RESEARCH REVIEW JOURNALS
Volume-04
Issue-01
January -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Assessment of Comparison between SOM and Distributed Detection Approach

[1]Anup Ingle, [2]Dr. Avinash Gour and [3]Dr. Ketki Kshirsagar

[1]Research Scholar, Dept. of Electronics and Communication Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India
[2]Research Guide, Dept. of Electronics and Communication Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India
[3]Research Co-Guide, Dept. of Electronics and Telecommunication, VIIT, Pune, Maharashtra, India

ARTICLE DETAILS

Article History
Published Online: 20 January 2019

Keywords
SOM, DDoS

ABSTRACT

The study of systems able to identify networking borne intrusions offers obstacles that are numerous. Because of the significance of the intrusion detection issue, there were different initiatives which try to quantify the present state of the art. A method of network intrusion detection is actually examined, based strictly on a hierarchy of Self Organizing Feature Maps. The principle interest of ours is establishing precisely how much such an approach may be had in training. The basic objective of this work is to assess just how far a detection approach based on comparison between SOM and distributed scheme may be taken.

1. Introduction

As a component of the attack cycle, malicious nodes generate an enormous arrangement of trick packets, for move towards a bunch of chosen target nodes for example nodes at basic locations of the network. These attacker nodes may belong to the existing network, basically, implying bargained yet authentic sensor nodes. In addition, the nodes may likewise be injected into the network by the adversary class, for reasons for participating in the attack traffic generation measure. Upon effective attack completion, these injected nodes can supplant the genuine nodes of the network, and generate false (misleading) sensory data for move and conveyance to the base station. An attack dispatched from a single passage point of the network is discernible by a single finder hub. On the contrary, a distributed denial of service attack requires a coordinated exertion by a bunch of finder nodes, present at different locations of the wireless sensor network, to accurately recognize such attacks. Our attack detection scheme proposed in this section performs detection of such attacks, when they are dispatched by both injected sensor nodes just as laptop-class nodes.

The attack identifier nodes wantonly monitor traffic packets generated and/or transiting through their individual nearby areas. These nodes are additionally customized to coordinate and trade traffic observation messages with neighboring (peer) GN nodes, for pattern reconstruction and traffic observation verification purposes.

2. Review of related literature

Hosny, Khalid and Rushdy, Ehab (2020) Software defined networks (SDN) are an as of late created structure for controlling network the executives by giving concentrated control unit called the Controller. This expert Controller is an incredible force point and yet it is sadly a disappointment point and a genuine proviso in the event that it is focused on and dropped by attacks. One of the most genuine kinds of attacks is the powerlessness to get to the Controller, which is known as the distributed denial of service (DDoS) attack. This examination shows how DDoS attack can drain the assets of the Controller and proposes a light weight instrument, which works at the Controller and identifies a DDoS attack in the beginning phases. The proposed component can recognize the attack, yet in addition distinguish attack ways and start a mitigation cycle to give some level of assurance to network gadgets following the attack is identified. The proposed instrument relies upon a mixture procedure that converges between the normal flow inception rate, and the flow particular of the coming traffic to the network.

Shurman et al., (2020) in the latest years, Denial-of-Dervice (DoS) or perhaps Distributed Denial-of-Service (DDoS) attack has distributed significantly and attackers make online systems unavailable to genuine owners by sending substantial selection of packets to the target phone. With this paper, we proposed 2 methodologies to identify Distributed Reflection Denial of Service (DrDoS) attacks in IoT. The very first strategy utilizes hybrid Intrusion Detection System (IDS) to detect IoT DoS episode. The next strategy utilizes heavy learning versions, based on Long Short Term Memory (LSTM) trained with newest dataset for this kind of sorts of DrDoS. The experimental results of ours demonstrate this using the proposed methodologies is able to identify undesirable behaviour making the IoT network secure of Ddos and Dos attacks.

Sharafaldin et al., (2019) Distributed Denial of Service (DDoS) attack is actually a menace to network security which is designed at exhausting the target networks with malicious site traffic. Even though a number of statistical techniques have been created for DDoS attack detection, developing a real time detector with lower computational overhead is nevertheless one of the primary issues. On the other hand, the evaluation of different detection algorithms and methods heavily depends on the presence of well designed datasets. With this paper, for starters, we review the present datasets adequately & suggest an innovative taxonomy for DDoS attacks. Second, we produce a brand new dataset, specifically CICDDoS2019, which remedies all present shortcomings. Thirdly, making use of the produced dataset, we suggest a brand new detection as well as family classification approach based on a set of network flow characteristics. Last but not least, we supply the most

crucial feature sets to identify various kinds of DDoS attacks because of their corresponding weights.

Francisco Sales de Lima Filho, Frederico A. F. Silveira, et. al (2019) Users and Internet service providers (ISPs) are constantly influenced by denial-of-service (DoS) attacks. This digital danger continues to become even with the improvement of new protection advances. Developing instruments to identify this danger is a current test in network security. This article presents a machine learning-(ML-) based DoS detection system. The proposed approach makes inferences based on marks recently removed from tests of network traffic. The trials were performed using four present day benchmark datasets. The outcomes show an online detection rate (DR) of attacks above 96%, with high precision (PREC) and low false alarm rate (FAR) using a sampling rate (SR) of 20% of network traffic.

Toklu, Sinan & Şimşek, Mehmet (2018) Distributed denial of service (DDoS) attacks is one of the main attacks because of lessening the presentation of PC networks these days. As of late, the quantity of gadgets connected to the web has been expanding. These gadgets are PCs as well as objects of regular use. The concept of web has accelerated the expansion considerably. Subsequently, numerous issues emerge regarding DDoS attacks. One of them is low-rate DDoS attacks. While high-rate DDoS attacks are often performed with PCs, low-rate DDoS attacks can be effortlessly performed by PCs and web connected items. Thusly, viable guard component against the two attacks must be created. In this examination, new approaches are proposed to filter blended high-rate DDoS and low-rate DDoS attacks. The ns-2 simulation apparatus was utilized to assess the presentation of the proposed methods. Trial results show that the proposed methods are effectively filtered blended DDoS attacks.

Igbe, Obinna and Ajayi, Oluwaseyi and Saadawi, Tarek (2017) as one of the most common and forceful methods, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks cause genuine effect on computing systems and networks. This paper presents a system for detecting DoS attacks in a network using the dendritic cell algorithm (DCA). The proposed system classifies incoming network traffic into both of two classes: "ordinary" or "DoS attack." This paper investigates some common DoS/DDoS attacks that target communication networks, and how these attacks can be distinguished using the Dendritic Cell Algorithm (DCA) which is an Artificial Immune System (AIS) based algorithm. The viability of our proposed detection system is assessed using the mainstream NSL-KDD dataset. Our outcomes show that our system is exceptionally powerful in detecting DoS/DDoS attacks with high precision.

Yao, Haipeng & Liu, Yiqing & Fang, Chao (2016) Abnormality network detection is a significant method to investigate and recognize malignant conduct in network. An instruction to viably distinguish inconsistency network flow under the weight of huge data is a significant region, which has pulled in an ever increasing number of analysts' attention. In this paper, we propose another model based on enormous data examination, which can stay away from the influence brought by adjustment of network traffic distribution, increase detection exactness and lessen the false negative rate. Simulation results uncover that, contrasted and k-implies, decision tree and random forest algorithms, the proposed model has a vastly improved presentation, which can accomplish a detection rate of 95.4% on ordinary data, 98.6% on DoS attack, 93.9% on Probe attack, 56.1% on U2R attack, and 77.2% on R2L attack.

Yan, Gao (2016) Network traffic is the measure of data moving over a network at a particular time, and peculiarity traffic detection is vital in PC networks. In this paper, we integrate the entropy hypothesis and support vector machine to recognize Network irregularity traffic. We use the entropy hypothesis to build up the network traffic highlight vector using the entropy hypothesis, and then endeavor the support vector machine to identify the network peculiarity traffic by tackling a classification issue. Especially, six kinds of network highlights are utilized to construct include vector in this work, for example, Source IP, Destination IP, Source Port, Destination Port, Packet Size and Packet Type. Subsequently, we give the network highlight vector to SVM to learn network traffic practices. Exploratory outcomes demonstrate that contrasted and existing method; our proposed method can recognize network oddity traffic with high exactness.

3. Experimental Data Setup

3.1 Data Classification

During the classification phase of the scheme, the k-dimensional weight exhibits related with the input vectors are contrasted and the weight vectors of the l neurons of the map. The neuron with the nearest coordinate is announced a winner, and the corresponding input vector is classified accordingly. The decision making layer of the scheme generates the final decision on the classification of the noticed input pattern vector into attack or typical traffic flow.

3.2 Parameter selection

The training phase of the SOM algorithm is performed offline on the base station, using the patterns generated as a component of the example data. Before execution of the training phase, the SOM application is initialized with the chose SOM training parameter esteems. The initial qualities chose for the map are critical in defining a decent quality map design toward the finish of the training phase. The loads must be within the scope of estimations of the r dimensional pattern vectors in the example data set. Using simulations, we generated parameter esteems for the initial map dimensions, based on the example data consisting of both attack and ordinary network traffic. The map dimensions are chosen with the end goal that the proportion of the map dimensions is proportional to the square base of the determined proportion. The estimation of Δopt is chosen based on $\alpha = 0.95$ and other qualities are differed based on the hub sending thickness (N). The optimal map size is a function of the size of the training data set, and the k-dimensional estimations of the training data. A 100% finder hub proportion (n) is considered for all simulations. A sum of 5000 traffic packets comprising of both attack just as expected packets are introduced to the SOM application during the learning phase thus, another 5000 packets are introduced to the SOM application for genuine classification.

3.3 Evaluation

We performed simulations to generate results for the attack detection rates, false positive rates, and the false negative rates for varying estimations of N, and varying network traffic intensities.

4. Comparative Analysis

In Table 1, the normal detection rates for our proposed distributed attack detection scheme, are contrasted and corresponding detection rates, both initial (following network initialization), and normal over an objective hub's lifetime, of the SOM-based attack detection approach, for the following parameter esteems:

- α = 0.95.
- TI = 500.
- n = 100%.

The distributed attack detection scheme consistently yields high attack detection rates, when contrasted with the SOM-based approach. For N =128, both the distributed attack detection just as the SOM-based approach yield a normal detection rate of 56%.

Table 1: Detection Rate Comparison - distributed detection and SOM-based schemes

N	Distributed Scheme	SOM-based Scheme	
		Initial	Average
128	56	56	9
256	72	62	10
512	76	71	11.7
1024	87	84	13.4
2048	94	85	13.7

Nonetheless, the SOM-based scheme has consistent degradation in its performance over the time of the lifetime of the objective nodes. The normal detection rate of the SOM-based approach is only 9% before the energy content of the objective hub is totally drained. For all estimations of N, the SOM-based scheme has lesser accomplishment in attack detection, both regarding the initial detection rates, just as the normal detection rates. The reason for this consistent degradation in detection rates of the SOM-based approach is the inability of this strategy to perform retraining of the SOM neurons while the attack detection is taking spot, after the neurons are initially trained, at the base station. The postponements related with SOM re-training at runtime, hinder the chance of having such an approach applied in such a network environment, for attack detection. Comparisons between the normal detection rates for the two schemes imply the requirement for having distributed pattern recognition set up, to sustain high attack detection rates over the whole lifetime of the network.

In Table 2, we look at the initial and normal false alarm rates of the SOM-based detection scheme, with the normal false alarm rates of the distributed detection scheme. For all estimations of N, the false alarm rates (both false positive rate and false negative rate) are higher for the SOM-based scheme. The false positives of the two schemes are lower when contrasted with the false negative rates. In both the detection schemes, indicator nodes speak with their particular decision-making nodes, for example GN nodes with their assigned mGN nodes, and locator nodes with the base station in the SOM-based scheme. During this communication phase of the schemes, the complete numbers of malicious packets penetrating the network, and remaining unnoticed, increment the false negatives. On the contrary, the false positive rates are fundamentally influenced by the precision of the algorithm used in the detection scheme. For the distributed scheme, the false positives are generated when GN nodes generate attack signals, based on incorrect companion readings, for de-attire to their individual mGN nodes. In the SOM-based scheme, the false positives are generated based on the incorrect clustering of attack packets in the neurons, named as ordinary, during the initialization and training phases.

Table 2: False Alarm Rate Comparison - Distributed detection scheme and SOM-based schemes

	Distributed Scheme		SOM-based Scheme			
			Initial		Average	
N	FP Rate	FN Rate	FP Rate	FN Rate	FP Rate	FN Rate
128	5.2	39	14.5	29	30	60.2
256	3.4	25	23	11.4	29.6	59.3
512	2.9	22	16.7	8.4	29.1	58.3
1024	1.6	10	9.3	4.7	28.8	57
2048	0.4	4	8.1	4.1	28.5	56.9

The initial false negative rates are more similar for both the schemes. This is because of the property of the two schemes which demands regular communications both at the inter-hub level, just as at the hub base station level. The concentrated approach of the SOM-based approach yields preferable initial false negative rates over the distributed detection scheme.

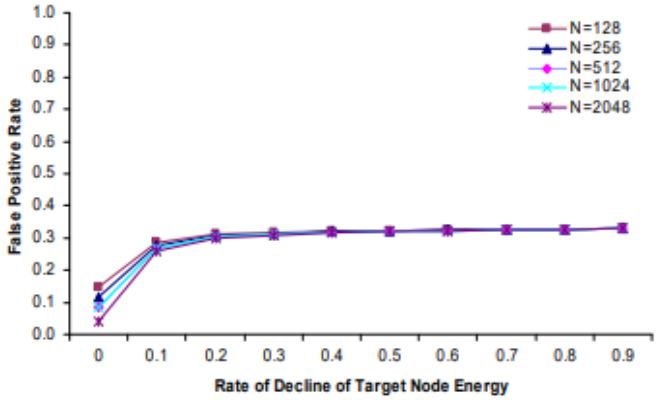

Figure 1: Average False Positive Rate vs. Rate of Decline of Energy Content in the Target Nodes. TI=500

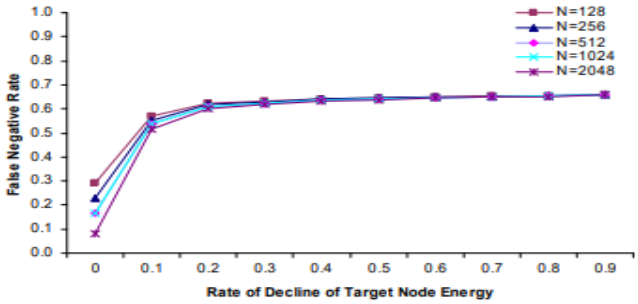

Figure 2: Average False Negative Rate vs. Rate of Decline of Energy Content in the Target Nodes

The affirm age false alarm rates over the lifetimes of the objective nodes, as illustrated in Figures 1 and 2, portray a degrading performance, with decrementing lingering lifetimes of target nodes. The normal false positive rate for N =2048 is 28.5%, and the normal false negative rate is 56.9%, when contrasted with corresponding estimations of 0.4% and 4%, for the distributed detection scheme. This is a direct result of the inability of the SOM-based scheme to update patterns at run-time to mirror the changing sub pattern values, depicting declining energy content of the objective.

5. Conclusion

The attack detection rates demonstrated a huge increase with increasing quantities of attack indicator nodes in the network. For more modest hub arrangement densities, the detection rates were lower, in any event, when not many packets (both attack and typical) penetrated the network. The motivation behind attack modeling was to ascertain that fitting attack detection approaches are hence proposed for detecting such attacks in a timely and energy-productive manner. In addition, the detection of such attacks is the initial move towards any counter-measures, including mitigation that might be fundamental for appeasing the impacts of the attack upon achieving accomplishment in attack detection.

References

[1] Hosny, Khalid & Rushdy, Ehab. (2020). New Detection Mechanism for Distributed Denial of Service Attacks in Software Defined Networks. International Journal of Sociotechnology and Knowledge Development

[2] Shurman, Mohammad & Khrais, Rami & Yateem, A.Rahman. (2020). DoS and DDoS Attack Detection Using Deep Learning and IDS. International Arab Journal of Information Technology. 17. 655-661. 10.34028/iajit/17/4A/10.

[3] Sharafaldin, Iman & Habibi Lashkari, Arash & Hakak, Saqib & Ghorbani, Ali. (2019). Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. 1-8. 10.1109/CCST.2019.8888419.

[4] Francisco Sales de Lima Filho, Frederico A. F. Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, Luiz F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning", Security and Communication Networks, vol. 2019, Article ID 1574749, 15 pages, 2019. https://doi.org/10.1155/2019/1574749

[5] Toklu, Sinan & Şimşek, Mehmet. (2018). Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service (DDoS) Attack Detection and Filtering. ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING. 43. 7923-7931. 10.1007/s13369-018-3236-9.

[6] Igbe, Obinna & Ajayi, Oluwaseyi & Saadawi, Tarek. (2017). Denial of Service Attack Detection using Dendritic Cell Algorithm. 10.1109/UEMCON.2017.8249054.

[7] Yao, Haipeng & Liu, Yiqing & Fang, Chao. (2016). An Abnormal Network Traffic Detection Algorithm Based on Big Data Analysis. International Journal of Computers Communications & Control. 11. 567. 10.15837/ijccc.2016.4.2315.

[8] Yan, Gao. (2016). Network Anomaly Traffic Detection Method Based on Support Vector Machine. 3-6. 10.1109/ICSCSE.2016.0011.

[9] Suroso, Jarot. (2016). Cyber Security for Website of Technology Policy Laboratory. 10.1007/978-981-287-988-2_58.

