Detection and Prevention of DDoS attacks on Software Defined Networks Controllers for Smart Grid

Abstract

With the evolution of smart grid, the operations, planning and maintenance of an electric grid have improved. On the contrary, smart grid totally relies on the computer network so there is a need of complex and efficient network management. Software defined networks (SDN) is a completely new modern architecture that allows the network to be centrally controlled or explicitly programmed using software applications. Traditionally in computer networks, the routing and switching decisions are implemented on a dedicated hardware. This hardware can be a switch or a router. But with the evolution of Software defined networks, the routing and switching function has been separated and is classified in Control and data planes respectively. Generally, in SDN, the control plane is centralized and is responsible to make a decision on what to do with the incoming packet. Once the decision is made, it is saved in the forwarding table of a switch on the data plane. While Software Defined Network (SDN) has its advantages of central management, programmability, agility and vendor neutrality, they carry a high risk of Distributed Denial of Service attack (DDoS). Centralized nature of the control plane in SDN is a huge risk factor because the attacker may bombard the control plane with malicious packets.
resulting in a single point of failure of the control plane. If the control plane fails, the entire smart grid network will collapse resulting in a massive outage and financial loss to the stakeholders. In this paper, we have devised a distributed approach, using blockchains, to detect and prevent DDoS attacks on the centralized control plane of SDN. We have simulated our approach using AnyLogic simulator and the results show that the proposed approach is more efficient as compared the existing techniques as it substantially reduces the risk of DDoS attacks and SDN controller overhead.

References


Index Terms

Computer Science       Security

Keywords

SDN, Smart Grid, DDoS