Ministry of Higher Education and Scientific Research, Iraq

University of Babylon

information technology collage

Information Security Department

SDN-Based Intrusion Detection Using Univariate Statistical Analysis

A Graduate Project Submitted to the Department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology

STUDENT'S NAME

Zainab Dawood Muslim

Supervised by

Assist. Lec. Shahad A. Hussein

2023-2024

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a major threat to network availability and can cause significant damage to network infrastructures. we propose an entropy-based approach for detecting and mitigating DDoS attacks in Software Defined Networks (SDN). The proposed approach leverages the programmability and centralization of SDN to calculate entropy on a per-IP basis and identify abnormal traffic patterns that indicate an ongoing DDoS attack. The proposed technique utilizes the source IP in the network and various attributes of UDP flags to calculate entropy. This statistical approach is effective in detecting volume-based and application-based DDoS attacks such as UDP floods. The approach is implemented using Python and evaluated through emulation using Mininet. Our experiments demonstrate that the proposed approach effectively detects and mitigates DDoS attacks while minimizing the impact on legitimate traffic. The proposed approach is implemented in a POX controller and uses the SDN control plane to facilitate real-time mitigation of DDoS attacks by blocking the targeted UDP port. The proposed approach can potentially be used as an effective tool for network administrators to secure their SDN environments against DDoS attacks.