

SDN based Network Security Challenges and Methods of Mitigation

Monica M. Jagtap¹ and Dr. S. Renuka Devi²

¹⁻²School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Chennai, Tamil Nadu - 632014, India

Email: monicajagtap01@gmail.com, renukadevi.s@vit.ac.in

Abstract—The software-defined network is one of the most important areas for future networking in 5G and next-generation networks (SDN). As a result of the SDN design, the conventional network is forced to be software-based, which boosts mobility, substantially automates workflows, and accelerates delivery. It is easier to manage and keep track of the network's resources with a centralized view of the entire network and dynamic SDN separation of the control plane from the network layer. The early SDN architecture misinterprets the security requirements due to its centralized control point, raising security vulnerabilities. This paper contributes to the advancement of both the scientific community and the industry by investigating the security and authentication processes used in SDN. Make a list of every security threat and SDN violation that is currently known. The study investigates the previously mentioned SDN security and authentication methods. The defense against attacker is challenging task. These challenges and security requirements in SDN are discussed. Future research directions will be determined based on the essential elements needed for the creation of algorithms for delivering security in SDN.

Index Terms— Authentication, SDN, Security, DDoS Detection.

I. INTRODUCTION

The huge requirements from consumers', such as data rate, accessibility help, bandwidth growth, delays are being satisfied by network operations. It would be hopeful if the fifth-generation (5 G) network could eventually satisfy these user needs. All networks such as Long Term Evolution (LTE) or 5G, should now include security as a fundamental function. Every network must have security.

The attack types such as IP spoofing and denial of service (DoS) or distributed denial of service (DDoS) have been used in attacks against 5 G networks. A DDoS assault is considered to be more disruptive in this case because it affects all three systems.

Other attacks will have an impact on any of these systems or any combination of these technologies. Information is everywhere, and this period of time in human history is referred to as the "Information Age." Since the Internet's inception in the 1960s, it has been used extensively by roughly 40% of the world's population, revolutionizing the economy through the growth of the communication and entertainment industries. This paper presents a study on several security concerns in Software Defined Networks (SDN) and approaches developed for authentication and DoS/DDoS attack detection.

II. LITERATURE REVIEW

A. SDN architecture and Security

The requirements of modern networking have been divided into seven areas by the Open Data Center Alliance (ODCA) On-demand scaling, model management, integrated security, mobility, flexibility, automation, and maintenance. Each of these goals is met by SDN, which is more open and flexible than proprietary solutions. In SDN configured environment data plane and control plane are on distinct devices. These two planes serve as the divisions of the switching function. The data plane is in charge of packet forwarding in this case. The data plane is composed of actual switches and virtual switches. By selecting the parameters for the priority and routing policies, creating routes, and adapting to changing traffic patterns the QoS and QoE requirements must be met, and it is the control plane's responsibility to do so. Open interfaces are used to enable communication between SDN controllers and networking applications and to guarantee a consistent user experience regardless of internal implementations. A physical server or a virtual server can be used to set up an SDN controller.

A few of the attacks on SDN that are mentioned in [1] include eavesdropping, distributed denial of service (DDoS), password-related attacks, identity spoofing, sniffer attacks, applications attacks, man in the middle (MITM) attacks, denial of service (DOS), sensitive data protection, and security into software.

Figure 1 illustrates how security issues might appear at any of the three layers as well as during interlayer communication. A system attack, such as a software or hardware attack, can occur at any layer of the SDN, as shown in Figure 1. Protocol attacks occur when the aero planes communicate with one another.

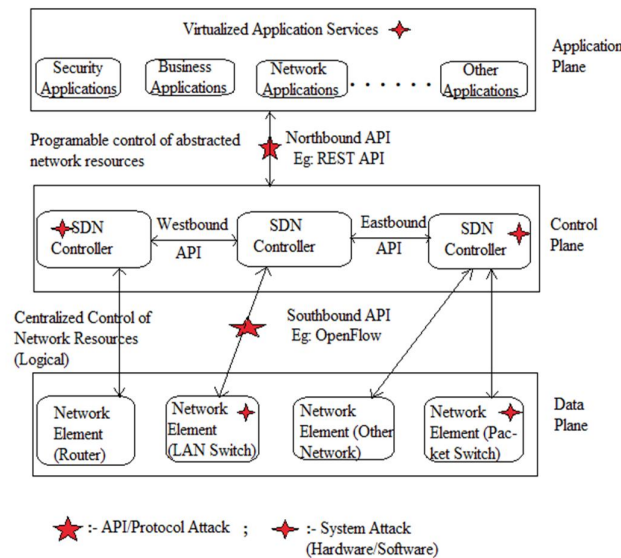


Figure 1: Security in SDN Networks

B. Classification of SDN Security

The links between SDN components may cause new security issues for existing networks. For instance, the Open Flow network does not mandate the use of a secure transport layer. Therefore, the peculiarities of the communication protocol could result in safety issues including DoS, fictional flow rules, and rule alterations. All three SDN planes—the data plane, control plane, and application plane—are under jeopardy. Applications flaws could endanger SDN controllers. There are variety of SDN controllers which includes Opendaylight, ONOS, and Floodlight. Additionally, there can be security vulnerabilities in the channels of communication between the three levels' southern (four) and northern APIs (5). Several of the target component attack vectors are thoroughly explained below:

Application Plane: Applications developed for SDN operations like orchestration, telemetry, and others might have security issues. In normal web applications, common issues of security that may arise incldes Cross-Site Scripting, are relevant to SDN due to the Cross-Site Request Forgery (CSRF) vulnerability (XSS). The network will be vulnerable to attacks because of the malicious/committed programs.

Control Plane: This control unit, which manages many protocols like OpenDaylight, POX, ONOS, and other plugins and applications, is made up of one or more controllers. The attacker will use the IP address to produce a lot of traffic and send it to the controller. The switch and controller will struggle to communicate as a result of this assault, which will lengthen network latency.

Data Plane: The attackers generate an imaginary scenario by cloning the Link Layer Discovery Protocol (LLDP) packets. Attackers utilizing specially created packets can also see the lag in communication with the control plane apps that correspond to the data plane apps. The main intension of this strategy is to locate the system logical controller. Switches are also used by attackers in similar fashion. Too many flood controls can cause the data flow control switch's memory to overflow because it is often restricted.

Communication Channels: A man in the middle (MITM) attack is performed by connecting managed devices between south bound and north bound APIs and switches. By monitoring host-to-host communication and gradually rerouting traffic between hosts the records are generated by authors for attacks monitoring. In order to determine whether a better SDN stage structure could help manage both internal and external security threats, some of the most significant SDN Threats Vectors (TVs) are examined in-depth in this section.

C. Threats in SDN

Fake Traffic Flows (threat Type 1): DoS attacks can be used to deactivate the switches by the attackers. In this type, switches may include the type TCAM (ternary content-addressable memory). The issue can be resolved with a straightforward authentication scheme, but if the attacker is successful in accessing the application server that houses client data, they can inject forged approved streams into the network using the same validated ports and source MAC addresses.

Switch Specific Vulnerabilities (threat Type 2): The switches used in the SDN environment could have problems. The SNMP MIB-II subagent daemon (mib2d) in Juniper OS is an illustration of this. It includes a vulnerability (CVE-2018-0019) that enables a remote attacker via a network to crash the mib2d function and subsequently in SNMP subsystem a denial of service (DoS) attack is performed. In an SDN setting, a switch can be used to restrict traffic, redirect network traffic for data collection, or create fictitious traffic needs in an effort to overburden the controller or other switches.

Control Plane Communication Attack (threat Type 3): TLS/SSL security is not applied to data transfers between the control and data planes. In an SDN setting, Public Key Infrastructure (PKI) is available, but the channel correspondence is not entirely secure. There are studies available on TLS/SSL security concerns. Through a weak Certificate Authority (CA) application, an attacker might gain access to the SDN's control plane channel. If there are constrained switches in control plane, such switches are targeted by attackers for DDoS attacks.

Controller Vulnerabilities (threat Type 4): In an SDN setup, the controller is the most crucial component. An unreliable controller has the power to bring down the entire network. For instance, in a remote denial of service attack (CVE-2015-7516), an older version of the SDN controller ONOS was targeted. The attacker can perform a switch disconnect and a NULL pointer dereference by sending the ONOS controller having version v1.5.0 using Ethernet outlines from the Jumbo Frame (0x8870) ether type. The specific set of circumstances that lead to a certain action or the question of whether it is risky or not cannot be answered by a combination of mark-based interruption location devices.

Between the management applications to the controller Trust (threat type 5): Applications on the executive's and controller's aircraft are lacking in a system to build trust. In the SDN scenario, there may be differences in the trust system between ordinary programs, endorsement creation, and trust confirmation between organizing devices.

D. Challenges in SDN Security

In addition to the indicated treat types in the paragraphs above, some security issues unique to SDN are not present in traditional networks. In this subsection, these security issues and appropriate practices are emphasized in an effort to prevent them in SDN.

1. Programmability: Thanks to SDN, customers from diverse industries and organizations can select among programmable options. Modern businesses have an organizational structure that mimics a closed domain. In a number of business and administrative domains, the SDN business model is necessary to protect system integrity, data from outside parties and open interfaces.

Isolation in Traffic and Resource: One program's corporate planning and real-time data must be totally segregated from other applications. Tenants must be given the assurance of traffic and resource isolation in the SDN scenario. Due to the SLA requirements and private addressing approach, fine-grain isolation can be obtained by complex interactions.

Third-party applications and controller trust factor: To lessen the controller's susceptibility, authorization and authentication at the application registration stage should be implemented.

2. Legacy Protocols and their integration facility: Some operational and technical issues with the conventional protocols were resolved with the introduction of SDN. However, it could be challenging to upgrade security measures for currently in use systems like DNS and BGP. Prior to incorporating the present protocols into SDN, it is critical to validate their functionality.

3. Cross-Domain Connection: Various physical servers, data centers and clusters are connected via SDN infrastructure. Each security domain may have one or more controllers in charge of it. A viable approach for developing trust between controllers must be provided by the SDN design. Abuse must be prevented by the confidence structure, which must also establish a secure channel.

E. DoS/DDoS Detection Methods

The DoS attack was discovered to be a weakness in SDN. To create an efficient and trustworthy DoS/DDoS security mechanism, a variety of methods were combined with traffic monitoring at the control layer and data layer programmability. Traffic data are introduced in each situation, depending on the network environment, to identify the DDoS intrusion using the chosen technique. The challenges and recommendations made for each research project addressed under the topic "DoS/DDoS Protection on Network Security Enhancements in SDN" are thoroughly explained in Table I.

TABLE I: DOS/DDOS DETECTION METHODS

Paper	Problem	Solution
[2]	DoS attack problem affecting SDN performance at the controller	Introduced an NID approach to bolster the DoS attack defences of SDN controllers.
[3]	SDN lacked a reliable system for identifying malicious traffic. The issue with utilising a single controller Problem with connected data in a dataset that is available	Proposed NIDS detection techniques based on machine learning. Introduced several controller mechanisms to deal with incoming packets that were new. Introduced feature selection techniques to a dataset that was prepared without duplication.
[4]	The Controller's DoS issues and performance flexibility	To recognize DDoS assaults against SDN controllers, correlation-based and entropy-based rules have been introduced.
[5]	DDoS assault detection problem	Presented how self-organizing maps can be used to classify traffic flow as either normal or malicious statistically.
[6]	To prevent Threat from overloading the SDN controller and targeting it	A method for classifying and identifying fraudulent network flow based on traffic statistics was presented.
[7]	Machine learning classifiers are ineffective at classifying DoS traffic redundancy	Utilized feature selection techniques before processing the data.
[8]	to solve the issue of botnet DDoS attack detection and blocking	Presented a DDoS blocking method for SDN-controlled network infrastructure.
[9]	Network performance issues brought on by DoS cyber attacks	Client-side implementation of a security system for an SDN architecture.
[10]	Traffic congestion issues at the controller	To prevent the incidence of DDoS assaults, mean entropy and the rate of percentage drop were introduced.
[11]	DoS attack detection and mitigation issues with OpenStack Cloud	An effective paradigm for safeguarding OpenStack cloud infrastructures is the newly announced firewall security mechanism.
[12]	issues with detecting and responding to DDoS attacks in content-oriented networks	To spot DDoS assaults, the frequency and pattern of content requests are analyzed.
[13]	The challenge of detecting and responding to DDoS attacks	Based on the capacity of the traffic flow, identify DDoS traffic using OpenFlow and drop it.

F. Authentication as a Step to Prevent Attacks

In the modern world, network managers put in a lot of effort to protect corporate networks, which frequently store significant data and resources. Sadly, despite the guidelines and safety measures implemented, these networks are nevertheless vulnerable to abuse, insider attacks, and inadvertent application flaws. Making sure that network connections are simple but uncontrolled is the responsibility of the Network Access Control. IEEE 802.1x standard technology describes a network access control system based on Ethernet ports. The IEEE 802.1x specification provides a technique for encapsulating communications using EAP (Extensible Authentication Protocol) sent across a LAN (Local Area Network).

This is termed as EAP over LAN (EAPOL). When network accessibility through switch port is required user credentials are essential. Direct network connections are not practical. The IEEE 802.1x EAP protocol provides

EAP-TLS, EAP-IKE MD5, EAP-V2 and other authentication methods. The source (host), authentication server and authenticator are the three components that make up the 802.1x standard specification. Figure 2 shows a typical authentication process.

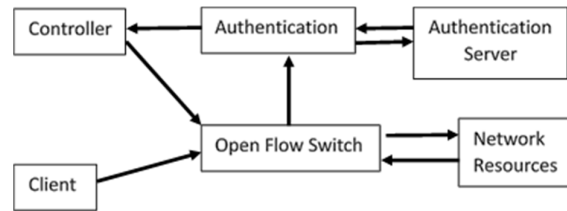


Figure 2: Typical Authentication Process in SDN open flow networks

G. Brief Discussion on various DoS/DDoS detection methods

With the emergence of SDN, a hierarchical authentication mechanism is offered by Xiao Liang et al. [14] for the IPv6 source address (SDN). This tool integrates the evaluation of the three entry organize, between space components and intra-area. Additionally, it can provide an extremely fine-grained level of security assurance for IPv6-capable devices.

In 5G HetNets based on SDN, Jin Cao et. al. [15] synchronization's of client capability and SDN process also offers a security assurance handover which is capacity-based verification mechanism. Our suggested method can greatly reduce the cost of verification handover while achieving critical understanding between BSs and User Equipment's (UEs) in 5G HetNet. Authors demonstrate that suggested method can provide a strong security guarantee through the use of a few security evaluation tools. The tools are used such as BAN and Scyther. Additionally, the evaluation results for the presentation demonstrate that our technique works better than other recent strategies.

For cloud radio over fibre and 5G, Hui Yang et al. [16] suggest a blockchain-based anonymous access (BAA) technique and a blockchain-based trustworthy authentication (BTA) concept. On an improved SDN testbed, the viability and productivity of using blockchain as support are evaluated.

A 5G heterogeneous network powered by software-defined radio (SDN) is provided with physical layer quick authentication by Ting Ma et al. [17]. (HetNet). Authors propose to implement the handover authentication in the plan using the Kolmogorov-Smirnov (K-S) theory test. The quick and efficient authentication is seen with the use of K-S method.

Cong Wang et al. [18] present an overview for a unique and successful authentication in SDN-based handover mechanism. This is for MEC in CPS. The SDN controller uses an authentication handover module (AHM) for key distribution and board confirmation. The AHM obtains a key from the active AP in order to get ready for an ECN handover. The one-time session key (OSK) is requested by AP, from the AHM during a handover. The shared authentication is achieved by the OSK-established three-way handshake procedure between AP and ECN. A potent enemy of attacking capability is validated by utilizing formal check via Internet security protocols and applications (AVISPA) automatic validation process. The simulation results demonstrate that the SHAS conspiracy has less computational postponement and utilizes less correspondence resources. The practical validation of our approach is completed by the widely used NS-3 replication.

The hidden authentication (HiAuth) method, developed by Osamah Ibrahim Abdullaziz et al. [19], safeguards the SDN controller. Bitwise operations are used by HiAuth which combines the characters from sender into the control packets. DoS attacks prevention by data covering is done firstly by company HiAuth in OpenFlow network. In two independent confirmation processes, HiAuth makes use of the exchange distinguishing proof field in OpenFlow and the IP ID field in IPv4. The test results demonstrate that HiAuth may significantly increase attacker imperceptibility while successfully reducing trespasser DoS attacks.

SDN Authentication and Attack Detection Methods with Machine Learning:

Managing the IoT devices is becoming difficult due to the enormous amount of data being generated. One of the major problems in the digital age is IoT security. IDSs have been developed utilizing a variety of approaches and strategies to defend and protect IoT networks [20]. As a response to numerous IoT-related challenges, an SDN-based IoT framework has recently been developed [21]. In SDN controller software programs manage the IoT devices [22–24]. The control related tasks and administration tasks are carried out in the underlying IoT network. These notable intrusion detection models were created recently to solve security issues in SDN-based networks.

Deng et al. [25] have described the many invasions that use the SDN-based IoT system. Authors also discussed detection and preventative measures. The accessibility, confidentiality, and integrity of IoT security have all

been studied by the writers. A research viewpoint is provided based on an evaluation of how various intrusion detection systems operate.

The principal component analysis and suppressed fuzzy logic for SDN-IoT intrusion detection have been introduced by Liu et al. [26]. There are two sorts of traffic. To comprehend the elements influencing the algorithms employed in the suggested strategy, simulated experiments are conducted. The experiment's findings show that the suggested IDS loses efficiency and accuracy as data volume increases.

The outcomes are superior to two other methods presented in the research, though. By combining SDN and machine learning, the IoTIDM model by Nobakht et al. [27] creates a network Intrusion detection system (IDS). IoT-IDM notifies the network devices of the attack. As a module for the SDN's lighting controller, IoT-IDM is being developed. For use with IoT networks in smart homes, IoT-IDM was developed. Hossien et al. developed a minimal Artificial Immune System (AIS)-based IDS for the Internet of Things. [28]. Three categories-cloud, fog, and edge-have been used by the authors to categorize the Internet of Things. In the cloud layer, training for detection is carried out. The concept of smart data is used in the fog segment's work on incursion notifications. The detectors are put into use on edge computing systems. Kalis is a knowledge-driven, self-adaptive intrusion detection system created by Midi et al. Kalis gathers network features before automatically customizing the detection method for the network. To accommodate IoT devices with limited resources, the suggested approach can also be implemented on a standalone device. For evaluation, the ICMP flood attack and Smurf attack are taken into consideration.

In their suggested IDS, Hassan et al. [30] used the Nave Bayes algorithm to categorize the traffic for intrusion detection. The Weka tool was employed by the authors to process assault data and other information. The device or the administrator receives notification of the attack.

An IDS for IoT that incorporates a more recent dataset and seeks to identify recent assaults was proposed by Kumar et al. [31]. According to the research, the suggested method outperforms several modern IDS and even guards against malicious internal attacks. An IDS for IoT based on SDN and with the use of machine learning is presented by authors in their earlier work [7]. The classifier makes use of the backward propagation technique. For the purpose of assessing how well the model works, the ICMP flood assault has been simulated.

Jagtap et al [33] used long shrt term memory (LSTM) and Grded rated Unit (GRU) for development of attack mitigation model. The model shown 96% efficiency for mitigating different types of DDoS attacks. The LSTM Fuzzy model is given in [34] by Mathus et al. the model uses fuzzy rules and LSTM model for attack mitigation which shows 88% efficiency. The deep learning based intrusion detection system is designed by Han et al [35]. The efficiency of model is seen around 89% for mitigating the DDoS attacks.

III. COMPARATIVE ANALYSIS

The comparative analysis is performed for various methods which make use of CIC2019 DDoS attack dataset [32].

TABLE II: COMPARATIVE OF DIFFERENT TECHNIQUES FOR THEIR CAPACITY TO DETECT ATTACKS

Paper	Method Used	Number of Stages	Types of DDoS Attacks Mitigated	Number of requests blocked	Update of model feasible?
Jagtap MM et al [33]	LSTM-RNN	2	7482	96%	Yes
Matheus et al [34]	LSTM-FUZZY	1	7466	88%	No
Han et al [35]	DL-IDS	1	7336	89%	No

A. Important points from study

1. Authentication can be the first step towards selective access for the services provided which may prevent introduction of malicious node in the network.
2. The SDN platform has wide range of risks associated during services allocation in which server has to perform various tasks to provide responses to the requests.
3. The request based DDoS attacks is the important factor of concern in which variety of attack types can be observed. (e.g. dataset [32])
4. The attack records based on packet in depth analysis can be used for machine learning based algorithm development for SDN security.

5. The machine learning conventional classifiers such as Support vector machine, naïve bays, decision tree, artificial neural network, random forest can be used for classification. The feature extraction in conventional methods will be dependent on hand crafted methods.
6. The deep learning based dense network have shown better results especially use of RNNs. The LSTM and GRU combinations show improvement in results.

IV. CONCLUSION

The advancement in network technology these days make use of software defined networks (SDN). Though SDN has variety of advantages, the SDN platform is exposed to a wide range of risks, some of which are brought on by authorization and authentication weak processes and others which are brought on by the SDN design. In SDN, one attack vector must be the only focus of the construction of a secure cloud networking architecture. The security concerns affecting SDN's dependability, availability, and security were the main emphasis of the study presented in this paper.

The goals of the security design and security countermeasures have been extensively discussed for OpenFlow protocol and for the SDN data and control plane. The controlled architectural configuration is also dependent on a number of other parameters, such as the effects of a certain secured configuration on throughput and latency, in addition to the techniques detailed in this section. But since they are outside the purview of this study, they must be considered before the survey's recommendations are put into practice.

REFERENCES

- [1] C. Bouras, A. Kollia and A. Papazois, "Teaching network security in mobile 5G using ONOS SDN controller," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017, pp. 465-470, doi: 10.1109/ICUFN.2017.7993828.
- [2] 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.
- [3] 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.
- [4] 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, 02012.<https://doi.org/10.1051/mateconf/201821802012>.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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), International Conference on. IEEE, pp. 63–68.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] Xiao Liang ; Heyao Chen "A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address" 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) Year: 2019 | Conference Paper | Publisher: IEEE.
- [15] Jin Cao ; Maode Ma ; Yulong Fu ; Hui Li ; Yinghui Zhang "CPPHA: Capability-based Privacy-Protection Handover Authentication Mechanism for SDN-based 5G HetNets" IEEE Transactions on Dependable and Secure Computing Year: 2019 | Early Access Article | Publisher: IEEE.

- [16] Hui Yang ; Haowei Zheng ; Jie Zhang ; Yizhen Wu ; Young Lee ; Yuefeng Ji “Blockchain-based trusted authentication in cloud radio over fiber network for 5G” 2017 16th International Conference on Optical Communications and Networks (ICOON) Year: 2017 | Conference Paper | Publisher: IEEE.
- [17] Ting Ma ; Feng Hu ; Maode Ma “Fast and efficient physical layer authentication for 5G HetNet handover” 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) Year: 2017 | Conference Paper | Publisher: IEEE.
- [18] Cong Wang ; Yiying Zhang ; Xi Chen ; Kun Liang ; Zhiwei Wang “SDN-Based Handover Authentication Scheme for Mobile Edge Computing in Cyber-Physical Systems” IEEE Internet of Things Journal Year: 2019 | Volume: 6, Issue: 5 | Journal Article | Publisher: IEEE.
- [19] Osamah Ibrahim Abdullaziz ; Li-Chun Wang ; Yu-Jia Chen “HiAuth: Hidden Authentication for Protecting Software Defined Networks” IEEE Transactions on Network and Service Management Year: 2019 | Volume: 16, Issue: 2 | Journal Article | Publisher: IEEE.
- [20] Lu, Y., Da Xu, L.: Internet of things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. 6(2), 2103–2115 (2019)
- [21] 14. Azka., Revathi, S., Geetha.: A survey of applications and security issues in software defined networking. Int J of Comput Netw and Inform Secur. 9(3), 21–28 (2017)
- [22] Li, J., Altman, E., Touati, C.: A General SDN-based IoT Framework with NVF Implementation. ZTE Communications, ZTE Corporation, 13, pp. 342–45. HAL (2015)
- [23] Vilalta, R., et al.: End-to-End SDN Orchestration of IoT Services Using an SDN/NFV-enabled edge node. In: Optical fiber Conference and Exhibition (OFC), pp. 7–9. (2016)
- [24] Kalkan, K., Zeadally, S.: Securing internet of things with software defined networking. IEEE Communications Magazine, vol. 56(9), pp. 186–192 (2018). <https://doi.org/10.1109/mcom.2017.1700714>
- [25] Deng, L., et al.: Mobile network intrusion detection for IoT system based on transfer learning algorithm. Cluster Comput. 1–16. (2018)
- [26] Liu, L., et al.: An intrusion detection method for internet of things based on suppressed fuzzy clustering: EURASIP J. on Wirel Comm. and Netw. 2018(1), (2018). <http://doi.org/10.1186/s13638-018-1128-z>
- [27] Nobakht, M., Sivaraman, V., Boreli, R.: A host-based intrusion detection and mitigation framework for smart home IoT using openflow. 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, pp. 47–156 (2016)
- [28] Hosseinpour, A., et al.: An intrusion detection System for fog computing and IoT based logistic systems using a smart data approach an intrusion. Int J Dig Content Technol Appl. 10(5), 34–46 (2016)
- [29] Midi, D., et al.: Kalis – A system for knowledge-driven adaptable intrusion detection for the internet of things. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, pp. 656–666. (2017)
- [30] Hassan, S., Houbing, A., Malik, K.M.: NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. J Supercomput, 74(10), 5156–5170 (2018)
- [31] Kumar, V., Das, A.K., Sinha, D.: UIDS: A unified intrusion detection system for IoT environment. Evol. Intell. 0123456789 (2019).
- [32] Dataset for DDoS algorithm development: <https://www.unb.ca/cic/datasets/index.html>
- [33] Jagtap, MM, Saravanan, RD. Intelligent software defined networking: Long short term memory-graded rated unit enabled block-attack model to tackle distributed denial of service attacks. Trans Emerging Tel Tech. 2022;e4594. doi:10.1002/ett.4594
- [34] Matheus P. Novaes, Luiz F. Carvalho, Jaime Lloret and Mario Lemes Proenca Jr., “Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment”, IEEEAccess volume 8, 2020, 10.1109/ACCESS.2020.299204
- [35] Tsung-Han Lee, Lin-Huang Chang and Chao-Wei Syu, “Deep Learning enabled Intrusion Detection and Prevention System over SDN Networks”, 2020 IEEE International Conference on Communications Workshops (ICC Workshops).