DEFENSE AGAINST SOFTWARE-DEFINED NETWORK TOPOLOGY POISONING ATTACKS

Sadiya Sultana[1], Sara Begum[2], Asfia Jabeen[3] , Dr. Syed Asadullah Hussaini[4]
[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.
[4]Associate Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

Abstract: Software-Defined Network (SDN) represents a new network paradigm. Unlike conventional networks, SDNs separate control planes and data planes. The function of a data plane is enabled using switches, whereas that of a control plane is facilitated by a controller. The controller learns network topologies and makes traffic forwarding decisions. However, some serious vulnerabilities are gradually exposed in the topology management services of current SDN controller designs. These vulnerabilities mainly exist in host tracking and link discovery services. Attackers can exploit these weak points to poison the network topology information in SDN controllers. In this study, a novel solution is proposed to defend against topology poisoning attacks. By analyzing the existing topology attack principles and threat models, this work constructs legal conditions for host migration to detect host hijacking attacks. The checking of the Link Layer Discovery Protocol (LLDP) source and integrity is designed to defend against link fabrication attacks. A relay-type link fabrication attack detection method based on entropy is also designed. Results show that the proposed solution can effectively detect existing topological attacks and provide complete and comprehensive topological security protection.

INTRODUCTION

Software-defined networks (SDNs), which were first introduced in the campus network of Stanford University, were designed to address the issues of complexity and inefficiency that are often seen in conventional networks. SDNs enable the realization of centralized control and distributed forwarding in networks by separating the data forwarding and routing control that is often found in the conventional Internet. Programming takes the shape of an interface that connects with the external environment. The dynamic and adaptable nature of Software-Defined Networks (SDNs) has garnered significant interest from both academic and industrial sectors. Researchers across several disciplines extensively use Software-Defined Networks (SDNs) to develop novel solutions for addressing issues such the constrained scalability of conventional topologies, wireless sensor networks, the Internet of Things, and optical networks. The current research on the security of the SDN topology discovery mechanism primarily focus on three key areas: development of a robust security framework, implementation of a new protocol, and incorporation of encryption authentication. TopoGuard is a security add-on for the SDN controller that identifies and addresses security weaknesses in the controller, namely by detecting attacks on the SDN network topology view. Unfortunately, TopoGuard lacks the capability to identify switch-based link fabrication attacks. PolicyTopo presents a way for determining the state of a connection by analyzing the information entropy of the network latency. Topology attacks are characterized by their occurrence when the network latency is minimal. PolicyTopo identifies assaults using secure ports when there is a significant increase in network latency. A drawback of this approach is that the state relies only on the linear correlation between neighboring entropy levels, and the inclusion of secure ports adds additional strain to the

network. The suggested defensive system in the reference relies on a statistical analysis of link delays to identify relay-type link fabrication assaults. However, this technique may be circumvented by altering the timestamp of the Link Layer Discovery Protocol (LLDP) packet. Azzouni et al. enhanced the topology discovery approach by devising a novel protocol, which resulted in decreased workload for the controller, as well as enhanced efficiency and safety. Nevertheless, as the "open-flow discovery protocol" matures, the introduction of a new protocol is certain to impact network deployment, application, standardization, and other related areas. The current research in the domain of SDN topology security has made advancements, but, most studies focus on specific security threats, resulting in a lack of comprehensive protection strategies. During implementation, it may be necessary to modify or augment current methods with additional security solutions. As a result, the process of system integration becomes notably challenging. Furthermore, the effectiveness of security mechanisms against relay type topology assaults is strongly dependent on the LLDP frame delay threshold. However, this threshold may lose its validity in situations when network latency is significant. Building upon previous research findings, this study presents an innovative approach to address the security issues that arise during the topology discovery process of Software-Defined Networks (SDNs). This study aims to identify instances of host hijacking assaults by formulating legitimate criteria for host migrations. Additionally, it proposes the implementation of source and integrity verification mechanisms for LLDP frames to mitigate the risk of link fabrication attacks. Next, a strategy for detecting relay-type link fabrication attacks is suggested, which is based on entropy. This technique utilizes the LLDP frame transmission threshold and entropy threshold to identify and detect irregularities or abnormalities in a network. The SDN simulation environment for the design experiment is constructed using the Mini net and Floodlight controllers. The findings demonstrate that the suggested technique provides efficient protection against common topology assaults and full security for topology.

LITERATURE SURVEY

The paper titled "Fog computing and its role in the internet of things" is authored by F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. The year is 2012. Fog computing expands the Cloud Computing concept to the network's edge, allowing for the development of novel applications and services. The Fog is characterized by many key features: a) It offers low latency and location awareness; b) It has a wide geographical distribution; c) It supports mobility; d) It consists of a very high number of nodes; e) It primarily relies on wireless connectivity; f) It is heavily used for streaming and real-time applications; g) It exhibits heterogeneity. This study asserts that the Fog is the suitable foundation for many crucial Internet of Things (IoT) services and applications, including Connected Vehicle, Smart Grid, Smart Cities, and Wireless Sensors and Actuators Networks (WSANs).

The paper titled "Micro services scheduling model over heterogeneous cloud-edge environments as support for IoT applications" was authored by I.-D. Filip, F. Pop, C. Serbanescu, and C. Choi. The year is 2018.Driven by the strong need to enhance the use of specialized devices for achieving computational goals at a lower cost, we provide a novel framework for organizing microservices across diverse cloud-edge contexts. Our model employs a specific mathematical formulation to describe an architecture that encompasses diverse machines capable of handling various microservices. Due to the need for an early risk analysis of the solution in every new model, we enhanced the Clouds simulation framework to accommodate an experiment that incorporates

such a system. This study examines two instances of practical applications of our suggested scheduling system. To provide an unbiased evaluation of the first example, we have included experimental findings obtained from the simulation tool that was created. Based on our analysis of the experimental data, we discovered that some basic scheduling algorithms may outperform others in certain scenarios often seen in cloud-edge settings when using a micro service-oriented approach..

The paper titled "Design and performance evaluation of containerized microservices on edge gateway in mobile IoT" was authored by A. S. Gaur, J. Budakoti, and C.-H. Lung.The year is 2018. on recent times, the concept of Internet of Things (IoT) has gained significant attention and is being anticipated to have a significant impact on several industries in the next years, owing to its potential advantages. Nevertheless, the continuous and fast expansion of IoT devices also presents novel obstacles stemming from limited power and resources linked to them. One of the difficulties is in ensuring uninterrupted connection in mobile IoT. Furthermore, IoT devices have the capability to transmit a vast volume of data. Therefore, it is essential to develop a solution that can efficiently minimize the expenses associated with transferring this data. There are difficulties in managing and deploying services that operate on mobile IoT Edge Gateway. Containerized virtualization solutions may be important in efficiently managing and deploying microservices to ensure smooth communication. This article presents a lightweight container-based virtualization technique for the Internet of Things (IoT). It utilizes a Docker container-based microservices architecture to efficiently deploy applications in a virtualized environment. We assessed the efficacy of the suggested method on an actual IoT testbed, using Raspberry Pi 3 as a mobile IoT Edge Gateway for determining network handover among several options, including Wi-Fi, Radio, and Satellite. The findings showed superior performance in comparison to the native environment, namely the one that did not have a virtualization layer. The findings also indicated that the Docker container incurs little resource overhead and may be used on mobile IoT Edge Gateway devices with limited resources, such as the Raspberry Pi 3, to effectively manage IoT applications and services.

The paper titled "Dyme: Dynamic microservice scheduling in edge computing enabled IoT" was authored by A. Samanta and J. Tang in 2020. The fast advancement of mobile edge computing (MEC) in recent years has offered a very effective execution platform at the edge for Internet-of-Things (IoT) applications. However, the MEC also offers appropriate resources to various microservices. Nonetheless, the execution process in MEC is intrinsically influenced by underlying network circumstances and infrastructures. Hence, when faced with fluctuating network circumstances, it is crucial to efficiently carry out the tasks of end users while optimizing energy efficiency on the edge platform, all while ensuring equitable Quality-of-Service (QoS). However, it is essential to dynamically schedule the microservices in order to reduce both the overall network latency and network cost. In this paper, we provide a novel and dynamic microservice scheduling system for Mobile Edge Computing (MEC), which distinguishes itself from previous research. We theoretically build the micro service scheduling framework and analyze the computing cost of the scheduling method. The extensive simulation findings demonstrate that the micro service scheduling framework greatly enhances performance indicators such as total network latency, average price, satisfaction level, energy consumption rate (ECR), failure rate, and network throughput compared to other current baselines.

The paper titled "Secure edge computing management based on independent micro services providers for gateway centric IoT networks" was authored by W. Jin, R. Xu, T. You, Y.-G. Hong, and D. Kim in 2020. Edge

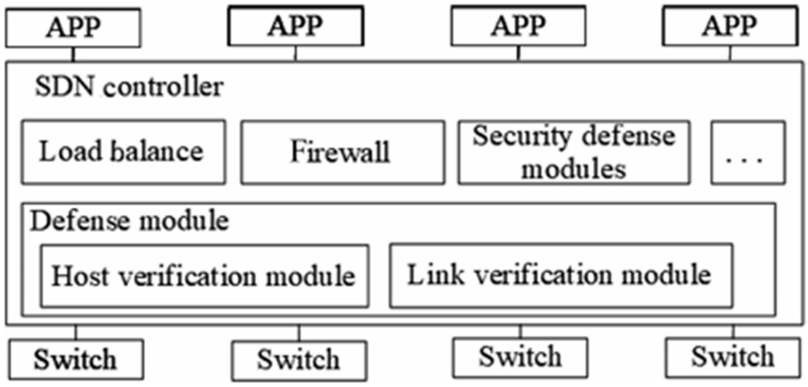
computing is a developing computing model that decentralizes computational power to the periphery of networks, allowing for computation to occur in close proximity to the environment where sensors and actuators are installed. Thus, the Internet may be equipped with many solutions that are tailored to its needs, thanks to the considerable computer power available at the network edge. However, devices at the network edge have limitations in terms of computational and networking resources. Delivering secure services using edge computing is a difficulty due to limited resources. This article presents a proposal for a secure edge computing system that manages devices, data, users, and extra services. The system is built on deploying independent microservice providers together with a security gateway on an edge gateway. The edge gateway serves as the central point of a local network, where several IoT devices are installed to interact with the physical environment for the purpose of detecting and actuating. The gateway facilitates the administration capabilities via microservices that rely on many autonomous server modules. Each local network that is centered on a gateway has its own independent management service that is built upon the gateway. In order to offer secure edge computing services via the edge gateway, a security gateway is installed on the proposed edge gateway. This security gateway utilizes Representational State Transfer Application Programming Interfaces to make the security services accessible to the Internet, rather than relying on microservices from management modules.

The paper titled "Docker enabled virtualized nano services for local IoT edge networks" was authored by J. Islam, E. Harjula, T. Kumar, P. Karhula, and M. Ylianttila in 2019.
The following subjects are covered: 3G mobile communication; 5G mobile communication; telecommunication traffic; Internet of Things; quality of service; telecommunication network dependability; virtualization; telecommunication security; Long Term Evolution; cellular radio.

PROPOSED SYSTEM

This paper introduces a new approach to protect against topology poisoning attacks. This study establishes legal criteria for host migration to identify host hijacking assaults by examining the current principles of topological attacks and threat models. The purpose of verifying the source and integrity of the Link Layer Discovery Protocol (LLDP) is to protect against link fabrication attacks. Additionally, a technique for detecting relay-type link fabrication attacks is developed, using entropy as a basis. The results demonstrate that the suggested approach is capable of accurately identifying and mitigating topological assaults, ensuring thorough and comprehensive protection for network topology. Next, a strategy for detecting relay-type link fabrication attacks is suggested, which is based on entropy. This technique utilizes the LLDP frame transmission threshold and entropy threshold to identify and identify irregularities in the network. The SDN simulation environment for the design experiment is constructed using the Mininet and Floodlight controllers. The findings indicate that the suggested method provides a robust defense against common topological assaults and full security protection for network topology.

SYSTEM ARCHITECTURE



EXPLANATION

In this project, the data owner is required to register all the necessary information and thereafter log in. The data owner has the ability to upload a document. The data owner may initiate a request to deliver data to the data user. The user has the ability to search for a specific query using an uploaded document. The package also includes a download option that will display an encryption format. The data user also sends a request to the cloud server. A cloud server may be accessed with a login. The system will validate a provided key. Cloud servers have the ability to access and see all data information. The cloud server has the ability to access and see all user information. A cloud server has the ability to access and see all of the stored information. A cloud server has the capability to authorize a user's request for a key. Once the data owner receives the request, they may provide the user with a confidential key. Additionally, the user has the option to download a file. If the user provides incorrect keys, they will get a warning and their account will be permanently blocked. The file is subjected to assaults.

TYPES OF TESTS

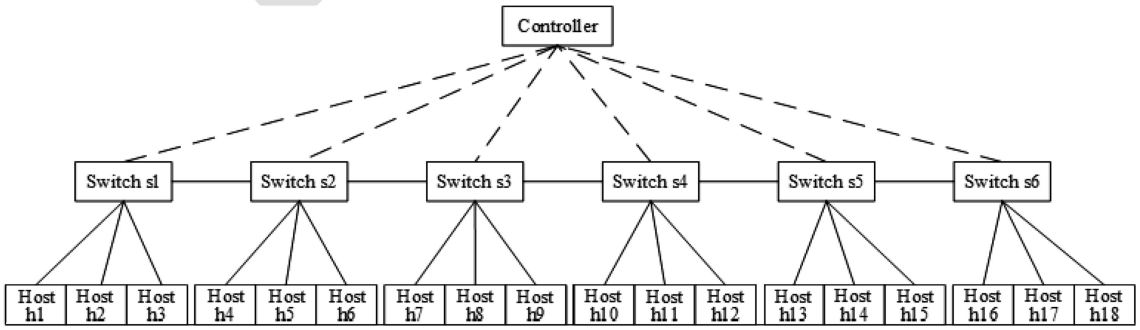


Fig. Test topology

Sl. No	Test scenario	User action	Expected result	Actual Result	Remarks
1.	Registration	Users registering into the system.	Register into the system.	Successfully alert registered message.	Pass
2.	Login	1. Entered correct password.	1. Log into the system. 2. Alert generated.	1. Successfully logged in. 2. Successfully generated the alert.	Pass
3.	Data User	Search File, Gets the requests from owner	Massages sending data user alert is generated.	Successfully generated the alert and massages sending	Successful
4.	Data Owner	Upload a Files and send request for user	Data owner has to actions	Successfully generated the alert to data owner message	Successful
4.	Cloud Server	Data owner information, data user information, files,keys and attack details	Massages Alert is generated	Successfully generated the alert for cloud server massages	Successful

RESULTS

Based on the experimental findings, the occurrence of false positives is significantly increased when the threshold is set at 1 and 2. Simultaneously, the threshold decreases to less than 50% when the threshold reaches 3. When the threshold is increased to 5, the false positive rate becomes 0. Raising the threshold leads to a reduction in the false positive rate and an increase in the time it takes to detect. To summarize, we established the threshold at 3. Ultimately, the efficacy of the defense is confirmed. The empirical findings are shown.

Table: Impact of abnormal queue counter threshold on false positive rate and detection time.

S.No	False positive rate (%)	Average detection time (s)
1	64	2.6
2	62	5.2
3	38	7.8
4	18	10.1
5	0	11.6
6	0	14.3

CONCLUSION

To solve the security problem in which the global topology view in the SDN controller is easily tampered with by attackers, this study designs a security solution. First, the existing principles and threat models of topology attacks are analyzed, and the legal condition detection for host migration is constructed to defend against host hijacking attacks. Second, LLDP source check and integrity check are designed to defend against link fabrication attacks. Third, a relay-type link fabrication attack detection method based on entropy calculation is defined to construct LLDP frames. Finally, an SDN simulation environment is built through the Mininet and Floodlight controllers. The results verify the effectiveness of our solution against mainstream topology attacks and indicate its capability of providing complete and comprehensive topology security protection.

FUTURE ENHANCEMENT

In the future, the results verify the effectiveness of our solution against mainstream topology attacks and indicate its capability of providing complete and comprehensive topology security protection.

References:

1. Yang Gao and Mingdi Xu_Defense Against Software-Defined Network Topology Poisoning Attacks, TSINGHUA SCIENCE AND TECHNOLOGY, ISSN 1007-0214 04/18 pp39–46, Volume 28, Number 1, February 2023
2. N. McKeown,T.Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, OpenFlow: Enabling innovation in campus networks, ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008.
3. X. Mingdi and G. Yang, Distributed deception defense system based on SDN, (in Chinese), J. Commun., vol. 39, no. S2, pp. 54–60, 2018.
4. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023

5. Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*", Journal of Sensor, Volume2023.
6. Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*", Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).
7. Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*", Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)
8. Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies", Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022
9. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
10. Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021
11. M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*", in 3rd International Conference ICCIDM, Springer - 978-981-10-3874-7_3 Dec (2016)
12. Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017
13. Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022
14. Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7
15. Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
16. Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
17. Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
18. Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.

19. Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.
20. Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017
21. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;
22. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
23. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021
24. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
25. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
26. .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011
27. Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253
28. Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)
29. Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)
30. Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486
31. Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016

32. Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)
33. Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)