Software Defined Network: Security Attacks and Solutions for Security Enhancements

SULBHA MANOJ SHINDE[1], Dr. GIRISH ASHOK KULKARNI[2]
[1] *Associate Professor, Department of E&TC, SSGBCOET Bhusawal, India*
[2] *Head and Professor, Department of E&TC, SSGBCOET Bhusawal, India*

Abstract— The fundamental idea behind SDN technology is the separation of the data (forwarding) layer from the control layer. Contrary, the traditional network comprises the data layer and the control layer together. The framework of the SDN offers a logically centralized network control and its management through a central controller. The communication devices in the data layer forward traffic according to control requests. It also provides dynamic programming and reconfiguration of rules and policy settings, which decreases the risk of cybercrime attacks. The downside of SDN separation led to innovative network security challenges, such as Denial-of-Service (DoS) threats. This paper deals with main security issues of the SDN Network and it's problems and security attacks that may affect the structure of network. Review of previous research done is also presented. Different Attempts associated with security related design issues for SDN and the future needs to secure SDN Network is also presented.

Indexed Terms- SDN, firewall, DDoS, POX, authentication.

I. INTRODUCTION

There are the following main issues related to SDN:
Forwarding Device Attack: The network traffic can be disturbed by access points or switches, which results in malicious users launching denial of service (DoS) attack that can result in network failure or disruption.

Threats in Control Plane: Due to the use of central controller, any problem arising in the network results in the failure of the central controller. The approach that is being used to solve this problem is to use either horizontal or hierarchical controller distributions.

Vulnerability of Communication Channel: SDN southbound API's such as Open Flow protocol uses TLS for data-control channel communication security but it is often disabled administratively and is prone to man-in-the middle attacks thus not suitable for implementation of channel security.

Fake Traffic Flows: A non-malicious faulty device or an attacker can launch this or DoS attack to dissipate the resources in forwarding devices or controllers.

Authenticity: It refers to the property that entities in networks are actually the ones they claim to be. the issue of authenticity for forwarding devices in SDWN networks is similar to that in traditional networks; it can result as hindrance in network performance.

Confidentiality: it prevents from the expose of information to unauthorized users, if not ensured can lead unauthorized users to access network information or data.

Availability: It means that authorized users can access data, devices, and services whenever they need.

Open Programmable API: The open nature of API makes the vulnerabilities more transparent to attackers.
Man-in-the-Middle-Monitors: The switches and the controllers are not directly connected for the transmission of information, which "man-in-the-middle" monitors can steal or misuse the information without being caught thus leading to black hole attack.

II. SDN SECURITY ATTACKS AND SOLUTIONS

According to six features could be identified to achieve and obtain the prospective network security improvements based on the implementation of SDN infrastructure and deployment. The identification of these features provides effectiveness to build up or develop more secure and reliable SDN applications or SDN infrastructure. This section reviewed, the

opportunities introduced by SDN to network security from various research works. This will offer novel insights for future research in this significant area.

2.2Collect Traffic, Detect and Mitigate Attacks

In this stage, a method involved collecting intelligence data from previous Intrusion Detection Systems and Intrusion Prevention Systems, followed up by investigation and consolidated reprogramming of the network, which can offer the SDN more efficient and reliable to intrusion attacks than traditional networks will be discussed. This process is well illustrated as Step one the Collector, in which traffic information is collected through the Open Flow protocols. Step two the intrusion Detection, at this stage analysis is performed on the statistics, and intrusion is identified. Step three the intrusion Mitigation, at this stage flow-entry can be injected to override the known attack. In Table 2.2, a comprehensive fact of the problems and solutions presented for each research work introduced under collect, detect, and mitigate to protect and provide Network Security Enhancements in SDN is provided.

Table 2.2 Research Works Based on Collect-Traffic, Detects, and Mitigates Attacks.

Reference	Problem	Solution
[1]	Control layer DOS traffic overload during Open Flow traffic collection.	Developed an SDN-based Intrusion detection system and intrusion prevention system on traffic Collection Modules for intrusion Detection and intrusion Mitigation.
[2]	Defective and Uncertain Programmable Security Infrastructure.	Provided Network Response Control that providing consistent security.
[3]	Issues of intrusion detection for embedded portable devices.	Used Open Flow SDN to identify intrusion traffic and reconfigure the network.
[4]	Avoid data centre network congestion challenges.	Used Open Flow proxy device to identify traffic overload based on flow aggregation.
[5]	ome weaknesses of network security applications.	Orchestrator-based SDN model to implement security applications.
[6]	To provide effective security to SDNs at the infrastructure layer.	A cognitive module is applied in the infrastructure layer.
[7]	Issues of DDOS overload in SDN.	A confidence interval and mean throughput are applied at the SDN controller to identify intrusions.
[8]	The problem of monitoring and detection of anomalies behaviour at the data layer.	Introduced intrusion detection to classify and validate using machine learning algorithms.

2.3Rule Updating and Traffic Analysis

This category of SDN security enhancements s recognized by their effort on a particular intrusion detection and prevention scheme enforced. Precisely, the high-level security rules are established based on network traffic analysis and applied by computerized switches to enforce policy or rule updating [11]. This system is introduced for securing enterprise networks and its results are range from dynamic access control to traffic tagging an3108d filtering [12]. Generally, tools are used to checks a distinct traffic statistic condition against locally collected traffic packets to define an appropriate action or request [13], [14]. In Table 2.3 , a summary of the problems and solutions offered for each research work presented under Rule Updating and traffic analysis on Network Security Enhancements in SDN is supplied.

Table 2.3 Research Works Based on Rule Updating and Traffic Analysis

Reference	Problem	Solution
[15]	To increase the capacity of enterprise network attack response.	Provided Dynamic access control system for securing enterprise networks.
[16]	To Protect the Control layer against DOS intrusions and dynamics flow response.	Introduced Connection Migration Tool dropping data-control layer communication and Initiating Prompt to install flow rules.

[17]	To Protect enterprise networks against Computer viruses (malware) distribution.	Introduced Traffic flow monitoring and classification for flow tracking and filtering.
[18]	To recurrently change host IP addresses for mobile defense targets.	Presented Random Host Mutation using virtual-to-real IP translation.
[19]	To protect against network and service exploration.	SDN-based mobility Target network defense systems.
[20]	To protect exposed virtual systems in cyber space from being compromised.	Introduced Network anomaly detection, measurement, and counter measure assortment framework.
[21]	Overcome the performance flexibility problems of present Intrusion Prevention Systems.	Introduced an enhanced Open Flow-based Intrusion Prevention Systems to improve latency and accuracy.
[22]	The problem of reconfiguring cloud networking on the fly with the Intrusion Prevention Systems.	An enhanced SDN-based Anomaly Prevention solution.
[23]	Issue of increasing capacity of network traffic.	Provided Scalable IDS model with sampling rate modification technique.
[24]	Issues of home/ office network security problems.	Introduced Intrusion Detection techniques mounted in NOX controller.
[25]	To Use SDN to identify and secure the network from malicious attacks.	Develop a fuzzy logic-based information security management system for SDN.

2.3DOS/DDOS Protection

In Table 2.4 , a precise description of the problems and solutions provided for each research work presented under DOS/DDOS Protection on Network Security Enhancements in SDN is conveyed.

Table 2.4 Research Works Based on DOS/DDOS Protection

Reference	Problem	Solution
[26]	Issue of DDOS attack detection.	Presented Statistical information with self-organizing maps method to categorize traffic flow as normal or malicious.
[27]	Issues of DDOS attack detection and response in the content-oriented network.	The rate and pattern of content requests are examined to identify DDOS attacks.
[28]	The problem of DDOS attack detection and response.	Use Open Flow to identify and drop DDOS traffic based on traffic flow capacity.
[29]	To Overcome the problem of detecting and blocking DDOS attacks by botnet	Introduced DDOS blocking solution for SDN-managed network.
[30]	Problems of DOS at the Controller and performance flexibility.	roduced Entropy-based rule and Correlation-based rule to identify DDOS attacks against SDN controllers.
[31)	To stop Threat targeting and overloading the SDN controller.	Presented an optimized technique to Classify and identify malicious traffic flow based on Traffic Statistics.
[32]	Problems of DOS attack identification and mitigation on Open Stack Cloud.	The introduced firewall security system is an efficient model for protecting Open Stack cloud infrastructures.
[33]	Issues of network performance due to DOS cyber-attacks.	Implemented security scheme on SDN model, at the client-side.
[34]	Ineffectiveness of machine learning	Applied feature selection methods for data pre-

	classifiers in classifying DOS traffic redundancy.	processing.
[35]	Issues of traffic overload at the controller.	ed mean entropy andthe rate of percentage drop to stop the occurrence of DDOS attacks.
[36]	Issue of DOS attack flooded at the controller affecting SDN performance.	Introduced a NID scheme to improve the performances of the SDN controllers against DOS attacks.
[37]	SDN lacked an effective mechanism to detect malicious traffic. The problem of using a single controller. Issue of correlated data in an available dataset.	Proposed machine learning-based NIDS methods for detecting. Introduced multiple controller systems to tackle new incoming packets. Introduced feature selection methods to a produced redundancy-free dataset.

III. SDN Security Design and Services

It's important to consider SDN security challenges and middle boxes when designing and deploying SDN architecture. SDN security problems, middle boxes, and application service necessities to identify the vibrant platforms in which SDN will be deployed e.g. cloud, data centre, and mobile. SDN characteristics are provided to incorporate network layer with security middle boxes such as intrusion prevention system or Firewall to stop intruders at the network end. To offer protected visibility of networks through dynamic and multiple networks, innovative security designs will be essential. SDN-based Security models or applications have related to improving network security when integrated with intrusion detection systems or prevention systems. In Table 2.5 , a summary of the problems and solutions identified for each research work provided under SDN Security design and services for Network Security Enhancements in SDN is presented.

Table 2.5 Research Works Based on SDN Security Design and Services

Reference	Problem	Solution
[40]	To Guarantee consistency in network policy reinforcement in the presence of SDN Architectures.	SDN architecture adds tags to outgoing traffic flow to provide correct context.
[41]	To provide Efficient SDN-specific traffic steering.	Tag and tunnel traffic between SDN architecture.
[42]	To overcome the problem of Quality of Service assurance in security traversal.	Introduced dynamic security traversal scheme with SDN models.
[43]	To Restrict secret traffic channels.	Introduced Multi-level security network switch using Open Flow filter.
[44]	To control network traffic flow through security monitoring applications.	Used Open Flow to implement trigger policy for identifying and handling traffic paths.
[45]	To improve monitoring activities for cyberspace networks.	Introduced SDN Application to control and direct traffic flows through security services.
[46]	Use SDN to protect the internal network from intrusions.	Secure traffic analysis system to trace malicious behaviors on internal networks.
[47]	Problems of data exploration and conspiracy between compromised nodes.	Presented an SDN-based forensic model that monitors, investigates and tracks network behaviors.
[48]	Problems of program network devices flexibility to eliminate the need for third-party vendor-specific hardware.	Presented an SDN-based multi-vector DDOS detection system to secure enterprise network infrastructure.

IV. AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

AAA signifies Authentication, Authorization, and Accounting. It involves in a group of protocols that

facilitate network access control [49]. Scott-Hayward et al. defined AAA as a structure for logically controlling access to computer data and information, implementing policies/rules, checking network usage, and offering the data essential to bill for service requests. Moreover, accounting stands for record-keeping, monitoring, and tracing of client events on a computer network.

In an authentication and access control were introduced as a solution to the problem of unauthorized access in SDN models. The capability of an Open Flow-based SDN to aid access control to match services to identities could be involved as an SDN network security enhancement. An SDN-based authentication, authorization, and accounting system are introduced in to improve network security. In Table 2.6, a summary of the problems and the solutions proposed for each research work presented under Authentication, Authorization, and Accounting for Network Security Enhancements in SDN is conveyed.

Table 2.6 Research Works Based on Authentication, Authorization, and Accounting.

. eference	Problem	Solution
[50]	Reinforce network security by SDN-driven access control.	Provided Open Flow cantered controller with authentication.
[51]	To Provide robust, efficient security management for SDN experimental facilities.	Presented a certificate model that encloses authentication, authorization, and accounting for SDN experimental facilities.
[52]	Issue of unauthorized activities in SDN.	Offered a measurement system that assembles network traffic flow factors to detect unauthorized activities using machine learning.
[53]	Issue of sophisticated attack traffic and a large number of users accessing an unauthorized network resource.	Introduced robust entropy-based method to stop massive attack traffic flow in an SDN network.

V. CONCLUSION AND FUTURE SCOPE

We can conclude this paper by Applying SDN to improve performance, scalability of network is being widely used in industry for some years, for both wired and wireless connections. One of the challenges of SDN is to ensure the quality of service for various functions of network by resisting against intrusions, malicious attacks and liabilities, how to develop an authentication between a control plane and a data plane and how the sufficient security services can be provided in networks in future in an economic way.

ACKNOWLEDGMENT

Authors would like to welcome the reviewers comments and suggestions to carry out this research work. Authors would also like to thanks authorities of SSGBCOET College of engineering, Bhusawal for providing the research laboratory to carry out this research.

REFERENCES

[1] E.Lyczkowski,C.Sauer,N.Brödner,W.Kiess,and M.Schmidt,‘‘SDNcontrolledvisiblelightcommunicationclustersforAGVS,’’in*Proc.JointEur.Conf.Netw.Commun.6GSummit(EuCNC/6GSummit)*,2021, pp.154–159.

[2] R.Mohammadi,R.Javidan,M.Keshtgari,andN.Rikhtegar,‘‘SMOTE:Anintelligent SDN-based multi-objective traffic engineering technique for telesurgery,’’*IETEJ.Res.*,vol.0,pp.1–11,Mar.2021.

[3] W.Xia,J.Zhang,T.Q.S.Quek,S.Jin,andH.Zhu,‘‘MobileedgecloudbasedindustrialInternetofThings:ImprovingedgeintelligencewithhierarchicalSDNcontrollers,’’*IEEEVeh.Technol.Mag.*,vol.15, no.1,pp.36–45,Mar.2020.

[4] A.Yazdinejad,R.M.Parizi,A.Dehghantanha,Q.Zhang,andK.-K.-R.Choo,‘‘An energy efficient SDN controller architecture for IoT networkswith blockchainbasedsecurity,’’*IEEETrans.Services Comput.*, vol.13,no.4,pp.625–638,Jul.2020.

[5] D.V.Medhane,A.K.Sangaiah,M.S.Hossain,G.Muhammad,andJ.Wang,''Blockchainenableddistributedsecurityframework for next generation IoT:An edgecloudandsoftware-definednetwork-integrated approach, ''*IEEE InternetThingsJ.*,vol.7,no.7,pp.6143–6149, Jul.2020.

[6] A.Rahman,M.J.Islam,A.Montieri,M.K.Nasir,M.M.Reza,S.S.Band,A.Pescape,M.Hasan,M.Sookhak,andA.Mosavi,''SmartBlock-SDN:An optimized blockchain SDN framework for resourcemanagementinIoT,''*IEEEAccess*,vol.9, pp.28361–28376,2021

[7] P. T. Duy, H. D. Hoang, D. T. T. Hien, N. B.nh, and V.-H. Pham,''SDNLog-foren: Ensuring the integrity and tamper resistance of log files for SDN forensics using blockchain,'' in Proc. 6th NAFOSTED Conf. Inf. Comput. Sci. (NICS), Dec. 2019, pp. 416–421.

[8] Scott-Hayward, S., Natarajan, S., and Sezer, S. (2016). A Survey of Security in Software Defined Networks. IEEE Communications Surveys and Tutorials,18(1),623-654. https://doi.org/10.1109/COMST.2015.2453114

[9] Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., and Maglaris, V. (2013).Combining OpenFlow and sFlow for an effective and scalable Anomaly Detection and Mitigation mechanism on SDN Environments, Computer Networks

[10] Hand, R., Ton, M., and Keller, E. (2013) "Active Security," ACM SIGCOMM Hot Topics in Networks.Skowyra, R., Bahargam, S., and Bestavros, A.(2013). "SoftwareDefined IDS for Securing Embedded Mobile Devices,".[Online].

[11] Wang, Y., Zhang, Y., Singh, V., Lumezanu, C., and Jiang, G. (2013) "NetFuse: Short-circuiting traffic surges in the cloud,"IEEE International Conference on Communications (ICC). IEEE, pp. 3514–3518

[12] Zaalouk, A., Khondoker, R., Marx, R., and Bayarou, K. (2014). "OrchSec: An orchestrator-based architecture for enhancing network-security using Network Monitoring and SDN Control functions," Network Operations and Management Symposium (NOMS), IEEE. IEEE, 2014, pp. 1–9.

[13] Tantar, E., Palattella, M. R., Avanesov, T., Kantor, M., and Engel, T. (2014). Cognition: A Tool for Reinforcing Security in Software Defined Networks, ser. EVOLVE-A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation V. Springer, pp. 61–78

[14] Sangodoyin, A., Babagana, M., Irfan, A., Jules, P. D. (2018). An approach to detecting distributed denial of service attacks in software defined Networks. International Conference on Future Internet of Things and Cloud.DOI 10.1109/FiCloud.2018.00069. pp. 436 – 443.

[15] Jankowski, D. and Marek, A. (2016). On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks.International Journal of Electronics and Telecommunications. VOL. 62, No. 3, pp. 247 -252. DOI: 10.1515/eletel- 2016-0033.

[16] Muthamil, K. S. and Deepalakshm, P. (2020).A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 technique.Journal of High Speed Networks. No. 26, pp 55–76. DOI 10.3233/JHS-200630.

[17] Xing, T., Xiong, Z., Huang, D., and Medhi, D. (2014). "SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System in Clouds," pp. 308–311.

[18] Xing, T., Huang, D., Xu, L., Chung, C.J., and Khatkar, P. (2013)."Snortflow: Aopenflow-based intrusion prevention system in cloud environment," Research and Educational Experiment Workshop (GREE), 2013 Second GENI. IEEE, pp. 89–92.

[19] Shin, S., Yegneswaran, V., Porras, P., and Gu, G. (2013) ."AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks," Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security. ACM, pp. 413–424.

[20] Kampanakis, P., Perros, H., and Beyene, T. (2014). "SDN-based solutions for Moving Target Defense network protection," A World of Wireless,Mobile and Multimedia Networks (WoWMoM), 2014IEEE 15th International Symposiumon. IEEE, pp.1–6.

[21] Kaur, G. and Prinima, G. (2018).Proposed Optimization Technique to detect DDOS Attacks on Software Defined Networks.4th International

Conference on Computers and Management (ICCM).281-287.

[22] Nayak, A. K., Reimers, A., Feamster, N., and Clark, R. (2009).“Resonance: dynamic access control for enterprise networks,” Proceedings of the 1st ACM workshop on Research on enterprise networking. ACM, pp. 11–18.

[23] Shin, S., Yegneswaran, V., Porras, P., and Gu, G. (2013) .“AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks,” Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security. ACM, pp. 413–424.

[24] Ramachandran, A., Mundada, Y., Tariq, M. B., and Feamster, N. (2009). “Securing enterprise networks using traffic tainting,”.

[25] Jafarian, J. H., Al-Shaer, E., and Duan, Q. (2012). “Openflow random host mutation: transparent moving target defense using software defined networking, ”Proceedings of the first workshop on Hot topics in softwaredefined networks.ACM,pp.127–132.

[26] Jeong, C., Ha, T., Narantuya, J., Lim, H., and Kim, J. (2014).“Scalable network intrusion detection on virtual SDN environment,” in Cloud Networking (CloudNet), International Conference on.IEEE,pp. 264–265.

[27] Chung, C.J., Khatkar, P., Xing, T., Lee, J., and Huang, D. (2013). “NICE: Network intrusion detection and countermeasure selection in virtual network systems,” IEEE Transactions on Dependable and Secure Computing, p.1.

[28] Xing, T., Huang, D., Xu, L., Chung, C.J., and Khatkar, P. (2013).“Snortflow: Aopenflow-based intrusion prevention system in cloud environment,” Research and Educational Experiment Workshop (GREE), 2013 Second GENI. IEEE, pp. 89–92.

[29] Xing, T., Xiong, Z., Huang, D., and Medhi, D. (2014). “SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System in Clouds,” pp. 308–311.

[30] Manso, P., Jose, M. and Carlos, S. (2019). SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks.Information-Open Access Journal.10.106.1-17.

[31] Mehdi, S. A., Khalid, J., and Khayam, S. A. (2011). “Revisiting traffic anomaly detection using software defined networking,” Recent Advances in Intrusion Detection. Springer, pp.161–180.

[32] Dotcenko, S., Vladyko, A., and Letenko, I. (2014). “A fuzzy logic-based information security management for software-defined networks, ”Advanced Communication Technology (ICACT), 2014 16th International Conference on. IEEE, pp. 167–171.

[33] Braga, R., Mota, E., and Passito, A. (2010).“Lightweight DDoS flooding attack detection using NOX/OpenFlow,” IEEE 35th Conference on Local Computer Networks (LCN). IEEE, pp. 408–415.

[34] Lim, S., Ha, J., Kim, H., Kim, Y., and Yang, S. (2014). “A SDN-oriented DDoS blocking scheme for botnet-based attacks,” in Ubiquitous and Future Networks (ICUFN), InternationalConf on. IEEE,pp. 63–68.

[35] Suh, J., Choi, H., Yoon, W., You, T., Kwon, T., and Choi, Y. (2010).“Implementation of Content-oriented Networking Architecture (CONA): A Focus on DDoS Countermeasure,” European NetFPGA Developers Workshop

[36] Yu Hunag, C., MinChi, T., YaoTing, C., YuChieh, C., and YanRen, C. (2010).“A novel design for future on-demand service and security,” in Communication Technology (ICCT), IEEE International Conference on, pp. 385–388.

[37] Al-adaileh, M., A. A., Mohammed, A., Yung-Wey, C., and Ahmed, A. (2018). Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS). MATEC Web of Conferences.218,2012.https://doi.org/10.1051/matecconf/201821802012.

[38] Kaur, G. and Prinima, G. (2018).Proposed Optimization Technique to detect DDOS Attacks on Software Defined Networks.4th International Conference on Computers and Management (ICCM).281-287.

[39] Sooraj, V. H. and Prabhakar, K. (2019). SDN based Intrusion Detection System for OpenStack Cloud. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 8, 9, 2443-2449.

[40] Manso, P., Jose, M. and Carlos, S. (2019). SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks.Information-Open Access Journal.10.106.1-17.

[41] Kumar, S. D., Raihan, U. and Mahbubur, R. (2020).Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach.International Joint Conference on Computational Intelligence, Algorithms for Intelligent.pp.483 494.

[42] Ramkumar, M. P., Emil, S. and Bavani, K. (2020).Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined.International Conference on Advanced Computing & Communication Systems (ICACCS).No. 6.pp. 380 -385.

[43] Ahmad, F. A., Fatty, M. S., Ashraf, T. and Mohamed, H A. (2020). Performance Analysis and Evaluation of Software Defined Networking Controllers against Denial of Service Attacks. Journal of Physics: Conference Series.Conf. Ser. 1447 012007.

[44] Ajiya, A. A., Musa, A. B. and Aliyu, M. M. (2021). Solution Model for Intrusion Detection in Software Defined Networking (SDN) using Machine Learning. Quest Journals: Journal of Software Engineering and Simulation, Volume 7,Issue 8, pp: 40 -47.

[45] Scott-Hayward, S., Natarajan, S., and Sezer, S. (2016). A Survey of Security in Software Defined Networks. IEEE Communications SurveysandTutorials,18(1),623654.https://doi.org/10.1109/COMST.2015.2453114

[46] Shin, S. and Gu, G. (2012). "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," IEEE: International Conference on Network Protocols (ICNP). pp. 1 –6

[47] Fayazbakhsh, S. K., Chiang, L., Sekar, V., Yu, M., and J. Mogul, C. (2014)."Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags," in Proc. NSDI.

[48] Qazi, Z. A., Tu, C. C., Chiang, L., Miao, R., Sekar, V., and Yu, M. (2013)."SIMPLE-fyingMiddlebox Policy Enforcement Using SDN." ACM SIGCOMM.

[49] Chen, Y. J., Lin, F. Y., and Wang, L. C. (2014). "Dynamic Security Traversal in OpenFlow Networks with QoS Guarantee," International Journal of Science and Engineering, vol. 4, no. 2, pp. 251–256.

[50] Liu, X., Xue, H., Feng, X., and Dai, Y. (2011)."Design of the multi-level security network switch system which restricts covert channel," International Conference on Communication Software and Networks (ICCSN).IEEE, pp. 233–237

[51] Ballard,J.R., Rae,I., and Akella, A. (2010) "Extensible and scalable network monitoring usingOpenSAFE,"Proc.INM/WREN.

[52] Hirono, S., Yamaguchi, Y., Shimada, H., and Takakura, H. (2014)."Development of a secure traffic analysis system to trace maliciousactivitiesoninternal networks, "Computer Software and Applications Conference(COMPSAC),IEEE,pp.305–310.

[53] Bates, A., Butler, K., Haeberlen, A., Sherr , M. and Zhou, W. (2014). "Let SDN Be Your Eyes: Secure Forensics in Data Center Networks," Workshop on Security of Emerging Networking Technologies (SENT).

[54] Niyaz, Q., Weiqing, S. and Ahmad, Y. J. (2016). A Deep Learning Based DDoS Detection SysteminSoftwareDefinedNetworking(SDN).https://www.researchgate.net/publication/310671661.

[55] Toseef, U., Zaalouk, A., Rothe, T., Broadbent, M., and Pentikousis, K. (2014). "CBAS: Certificate-based AAA for SDN experimental facilities," European Workshop on Software Defined Networks (EWSDN). IEEE, pp.91–96.