Software-Defined Networking: A New Approach to Fifth Generation Networks: Security Issues and Challenges Ahead

Authors : Behrooz Daneshmand

Abstract : Software Defined Networking (SDN) is designed to meet the future needs of 5G mobile networks. The SDN architecture offers a new solution that involves separating the control plane from the data plane, which is usually paired together. Network functions traditionally performed on specific hardware can now be abstracted and virtualized on any device, and a centralized software-based administration approach is based on a central controller, facilitating the development of modern applications and services. These plan standards clear the way for a more adaptable, speedier, and more energetic network beneath computer program control compared with a conventional network. We accept SDN gives modern inquire about openings to security, and it can significantly affect network security research in numerous diverse ways. Subsequently, the SDN architecture engages systems to effectively screen activity and analyze threats to facilitate security approach modification and security benefit insertion. The segregation of the data planes and control and, be that as it may, opens security challenges, such as man-in-the-middle attacks (MIMA), denial of service (DoS) attacks, and immersion attacks. In this paper, we analyze security threats to each layer of SDN - application layer - southbound interfaces/northbound interfaces - controller layer and data layer. From a security point of see, the components that make up the SDN architecture have a few vulnerabilities, which may be abused by aggressors to perform noxious activities and hence influence the network and its administrations. Software-defined network assaults are shockingly a reality these days. In a nutshell, this paper highlights architectural weaknesses and develops attack vectors at each layer, which leads to conclusions about further progress in identifying the consequences of attacks and proposing mitigation strategies.