (2018): 157-170.

[17] Alhomoud, Adeeb, Rashid Munir, Jules Pagna Disso, IrfanAwan, and Abdullah Al-Dhelaan. "Performance evaluation study of intrusion detection systems." *Procedia Computer Science* 5 (2011): 173-180.

[18] Jha, Jayshree, and LeenaRagha. "Intrusion detection system using support vector machine." *International Journal of Applied Information Systems (IJ AIS)* 3 (2013): 25-30.

[19] Belchev, StanimirBogomilov. "Pattern matching algorithms for intrusion detection systems." PhD diss., California State University, Northridge, 2012.

[20] Ho, Cheng-Yuan, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai. "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems." *IEEE Communications Magazine* 50, no. 3 (2012): 146-154.

[21] Mukkamala, Srinivas, Guadalupe Janoski, and Andrew Sung. "Intrusion detection using neural networks and support vector machines." In *Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290)*, vol. 2, pp. 1702-1707. IEEE, 2002.

[22] Dhanabal, L., and S. P. Shantharajah. "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms." *International Journal of Advanced Research in Computer and Communication Engineering* 4, no. 6 (2015): 446-452.

[23] Asta, Brian. "Analysis of Machine Learning in Intrusion Detection Systems."