International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 3043–3047

Anomaly Detection in SDN Assisted Social Media Communications using Improved Deep Learning Algorithms

Gupta Rounak,
Ph.D. student , University of Technology, Jaipur.
Dr. Zha Chanakya Kumar,
Ph.D. Guide , University of Technology, Jaipur.
rounak_gupta@rediffmail.com

Abstract— *The internet traffic of social media saw tremendous growth in recent time, owing to the ongoing development and utilizing of application and services based on multimedia Nowadays the network based communications becomes more vulnerable to the several security threats called anomalies due to widespread growth and interest of using the social method web portals worldwide. Thus it becomes necessary to scan the Online Social Networking (OSN) multimedia communications to detect the security threats that may harm the important data of end users. Designing the paradigm of secure multimedia data transmission plays the vital part in finding out all essential necessities of OSNs like Quality of Service (QoS), reliability and measurability .The paper provides a review on anomaly detection in SDN using deep learning algorithms.*

Keywords—Anamoly Detection, SDN, Social Media Communication, OSN and Deep Learning Algorithms

I. INTRODUCTION

Due to open nature communications, it is required to scan the Online Social Networking (OSN) multimedia communications for security threats detection that may harm the important data of end users. Designing the paradigm of secure multimedia data transmission plays the vital job in estimating important necessities of OSNs like reliability, scalability, and Quality of Service (QoS). To mitigate the challenges with security threats detection, one can design the anomaly detection in combination with the Software Defined Network (SDNs); but there are several problems that must be address namely energy-conscious networking and security at runtime. The recent solutions introduced for both the problems are not reliable by considering the run-time data noise or drifts for runtime anomaly detection as well as non-optimization based multi-objective flow routing may creates the bottleneck in SDN assisted multimedia data transmissions.

To Internet of thoughts from Internet of Things this widening scope had led to popular network of social platform. It became most robust, richest, largest and highest level of dynamic proof of human behavioural pattern which had brought new landmark and scope for studying, analysing and understanding counties, societies, groups and individuals. Current focusing

and analysing into the arena of worldwide social media had shown that there exist almost 4 billion Internet users, part of whom makes active users on social media platform a whopping of around 3 billion [1]. Owing to such exponential expansion of socially active networks, Multiple-media based informative data have expanded with rate of uncontrolled manner [2]. But, object-oriented pattern and content-driven information from multiple-media of social networks focuses problems of scaling useful analysis about such continuous changing and always on expansion of size in information. Additionally, the considerable amount of multimedia content provided on social networking platform consist of delicate, personnel and sensitive data related to users and their communications. These massive availability of personal and sensitive information that is easily accessible results in high susceptibility to threats leading to identity theft and exploitation of personal information. Hence, security and information interchange like interoperability remains two major issue to be resolved in underlying network framework [3]. Therefore, persistent adding to its measurable communicative platform became the requirement for data analytic professionals and social multimedia data management thereby keeping sufficient amount of security for fool proof operations.

ISSN: 2233-7857IJFGCN

Numerous research and efforts has been done on SDNs that have attained worldwide attention from Industries as well as research scholars from academics. Its architecture is grouped in a control plane and data plane; this framework consist of a layered infrastructure, layered application and a layered control [4]. But, at the same time SDN is susceptible to attacks with least security, as it is prone to attacks like overloading of flow table, saturation of control plane , ID spoofing, link spoofing, Distributed Services on Denial (DDoS), new flow and man-in-the-middle attacks[5]. Either host or network base solutions can be useful for Security of SDNs. Multiple scatter sources attacks the system in DDoS attack, in such a manner that it does not allow access to authenticated users taking part in communication network [6].

Various method are used to detect and prevent DDoS attacks namely the Connection success ratios, blacklisting of IP, aggregate analysis and connections of throttled in working can detect as well as prevent attacks in DDoS domain. When SDN is attacked it disturbs function of data-control interfaces, control layer and data layer. DDoS attack Mitigation Framework (DDMF) and detection had been put forth by researchers of [4]. It's a network design that consists of a detection server, SDN router application and capture server. These parts functions by studying and analysing data traffic of network. By utilising a technique called an echo request messages, invalid switches are recognised; routers that are invalid are also estimated and determined. Blocking ofDDoS attacks which traffic flow had predicted is also the responsibility of detection server. Real time analysis of traffic Open Flow, DDoS attacks of different kinds could automatically sensed using simple sampling techniques [11]. To analyse operating policies and strategies, configuration of controller in open flow with the help of mechanism of Finite State Machine (FSM) . Using semi qualitative of open standard, To find out prone level of severity using semi quantitative scoring system in SDNs is explained [7]. Combination is done in Common Vulnerability Scoring System (CVSS) with support from an Analytical Hierarchy Process (AHP) and SDN characteristics. From AHP help, a hierarchal structure is designed and developed by measuring and calculating SDN asset weights mathematically. Later, CVSS executions takes place on the basis of their weights.

To perform DDoS attack mitigation, maximum number of researchers have emphasised on traffic analysis. Cloud architecture relates to association with Software Defined Networking (DaMask), rather than by a controller, mitigation and attack detection occurs through a cloud provider. SDN failure vulnerabilities of a single point (i.e., owing to single controller's failures)were resolved when design of distributed multi-controller is applied. From [8], a Distributed Rule Store (DRS) were suggested with application in multicontroller framework that consist protocols of flow were processed with cached applications that are present in controllers across all over. When a flow of suspicious in nature is detected and identified, every controller is equipped with a set of protocols hat can be changed. A cloud-supported multicontroller is designed to guard an SDN against Byzantine-Resilient attacks is discussed in [9], Requirement First Assignment (RQFA) algorithm is put forward by the authors here. Controllers to Switches that depends on necessity of a number of controllers is assigned by this algorithm (i.e., in accordance to fault-tolerances of switches, required controller numbers varies dynamically). Update confirmation in table flow records from switches are allowed by using multiple controllers. To defend against spoofing attacks CAuth is applied in SDNs. A collective method is designed and calibrated by exploiting messages of Open Flow systems.

Recently, researchers working on Cyber security have designed and developed various models for anomaly detection that guards SDN from assaults created from users of mischievous wicked behaviour against various multimedia uses like video conferencing, video-on-demand that is remotely controlled, online gaming, informative data delivery in real time , etc. With such scenarios, Architecture of deep learning like Deep Belief Networking (DBN), Convolution Neural Networking (CNN), Stacked Auto Encoders Restricted Boltzmann Machine (RBM), Recurrent Neural Networks (RNN), etc., are mostly used. This research efforts initiates and attempt to suggest deep learning depending upon efficient framework for suspicious flows detection and sensing in SDN architecture.

II. Literature Review

[10] Shows, An attack of IP spoofing behaves like a component like hub, other network device or as a switch, that later moves to higher level—man-in-middle attacks. Such assault could be sensed with help from application design which overlooks a packet of information whose validation outcome is expected to remain same outcome as that of spoofing of IP.

[11] Depicts, CDNi network detects IP spoofing attacks in SDN architectures, in which, to plot the network and transmission costs, Server Implementation of Application Layer Traffic Optimization (ALTO) were done. Information Packets are encoded after

ISSN: 2233-7857IJFGCN

reaching at switches, however they should align with already partition specific of IP and ID base addresses. After sensing packets of information that are spoofed they were primarily blocked and later traced backed to source. However, encryption of data packets need some time for decoding, leading for enhancing in delayed network if huge amount of data packets reaches at switches. IP addresses are not only involved during spoofing attack but can also occur during link transmission.

[12] Emphases, DoS attacks are sensed and detected by making use of proposed technique which construct a hopping multicast tree structure. Game theory is used to analyse attackers, but description of this is inadequate. A node is targeted by an attacker in a network during period of hopping. The attackers compromises the genuine nodes in this way. In multicast routing, designing of such task and development is done in preventing DoS assaults.

[13] Signifies, that authors had employed a method that uses remapping of user switches from SDN-dependent switches that are proxy in nature are accountable in relaying flow of data amongst the servers and users. To maximize rate of attack separation, greedy algorithm was also deployed. To find out if a data packet had actively participated in a DDoS assault, traffic detector and sensor was implemented over every proxy switch with suitable edge values. Originally at the beginning, users were dynamically plotted to switches of proxy; later, post sensing and identifying the perpetrator; remapping of authenticated users are dome to another proxy server. But, such recalibration of user procedure leads to complex network.

In [14], authors mentioned, controllers were prone with attacks of flooding (i.e., DDoS attacks). Thereby, they suggestion of possible technique for protecting with such attacks are discussed. A controller creates a temporary table ‘‘T’’ in this methodology, which keeps addresses of IP in forwarded data packets of information. Number of data packets that are accepted with every specific addresses of IP is also maintained in this tables. The controller utilises idle timeouts and hard timeouts for separation of usual records from attackers to diminish their effects. With increase in packet counts, DDoS attacks are identified correspondingly. However, Bulk attacker traffic was unable to withstand in this method.

For [15], Design of SDN signifies in resolving majorly three security threats: unchecked hashing techniques mitigates signifies attack of spoofing, with construction of framework based on star topology, flow table overloading is solved, fuzzy organizer mixed with L1-ELM executing on network of neural for segregating and quarantining anomaly packet of data from usual packet of information. For effective flow migration Finite-State Markov Chain model with Discrete-Time is used.

In [16], author developed a typical event detection method for application that uses videos where 3-dimensional CNN are used to get spatiotemporal data of inputs. This technique that is suggested depends on non-supervised learning. Unsupervised learning and sparse coding are collectively improved for video information to find out video anomaly detection.

For detection of uncommon events in videos through intra-frame classification and Stacked Sparse Coding strategies based on probabilistic outcome of SVM is proposed by author in [17]. Author used a full CNN for finding out differentiating outcome in crowded activities as mentioned in [18]. Convolutional Auto encoder (CAE) is presented by author In [19], for anomaly detection scheme where aggregation of high-level characteristics were performed along with input frames for analysing CAE performance effect.

Author proposes Motion Deep Net and Appearance model in [20], aimed at anomaly sensing and identification in videos by deep neural networks and multiple single-class SVM models. Aimed at abnormal event sensing author invented a model based on deep learning that was included in [21], where PCA Net was applied to learning of feature, and a proposal for studying the video happening patterns deep Gaussian mixture model was used.

Author advocated a hybrid model network of neural in [22], intended at typical identification of emotion and sensing at social media through combining of Memory scheme of Long-Short Term and CNN . As such techniques are dependent on end-to-end representation learning and training, they find common use in pattern recognition as compared to old fashion machine learning techniques .

Author constructed traffic anomaly based on SDN for detectionin [23], to recognise assault that rely on important diversion with already existing profiles of standard in use. With improved nature two algorithms: such as unsupervised cluster-dependent feature

ISSN: 2233-7857IJFGCN

choice mechanism and clustering algorithm that depends on density peak with sampling adaptation is also suggested for handling unlabelled, large-scale and high dimensional network data.

Author presents SDN-based flow detection method In [24], by applying K-nearest neighbours algorithm where transductive confidence machines with double P-value was used for grouping of SDN flows. Author specifies a strategy for sampling of traffic for software-defined networking (SDN)In [25]. The suspicious traffic sampling were performed instead of analysing all packets that reduces rate of capture-failure male volentin formation flow.

For detecting uncommon patterns on a network traffic an SDN-based ecosystem is presented by the author in [26], in which analysis of multiple -feature were implemented in profiles that exhibits usual usage of traffic. To provide encouraging outcomes in all these techniques, SDN had proven itself.

An anomaly based on hybrid deep-learning that is used for sensing and detecting techniques for detection in suspicious flowin [27] is proposed by author, in accordance to social multimedia. They constitutes of two modules as mentioned : (1) Top to bottom information transfer unit for fulfilling strict QoS is need with SDN, specifically, low latency and high bandwidth (2) an anomaly sensing and detecting unit which influences better limited Boltzmann machine and support vector machine that is gradient descent-based to detect activities of suspicious in nature.

TABLE 1: A Comparison Table of different methodology

Sr. No.	Name of the Implementation	Method	Dataset
1	Abnormal Event Detection in Large Videos using Sparse Coding Guided Spatiotemporal Feature Learning for	sparse and unchecked coding	UCSD , Subway and Avenue datasets
2	Suspicious Flow Detection using Anomaly Detection Scheme	Deep learning	Thapar Institute of Engineering & Technology (TIET)’s data traffic in real time.
3	Software-Defined-Networking-Enabled Detection of Traffic Anomaly	Density peak clustering algorithm and refined unsupervised feature selection	KDDCup99

III. CONCLUSION

This paper provides a review on anomaly detection using deep learning methods. It mainly focuses on detection in SDN assisted social media communication. The paper gives an introduction to anomaly detection. The previous work relate to paper is discussed. It also provides a comparison of different methods with different data sets.

ISSN: 2233-7857IJFGCN

REFERENCES

[1]. D. Chaffey, "Global Social Media Research Summary 2018," Smart Insights, Tech. Rep., 2018. [Online]. Available: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/
[2]. S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: Vision and challenges," Ad Hoc Networks, vol. 33, pp. 87 – 111, 2015.
[3]. M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: threats and solutions," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014.
[4]. Q. Yan and W. Huang, "A DDoS detection and mitigation system framework based on spark and SDN," in *Proceedings of the International Conference on Smart Computing and Communication*, vol. 10135, pp. 350–358, 2016.
[5]. N. M. Sahri and K. Okamura, "Collaborative spoofing detection and mitigation—SDN based looping authentication for DNS services," in *Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference, COMPSAC*, pp. 565–570, Atlanta, GA, USA, June 2016.
[6]. F. Shahzad, M. A. Khan, S. A. Khan, S. Rehman, and M. Akhlaq, "AutoDrop: automatic DDoS detection and its mitigation with combination of Openflow and Sflow," in *Proceedings of the International Conference on Future Intelligent Vehicular Technologies*, vol. 185, pp. 112–122, 2016.
[7]. S. Zerkane, D. Espes, P. Le Parc, and F. Cuppens, "Vulnerability analysis of software defined networking," in *Proceedings of the International Symposium on Foundations and Practice of Security*, vol. 10128, pp. 97–116, 2016.
[8]. H.-z. Wang, P. Zhang, L. Xiong, X. Liu, and C.-c. Hu, "A secure and high-performance multi-controller architecture for software-defined networking," *Frontiers of Information Technology & Electronic Engineering*, vol. 17, pp. 634–646, 2016.
[9]. H. Li, P. Li, S. Guo, and A. Nayak, "Byzantine-resilient secure software-defined networks with multiple controllers in cloud," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 436–447, 2014.
[10]. A. Kaur and A. Bhandari, "Detection and mitigation of spoofing attacks by using SDN in LAN," in Proceedings of the Sixth International Conference on Soft Computing for Problem Solving, vol. 547 of Advances in Intelligent Systems and Computing, pp. 240–247, Springer, Singapore.
[11]. N. I. Mowla, I. Doh, and K. Chae, "An efficient defense mechanism for spoofed IP attack in SDN based CDNi," in Proceedings of the 2015 International Conference on Information Networking, ICOIN 2015, pp. 92–97, Cambodia, January 2015.
[12]. Z. Zhao, F. Liu, and D. Gong, "An SDN based hopping multicast communication against DoS attack," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 4, 2017.
[13]. Q. Wei, Z. Wu, K. Ren, and Q. Wang, "An Openflow user-switch remapping approach for DDoSdefense," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 9, pp. 4529–4548, 2016.
[14]. N.-N. Dao, J. Park, M. Park, and S. Cho, "A feasible method to combat against DDoS attack in SDN network," in *Proceedings of the 2015 International Conference on Information Networking, ICOIN 2015*, pp. 309–311, Cambodia, January 2015.
[15]. DeqingZou, Israa T. Aziz,and Bin Yuan, "Validating User Flows to Protect Software Defined Network Environments," *Security and Communication Networks*, Volume 2018, Article ID 1308678, 14 pages.
[16]. W. Chu, H. Xue, C. Yao, and D. Cai, "Sparse Coding Guided Spatiotemporal Feature Learning for Abnormal Event Detection in Large Videos," IEEE Transactions on Multimedia, 2018, DOI: 10.1109/TMM.2018.2846411.
[17]. K. Xu, X. Jiang, and T. Sun, "Anomaly Detection Based on Stacked Sparse Coding With Intraframe Classification Strategy," IEEE Transactions on Multimedia, vol. 20, no. 5, pp. 1062–1074, 2018.
[18]. M. Sabokrou, M. Fayyaz, M. Fathy, Z. Moayed, and R. Klette, "Deepanomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes," Computer Vision and Image Understanding, 2018, DOI: https://doi.org/10.1016/j.cviu.2018.02.006.
[19]. M. Ribeiro, A. E. Lazzaretti, and H. S. Lopes, "A study of deep convolutional auto-encoders for anomaly detection in videos," Pattern Recognition Letters, vol. 105, pp. 13 – 22, 2018.
[20]. D. Xu, Y. Yan, E. Ricci, and N. Sebe, "Detecting anomalous events in videos by learning deep representations of appearance and motion," Computer Vision and Image Understanding, vol. 156, pp. 117 – 127, 2017.
[21]. Y. Feng, Y. Yuan, and X. Lu, "Learning deep event models for crowd anomaly detection," Neurocomputing, vol. 219, pp. 548 – 556, 2017.
[22]. X. Sun, C. Zhang, S. Ding, and C. Quan, "Detecting anomalous emotion through big data from social networks based on a deep learning method," Multimedia Tools and Applications, 2018, DOI: 10.1007/s11042-018-5665-6.
[23]. D. He, S. Chan, X. Ni, and M. Guizani, "Software-Defined-Networking-Enabled Traffic Anomaly Detection and Mitigation," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1890–1898, 2017.
[24]. H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. Sun, "A detection method for anomaly flow in software defined network," IEEE Access, vol. 6, pp. 27 809 – 27 817, 2018.
[25]. T. Ha, S. Kim, N. An, J. Narantuya, C. Jeong, J. Kim, and H. Lim, "Suspicious traffic sampling for intrusion detection in software-defined networks," Computer Networks, vol. 109, pp. 172–182, 2016.
[26]. L. F. Carvalho, T. Abr˜ao, L. de Souza Mendes, and M. L. Proenc¸aJr, "An ecosystem for anomaly detection and mitigation in software-defined networking," Expert Systems with Applications, vol. 104, pp. 121–133, 2018.
[27]. S. Garg, K. Kaur, N. Kumar and J. J. P. C. Rodrigues, "Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective," in *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 566-578, March 2019. doi: 10.1109/TMM.2019.2893549

ISSN: 2233-7857IJFGCN