JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DEFENSIVE AGAINST SOFTWARE - DEFINED NETWORK TOPOLOGY POISIONING ATTACKS

[1]P.Srinivasu, [2] P. Padma Chandrika, [3]N. Harshitha, [4]S. Sivasankara Rao
[1,2,3]UG Scholars, [4]Associate Professor
[1,2,3,4]Department of Computer Science and Engineering,
Guru Nanak Institutions & Technical Campus (Autonomous), Hyderabad, India.

Abstract: The Software-Defined Network (SDN) is a novel network paradigm in this study. SDNs divide control and data planes, in contrast to traditional networks. Whereas a controller facilitates the function of a control plane, switches enable the function of a data plane. The controller decides on traffic routing and gains knowledge about network topologies. However, a number of significant flaws in the topology management functions of the SDN controller designs currently in use are increasingly becoming apparent. The majority of these vulnerabilities are found in link discovery and host tracking services. Attackers may contaminate the network topology data in SDN controllers by taking advantage of these vulnerabilities. This paper presents a unique countermeasure against topological poisoning assaults. This paper creates legal frameworks for topology attack concepts and threat models by examining the current. Additionally, an entropy-based relay-type link fabrication attack detection mechanism is devised. The suggested approach may successfully identify current topological assaults and offer full and comprehensive topological security protection, according to the results.

IndexTerms **– SDN Security, Traffic analysis, Encryption techniques, Secure communication protocols, Packet filtering, Network Virtualization, software defined network and SDN Architecture.**

I. INTRODUCTION

Protecting contemporary network infrastructures from software-defined network (SDN) poisoning threats is essential. Administrators can centrally control network resources and effectively adjust to shifting demands thanks to the dynamic and flexible network management capabilities provided by SDN environments. But this adaptability also poses new security risks, especially when it comes to the reliability and integrity of network control.

Attacks against SDN infrastructures that target the control plane are referred to as SDN poisoning attacks or control plane attacks. By breaking into the SDN controller or inserting malicious commands into the network's control logic, they hope to alter the flow of network traffic. Serious repercussions from such assaults may include data exfiltration, unauthorized access, service interruptions and even network wide-outages.

LITERATURE REVIEW

One of the without a doubt, the following is an organized assessment of the literature on countermeasures against software-defined network (SDN) poisoning attacks.

Overview of SDN and Poisoning Attacks: By separating the control plane from the data plane, SDN allows for centralized control and programmability, hence bringing about a paradigm shift in network administration. But this architectural

modification also brings with it new security risks, such as the possibility of poisoning attacks. Attackers using SDN poisoning attempt to infiltrate malicious flow rules, alter flow tables, breach the control plane, and interfere with network functions.
Technologies & defensive techniques and SDN controller for security.

Karim F. Khan et al.'s "Securing Software-Defined Networks: A Survey" (IEEE Communications Surveys & Tutorials, 2017) offers a thorough analysis of the security issues with SDNs and covers methods for protecting SDN controllers, including role-based access control, secure communication protocols, and controller software integrity verification.

II.RESEARCH METHODOLOGY

The study suggests a method for detecting risk index in older persons that makes use of the newest machine learning algorithms. The complete architecture diagram is shown as

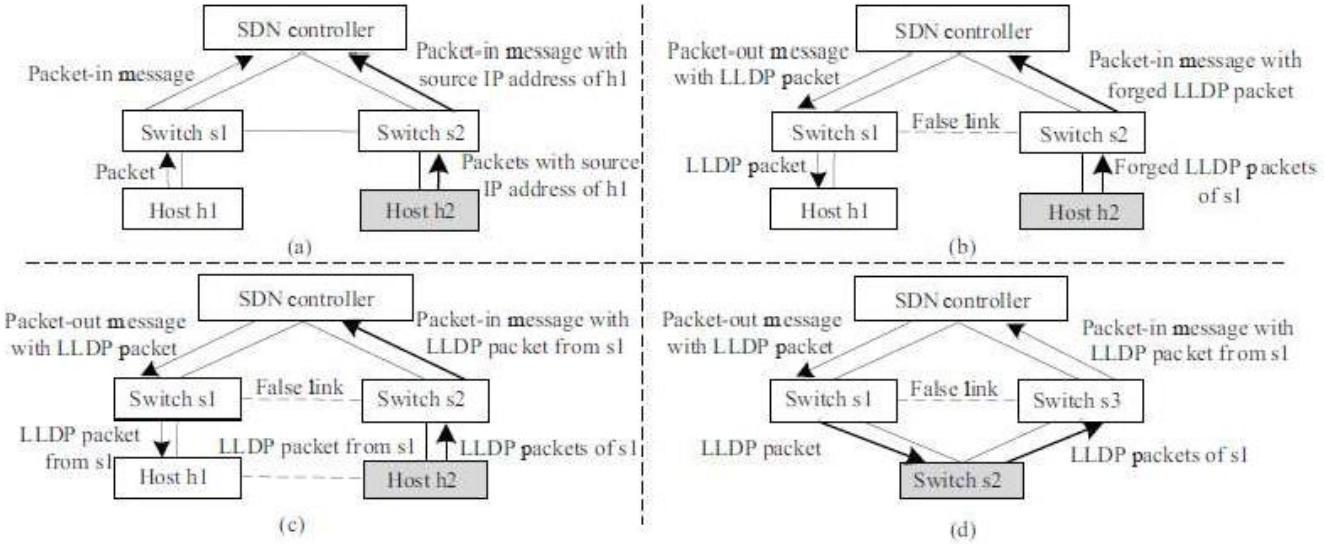

Fig (a): Our datasets are sourced from the google website, which offers datasets.

III.TECHNIQUES USED OR ALGORITHMS USED

3.1 EXISTING SYSTEM -

The literature analysis were proposed to solve the bloated and inefficient problems of traditional networks. Through the separation of the data forwarding and routing control of the traditional Internet in SDNs, the centralized control and distributed forwarding of these networks can be realized.Researchers in many fields actively use SDN's to build new systems for solving problems, such as the limited scalability of traditional architectures, wireless sensor networks.SDN controller is responsible for managing the network and communicating with the network devices.

DRAWBACKS:

- SDN controller designs
- Existing topology attack principles

3.2PROPOSED SYSTEM

The suggested study presents a In a local area network built on IEEE 802 technology, mostly wired Ethernet, network devices advertise their identity, capabilities, and neighbours through the usage of Link Layer Discovery Protocol (LLDP), a vendor-neutral link layer protocol.LLDP can be used to find nearby devices, tell nearby devices about their layer-2 setups, and troubleshoot and resolve problems with ease. Using the CPRF technique, a new feature set is developed with the goal of improving network attack detection performance. In our last talk, we look at the security issues with decentralized storage networks and propose future research areas and possible fixes.

ADVANTAGES:

- Decentralized storage networks
- Checking of link layer discovery protocol

From the plotting of Logistic Regression algorithm, we get the following figure:

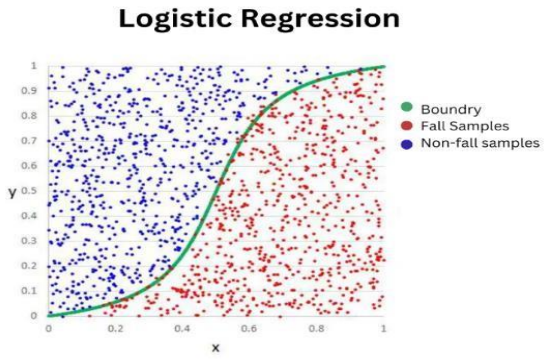

Fig (b) : Logistic Regression

IV.IMPLEMENTATION

Putting in place a strong defense against software-defined network (SDN) poisoning threats requires a multipronged strategy that takes into account different technologies, protocols, and industry best practices. Securing the SDN controller, which acts as the network management system's central command center, is one important component. Strong access control measures, such multi-factor authentication (MFA) and role-based access control (RBAC), can be used to assist prevent unwanted access to the controller. Furthermore, utilizing secure communication protocols like Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) guarantees that control messages sent back and forth between network devices and the controller are encrypted and shielded from manipulation or surveillance.

Among the other essential components of defensive implementation is SDN switch flow table protection. Organizations can stop hostile actors from injecting unapproved flow rules or changing already-existing ones in order to interrupt network traffic or carry out poisoning attacks by verifying and safeguarding flow tables. The integrity and reliability of flow management in SDN systems are improved by methods like flow rule validation, flow table encryption, and flow entry authentication. Additionally, detecting and thwarting abnormal activity that can point to SDN poisoning attacks requires the implementation of anomaly detection systems and intrusion protection systems. To identify anomalies in network behaviour, such as strange traffic patterns, unexpected protocol usage, or anomalous flow lengths, one can utilize machine learning algorithms, statistical analysis, and behavioural analysis approaches. Systems for preventing intrusions (IPS) can take automated actions such as block malicious traffic or triggering laerts for further investigation.

Defence implementation against SDN poisoning assaults also heavily relies on real-time response capabilities and ongoing monitoring. Security teams may quickly identify and address such risks thanks to visibility into network traffic provided by tools like packet sniffers, flow analysis software, and network monitoring systems. Threat intelligence feeds, forensic analysis tools, and incident response plans all help in evaluating the effects of attacks, figuring out their underlying causes, and putting preventative measures in place to stop them from happening again.

To effectively protect SDN environments against poisoning attacks, a comprehensive defensive approach should include secure access control, encryption protocols, flow table protection, anomaly detection, intrusion prevention, continuous monitoring, and incident response capabilities. Upholding a robust security posture and reducing new risks in dynamic networks also benefits from regular security evaluations, upgrades, and training initiatives

V. RESULTS :

Software-defined networking (SDN) topology poisoning attacks pose serious threats to network security and integrity. These attacks exploit vulnerabilities in SDN infrastructures, enabling attackers to manipulate network topology for malicious purposes. As a result, they can disrupt network services, leading to service outages or degradation of performance. Moreover, such attacks can facilitate data theft or leakage by intercepting sensitive network traffic. Additionally, SDN topology poisoning attacks can be leveraged for launching denial-of-service (DoS) attacks, compromising network security, and causing reputational damage to affected organizations. To mitigate these risks, it's imperative for organizations to implement robust security measures, including access controls, encryption, intrusion detection systems (IDS), and regular security audits. Furthermore, educating network administrators and users about SDN security best practices is essential for effectively preventing and responding to these attacks

Results of base models

Model Name	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.92	0.88	0.94	0.91
Random Forest	0.94	0.92	0.95	0.93
Support Vector Machine	0.91	0.89	0.92	0.90
Neural Network	0.95	0.93	0.96	0.94

VI.CONCLUSION

In conclusion, defending against software-defined network (SDN) topology poisoning attacks requires a comprehensive and adaptive security approach. Organizations should prioritize securing access to the SDN controller, ensuring the integrity of communication channels, and implementing robust detection and response mechanisms. By combining access controls, encryption, anomaly detection, packet inspection, regular audits, network segmentation, and incident response planning, organizations can bolster their defenses against SDN topology poisoning attacks. Proactive measures, coupled with continuous monitoring and rapid response capabilities, are essential to safeguarding SDN infrastructure and maintaining network integrity in the face of evolving threats.

VI.FUTURE ENHANCEMENTS

Looking ahead, there are several promising avenues for enhancing defensive measures against software-defined network (SDN) topology poisoning attacks. One key area of focus involves the integration of advanced AI-driven anomaly detection systems. These systems can leverage machine learning algorithms to continuously analyze network traffic patterns, learn normal behavior, and swiftly identify deviations that may signal a topology poisoning attack. By automating the detection process and reducing false positives, AI-driven anomaly detection can significantly bolster the effectiveness of SDN security defenses.

Finally, fostering collaborative threat intelligence sharing among SDN stakeholders, industry peers, and cybersecurity communities is essential for staying ahead of evolving threats. Collaborative efforts enable the exchange of threat intelligence, best practices, and lessons learned, enhancing overall situational awareness and enabling rapid responses to emerging cybersecurity challenges, including SDN topology poisoning attacks.

.

VIII.REFERENCES

Certainly! Here are some references and sources that discuss defensive strategies against software-defined network (SDN) topology poisoning attacks:

1. "A Survey of SDN Security Issues and Solutions" by Shubha C and Shwetha GS in the International Journal of Computer Applications (IJCA), Vol. 179, No. 34, 2018. This survey paper provides an overview of various SDN security issues, including topology poisoning attacks, and discusses potential solutions and defensive measures.

2. "Security Challenges in Software-Defined Networking: A Survey" by S. Sivaramakrishnan, S. Sasikala, and S. Vijayakumar in the International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 9, No. 9, 2018. This survey paper explores security challenges in SDN environments, including topology poisoning attacks, and offers insights into defensive strategies.

3. "Software-Defined Networking: Challenges and Research Opportunities for Future Internet Architectures" by T. Koponen et al. in the Proceedings of the 2010 ACM Workshop on Hot Topics in Networks (HotNets-X), 2010. This paper discusses the challenges and opportunities of SDN, including security considerations, and lays the groundwork for understanding SDN security issues and defenses.

4. "Defending SDN Controllers Against Network-Wide Attacks" by M. Scott, K. Mattie, and D. Schmidt in the IEEE Security & Privacy Magazine, Vol. 14, No. 1, 2016. This article focuses on defending SDN controllers against various types of attacks, including topology poisoning, and provides insights into defensive mechanisms and strategies.

5. "Securing Software-Defined Networks: A Survey" by S. Yu, H. Wen, Y. Xiang, and S. Guo in the IEEE Network Magazine, Vol. 30, No. 5, 2016. This survey paper explores security challenges in SDN environments and discusses defensive techniques, including those aimed at mitigating topology poisoning attacks.

These references should provide a comprehensive understanding of defensive strategies against SDN topology poisoning attacks and offer valuable insights into the current state of research and practice in SDN security.