International Journal of Mechanical Engineering

AN ADVANCED DDOS ATTACK DETECTION BASED ON LSTM DISTRIBUTED SECURITY NETWORK FUNCTIONS

[1]MADHUSUDHAN CHALAMAGUNTA, [2]SWATHI KAMBHAMPATI
[1]M.Tech Scholar, Dept of ECE, NRI Institute of Technology, Agiripalli, Vijayawada, A.P, India.
[2]Associate Professor, Dept of ECE, NRI Institute of Technology, Agiripalli, Vijayawada, A.P, India.

ABSTRACT:
Software Defined Networking (SDN) is a recent well known technology and defines as a new design and management platform approach for networking. The whole network will be affected if attacker access to the SDN controller. One of such security issues is the Distributed Denial of Service attacks (DDoS). So there is need to formulate an effective scheme to detect and mitigate DDoS attack in SDN. In this paper an advanced DDOS attack detection based on LSTM distributed security network functions is proposed. Time correlation of situation data can be established by the LSTM based neutral network which is used for raw data situation processing. Networks are generates this raw data. The real-time traffic is analyzed by the SDN controller with a set of distributed VNFs by examining every data packet properties individually and employing the classifier of Bayesian network (BN) along with machine learning Random forest algorithm to detect unusual packet flows. Entropy function can be calculated by finding protocol dependent VNFs to mitigate the DDoS attacks and functions of security network is implemented. Results gives that the proposed method have better discriminative performance in detecting and mitigating large-scale distributed attacks of network with less processing time and consequently assist in strengthening the security of the existing SDNs.

KEYWORDS: SDN, DDoS, LSTM, Machine learning, network security, botnets.

I. INTRODUCTION

Software defined networks (SDN) are used in the many companies and researchers plan to use it in the future also with more benefits. The security networks are strengthening by the architecture of SDN [1] the main advantages of SDN are centralized network monitoring and centralization of policy and security control those are not given by the present traditional networks.

So SDN becomes one of the most powerful security network platforms with these features [2].

There is no perfect network without any attacking of threats even the SDN networks also. The development of attacks in network is follows the network development. So of attacks in network should be one step after the security network development [3]. Even though SDN makes the secure system with its features, but central controller threats are attacked so that all the system may influenced by these central attacks [4]. The accessibility can be measures the availability of the system. If the unavailability of the system or data is affects the economical impact on the system.

The network security and their policies are guided by the CIA Triad pillar model which is abbreviated as Confidentiality, Integrity, and Availability. The privacy of the data can be explained by the confidentiality and trustworthiness of information which is refers to integrity of the data. For security purpose these integrity and confidentiality are the main parameters meanwhile availability of the data is secondary one [5].

Security intrusions are several types in that popular attack is Distributed Denial of Service (DDoS) by the attacker. In this attack the genuine users from same processing host or other sources network hosts are prevented. Due to these attacks various unnecessary actions are including in the communication which leads to disturbances in flexibility and scalability of system, different network types and applications integration, low latency [6].

By using machine-learning technique with neural network, DDoS attacks detection and mitigation of LSTM based security framework is proposed in this paper. Network attacks are immediately detected by the VNF in the data plane. According to three levels, the general structure of model is proposed in this paper. Situation awareness can be focused in the first layer. Situation of network security is reflected by the extracting indicators from network parameters of massive data.

Related data in first layer can be collected through LSTM based network and it is generated from the management and operation process. Present network security related information is extracted from the comprehension in the second layer. Input data is in the first layer and current security situation is described. Network security situation trend is changed before single intrusion alarm is focused. BN classifier and the machine leaning approaches are used in this paper. Based on current situation information, security situation of network is predicted. This prediction process is owned by the third layer and it gives awareness of the system security. This paper uses Entropy functions based on calculations of the layer.

II. DDOS ATTACK IN SDN

Entering of Distributed Denial of Service (DDoS) attacks into communication which reduces the system performance and increasing the power consumption of system by allowing the number of wicked traffic into system. DDoS attack is one of the main challenges in security of the Software Defined Network (SDN) [7]. Many different applications are offered by the SDN networks so DDoS attacks are removed and give the best SDN security system than normal networks.

Different types of DDoS attacks are can directly effects the control layer of SDN’s which are used for the purpose of communication between switches and controllers in SDN and these attacks such as State exclusion (Transfer Control Protocol state), application layer attacks (hypertext transfer protocol) and volumetric (amplification) attacks [8]. SDN structural design is having three layers as

- Application layer
- Control layer
- Infrastructure layer

These layers of SDN are affected by the DDoS attacks. The DDoS attacks are divided into three types according to the predefined targets in the network.

2.1 Application Layer DDoS Attacks

End-user business applications are existed in the Application layer and the user can accept the services and communication offered by the SDN. One of the DDoS attacks is Application Layer Distributed Denial of Service attacks where attackers target a particular application by exploiting application layer protocols, such as HTTP and SIP [9]. Two methods of application layer DDoS attacks are present in that first one is attacking of various applications and second one is attacking of northbound Application Programming Interface (API). All applications in the network are affected even one application contained DDoS attacks [10].

2.2 Control Layer DDoS Attacks

All switches in the network are controlled by the control layer so this layer is called as brain of SDN. By using the southbound API switches and controllers in SDN are communicated. DDoS attacks are targets the control layer because of its single point of failure risk for the SDN network. Control layer DDoS attacks lunching methods are attacking of northbound API, attacking of westbound API, attacking of southbound API, attacking of eastbound API and attacking of controller [11]. In the control layer DDoS attacks are attacked when several applications of different inconsistent flow rules [12].

2.3 Infrastructure Layer DDoS Attacks

Infrastructure layer is also named as data plane and containing the forwarding elements in addition with virtual switches like Open Switch and Juniper Junos MX-series called physical switches [13]. Through the open interface, switches and forward packets are accessed. Two types of Infrastructure layer DDoS attacks are present. First one is attacking of several switches and next one is attacking of southbound API. The packet should be stored itself in memory node awaiting the flow table entry is returned when the header information is transmitted to the controller [14]. Therefore in such case, DDoS attack can easily attacked on node by placing an unknown flow and new flows into the communication. The node of memory element is bottleneck because of its high cost so the attacker can easily entered the attacks into the memory. Many useless flow rules are generated by the fake flow request which should be hold by the Infrastructure layer so the flow rules storage for normal network flows is little hard [15].

III. LSTM BASED DDOS ATTACK DETECTION

This section presents the LSTM based distributed secure technique for early recognition and improvement of the DDoS (Distributed Denial of Service) attacks in SDN (Software Defined Network). The construction of this LSTM based security model for DDoS attack recognition and improvement is shown in figure (1), the overall performance analysis is explained in the following detailed manner.

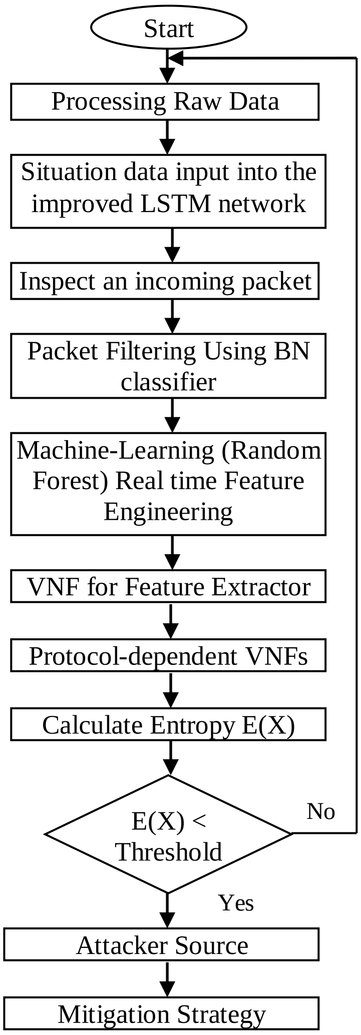
Start
Processing Raw Data
Situation data input into the improved LSTM network
Inspect an incoming packet
Packet Filtering Using BN classifier
Machine-Learning (Random Forest) Real time Feature Engineering
VNF for Feature Extractor
Protocol-dependent VNFs
Calculate Entropy E(X)
E(X) < Threshold
No
Yes
Attacker Source
Mitigation Strategy

Fig. 1: LSTM BASED SECURITY MODEL FOR DDOS ATTACK DETECTION AND MITIGATION

Improved LSTM network data source is pre-processes the obtained situation of raw data. In the beginning stage neural networks are trained by using the certain amount of labeled situation data. Networks can generate the Situation data which is processed and transferred into the network of LSTM. So into the controller of existing Open Flow new features of security type are implemented. On the Bayesian network model and filtering rules matching Packet filtering decisions are taken. By using the Random Forest algorithm, traffics are detected with the network monitoring based on machine-learning. In this algorithm VNF is missed so that accuracy of attack is improved. Every connection of input data and output classification is used in training model. Network security situation is achieved with calculation of quantitative situation values by using entropy and security situation changing trend is described in the classification results.

3.1 Processing raw data

According to time series, security situation of network is processed and maintained with the Network statistics. Simultaneously, in the overnight network attacks are not achieved. Several stages of relevant data behaviors are reflected and internal logical associations are generated serially. In processing some advantages are owned by the architecture of LSTM forms like serialized data but effective network security is not achieved by the single LSTM layer.

3.2 Improved LSTM network

Improved LSTM network design is proposed in order to overcome the above difficulties and leads to network security information improvement. Based on three layer LSTM stacks, depth of LSTM network is increased at starting stage. Neural network layer is directly connected to the LSTM network last layer. Security situations of different network data features are extracted by the trained model through LSTM stack network layers more accurately. So the mapping of time series with situation data is improved. Structure of neural network is optimized to a definite level and training time in a single-layer network, number of neurons is reduced with increasing the depth of network.

Neural network efficiency and performance are improved by this effect. Marked situation space is mapped with the pre-existing LSTM stack abstract features which is fully connected layer. Migration and Generalization of the model is guaranteed by the fully connected layer.

3.3 Packet filtering using BN

OpenFlow controller Security features are implemented by packet filtering of two types. One is packet filtering basic rules which are processed by inspecting each packet properties individually and second one is classifier of Bayesian network (BN) for filtering and detecting intrusion flows or DDoS attacks. On same IP destination address or same host repeated attacks are keeping track with a probability value of 0.8 and BN makes filtering decision. With this probability it is clear that the attacks are influenced the hosts. In the flow table packet information is stored in this case which is not needed.

3.4 Machine-learning-based Network

Machine learning based network monitor the SDN controller to detecting of huge traffic in the network and managing it by using Machine-learning algorithm. By using Random Forest algorithm in the proposed network, generates attacks with the public botnet dataset (CTU-13). Machine-learning techniques are not accepted by the proposed system directly, so with the Random Forest algorithm attacks are generated. The public dataset is having the best features in their generation of attack model and these features are type of services, flags, bytes, protocols and traffic information such as destination/ source port numbers and addresses. In the data plane real-time traffic feature dataset is collected by the SDN controller with the help of feature extractor network function. By using the Random Forest algorithm, attack model is retained with the public dataset in the control plane, and botnet real-time attacks are detected

According to intrusion detection systems of machine learning the attacks are analyzed. Based on feature extractor of virtual network function, information of real-time traffic is collected and also analyzed in the proposed system. Real-time traffic is monitored by generated attack models which are effectively used by the controller in coordinating with Network functions virtualization (NFV).

Previous datasets are generating the attack models. The machine-learning algorithm uses the collected and monitored feature information in the data plane by distributed network feature extraction in the controller. Large set of feature data or information is required for all techniques of machine learning and in the SDN controller; the switches slowing transfer to the statistical manager are overcome. This problem can be solved in NFV by feature extraction virtual network function which maintains a key role in detecting the intrusions SDN with NFV. Generated attack models are compared with incoming traffic which gives the confidence score results as presenting intrusions in the SDN incoming traffics or not. When existing attack models are exceeding the threshold value then controller reduces the incoming traffic. So real-time traffic is monitored by generated attack models and are effectively used by the controller in coordinating with Network functions virtualization (NFV)

3.5 Entropy Calculation

An event randomness and uncertainty is calculated by using the Shannon's entropy. Number of sending requests, destination IP and source IP are considered in this presented method. High value of entropy is obtained for more random variable and inversely, low entropy is obtained for less random variable. For every particular time window W, the victim server PACKET_IN entropy events are calculated.

The window can be expressed in the equation (1) and here random variable is x_i and frequency is denoted as y_i. The Equation (2) is used for calculating the entropy of specified time window W, where probability of predefined IP in the window W is denoted by $P(x_i)$.

$$W = \{(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_n, y_n)\} \text{ -- (1)}$$
$$P(x_i) = y_i/N \text{ ----- (2)}$$
$$N = y_1 + y_2 + y_3 + \cdots + y_n \text{ ---- (3)}$$

Specified time window receiving requests are denoted by N. All entropy in the particular time window for every source IP is calculated by below equation.

$$E(X) = \sum_{i=0} -P(x_i) log_2 P(x_i) \text{ --- (4)}$$

By using the particular time window entropy, the abnormal behavior of system is detected. According to the various elements these entropy values are calculated. The elements of fields are TCP flags, Source_IP address, number of requests per second and number of packets per second. There is a limited randomness is obtained for the attack. Then entropy value is decreases suddenly. For every time, window calculation is made to continuous in the system, if particular Source entropy is less than threshold and it will be continued for three consecutive time window then host of the botnet is separated out. If the system detected botnet host, then mitigation approach is performed, the hosts IP address is permanently blocked in the recognized botnet. Further any requests are not received by the server from the recognized botnet. Distributed Denial of Service attack Mitigation and Detection approach is performed inside the controller. The mitigating DDoS attack is illustrated in the system.

IV. RESULTS

The Mininet emulator is used in the presented method of this paper for testing. This process is consisting of three open flow switches with three hosts. In the network pre defined band width is 100 Mbps and in place of victim server host h3 is taken. The following DDoS attacks are executed in server and the attacker network called the botnet as Slow HTTP attack, Ping Flood attack and TCP SYN flood attack. Whole network configuration is described in the Table 1.

Table 1: CONFIGURATION OF NETWORK SETUP

Configuration	Resource
H3	Victim Server
HTTP	Victim Service
h1, h4, h5, h6, h7, h8	Botnet nodes
h2,h9	Benign nodes
200-300 packets for request/sec	Attack traffic
30-20 Packets per sec	Benign Traffic

Based on Python script, security functionalities are added to the existing Open Flow controllers and these are implements a prototype for the security evaluation of the proposed network. 42 attributes are involved in the 99 dataset and every record data processing in KDD CUP. In all attributes 41 are description and last one is a tag. In 41 attribute description, 34 are continuous attributes and 7 are discrete attributes. Actually 131 dimensions are present but only 42 dimensions are obtained. A model of trained neural network is set to test and generates a real situation comparison with reflected situation by models.

Mentioned attack parameters are set. 5 seconds of window size and 0.5 entropy threshold are made after different experiments outcome. Benign Traffic Scenario is implements the above calculations in the network. Targeted traffic is sending by the botnet host in order to perform the server attacks which are clearly mentioned in the Table 1. Proposed mitigation and detection technology uses the SDN controller POX based on python. Software Defined Network (SDN) OpenFlow protocol is provides flow rules efficiently in the controller and in addition to this packet dropping with forwarding is also implemented. TCP SYN connections and 1000 HTTP requests are processed by configured Victim Server. Normal operation of the server is disturbed by the traffic which is sending from the designed botnet. Then the victim server performs the attack. In the botnet, the attack script is raised for 20 seconds.

False positive rate is reduces in the improved LSTM network when other models are compared with it in the high risk situations and medium risk situations. Improved LSTM network evaluation and comprehension comparisons results are closer to the reality. Efficiency of different network structures is described in Fig. 3. High accurate security situation is obtained with the improved LSTM network while poor capability is achieved by traditional neural network.

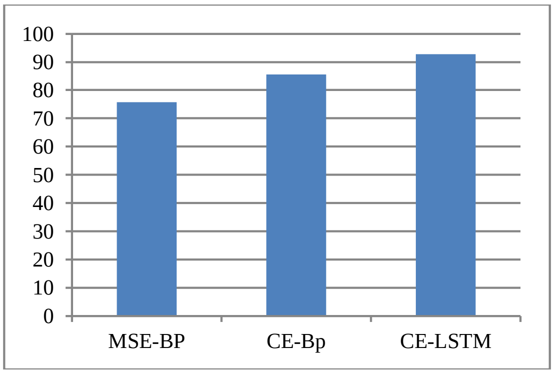

Fig. 2: COMPARATIVE EVALUATION ACCURACY OF DIFFERENT NEURAL NETWORK MODELS

Basic Open Flow controller is added to functions of proposed security system in order to evaluation of accuracy in detection. In this paper, fake packet filtering success rate is 90%. The comparative analysis of detection accuracy in both proposed Open Flow controller (BN Secure Flow) and basic Open Flow controller are described in the Fig. 3. Fake packets are detected between the accuracy as 86.00% and 95.00% (an average of 89.15%) and these results are better than the standard open flow controller.

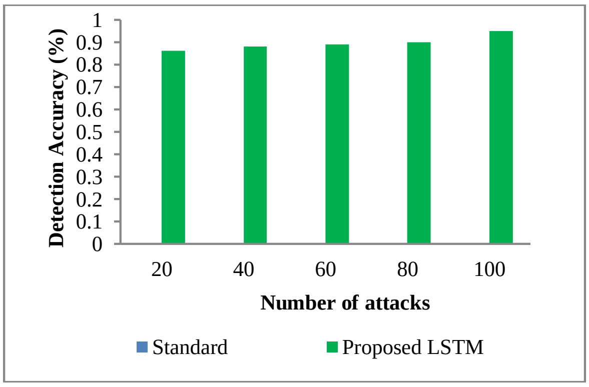

Fig. 3: ATTACK DETECTION ACCURACY

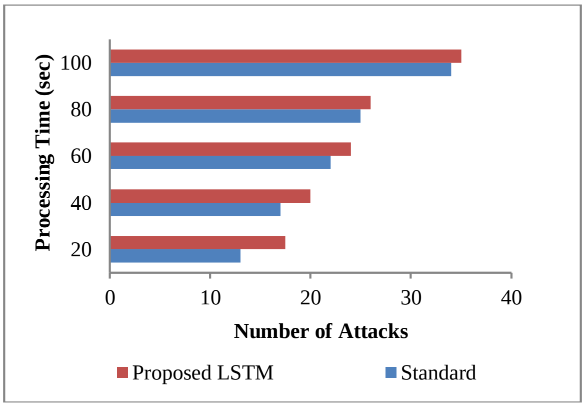

Fig. 4: DETECTION PERFORMANCE

On the other hand, the results are dependable and close to the target success rate. In the processing time results there is less difference in both standard open flow and proposed LTSM open flow models and depicted in the Fig. 4. The LSTM based distributed security gives less processing time, best performance and security.

V. CONCLUSION

In network environment major challenges are threats and these are influence the total system performance and security so their mitigation with detection is maintaining a main role. Thus this paper presented a LSTM based distributed security VNFs for DDoS attack detection and mitigation. Serialized data with Security situation awareness is analyzed with proposed improved LSTM network. Fake packets are filtered in the first step by using the filtering packet rules and properties individually. DDoS attacks are prevented by the classifier of Bayesian network (BN) and it is uses in second filter. botnet attacks are detected by the distributed security system using virtual security functions in NFV with an SDN controller is described in this paper. Protocol-specific attacks are detected by security network functions and traffic feature set information is extracted in the data plane. Distributed denial of service attack detection and its mitigation can be performed based on the entropy. Improved LSTM network evaluation and comprehension on comparisons results are closer to the reality. Real-time traffic is monitored by generated attack models and these are effectively used by the controller in coordinating with Network functions virtualization (NFV). Security threats in the environment of Software defined network can be detected and mitigated based on the traffic features and windowing of packets.

VI. REFERENCES

[1] Fernando Gehm Moraes, Luciano L. Caimi, Marcelo Ruaro, “A Systemic and Secure SDN Framework for NoC-Based Many-Cores”, IEEE Access, 2020

[2] W aseem Iqbal, Mahmoud Daneshmand, Haider Abbas, Yawar Abba Bangash, Bilala Rauf, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security”, IEEE IoT Journal, 2020

[3] Janakarajan Natarajan, Dijjiang Huang, Sandeep Pisharody, Abdullah Alshalan, Ankur Chowdhary, “Brew: A Security Policy Analysis Framework for Distributed SDN-Based Cloud Environments”, IEEE Trans. on Dependable and Secure Compu., Vol.: 16, Iss.:6, 2019

[4] Ye Li, Yanling Zhao, Guanggang Geng, Wei Zhang, Xichang Zhang, “A Survey of Networking Applications Applying the Software Defined Networking Concept Based on Machine Learning”, IEEE Access, 2019

[5] Anas AI-Far, Abdallah Qusef, Sufyan Almajali, “Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics”, 2018 International Arab Conf. on IT (ACIT), 2018

[6] Xiangyun Tang, Mohsen Guizani, Liehuang Zhu, Xiaojiang Du, Meng Shen, “Privacy-Preserving DDoS Attack Detection using Cross-Domain Traffic in Software Defined Networks”, IEEE Journal on Selected Areas in Commu., Volume: 36, Issue: 3, 2018

[7] Nelson A.S. Lima, Marcial P. Fernandez, “Towards an Efficient DDoS Detection Scheme for Software-Defined Networks”, IEEE Latin America Trans., Volume: 16, Issue:8, 2018

[8] Antanas Čenys, Simona Ramanauskaite, Justinas Janulevicius, Simona Ramanauskaite, “Modeling of two-tier DDoS by combining different type of DDoS models”, Open Conf. of Electrical, Electronic and Information Sci. (eStream), 2017

[9] Taghi M. Khoshgoftaar, Maryam M. Najafabadi, Clifford Kemp, Chad Calvert, “User Behavior Anomaly Detection for Application Layer DDoS Attacks”, IEEE International Conf. on Information Reuse and Integration (IRI), 2017

[10] Hitoshi Aida, Mohamad Samir A. Eid, “Secure Double-Layered Defense against HTTP- DDoS Attacks”, IEEE 41st Annual Computer Softw. and Apps. Conf. (COMPSAC), 2017

[11] Wu Chou, Li Li, Min Luo, Wei Zhou, “Design Patterns and Extensibility of REST API for Networking Applications”, IEEE Trans. on Network and Service Manag., Vol.: 13, Iss.:1, 2016

[12] Pin Liu, Jian Zhang, Yawei Zhang, Jianbiao He, “A Hadoop Based Analysis and Detection Model for IP Spoofing Typed DDoS Attack”, IEEE Trustcom/BigdataSE/ISPA, 2016

[13] Marinos Charalambides, Daphne Tuncer, George Pavlou, Stuart Clayman, “Adaptive Resource Management and Control in Software Defined Networks”, IEEE Trans. on Network and Service Management, Volume: 12, Iss.: 1, 2015

[14] Peter Pereíni, Dejan Kostic, Maciej Kuzniar, “OpenFlow Needs You! A Call for a Discussion about a Cleaner OpenFlow API”, Second European Workshop on SDN’s, 2013

[15] Xuan Luo, Conghui Bi, Yaohui Jin, Tong Ye, “On precision and scalability of elephant flow detection in data center with SDN”, IEEE Globecom Workshops (GC Wkshps), 2013