

## Scalable and secure SDN based ethernet architecture by suppressing broadcast traffic

### ABSTRACT

Ethernet is one of the widespread protocols residing in the second layer of the seven-layers Open Systems Interconnection (OSI) model. Ethernet offers various advantages which enable its widespread use in all types of network topology and becomes an essential part of computer and network architecture. Despite its features, Ethernet suffers from scalability issues where the increasing number of hosts in a single broadcast domain will significantly expand the broadcast traffic in the network. Since the emergence of software-defined networking (SDN), researchers exploited various attractive features of SDN to suppress the broadcast traffic. Although capable in addressing the scalability issue of Ethernet, the existing SDN based solutions are lacking of security mechanism, which may expose the network to various ARP based attacks. Owing to this issue, this paper proposes a floodless and secure mechanism to suppress broadcast traffic. In general, the proposed solution utilizes SDN architecture and accommodates a multistage security algorithm. The multistage security algorithm consists of three stages; each stage incorporates specific analysis to identify the packet status or behavior, and react accordingly based on its status. To demonstrate the efficiency of the proposed solution, several ARP based attack scenarios are generated and evaluated using Mininet emulator. The performance evaluation indicates that the true positive ratio for attack detection in the proposed solution is 57.14% for the first stage, 66.66% for the second stage, and in some cases may achieve 100% for the final stage.

**Keyword:** Software-defined network (SDN); Ethernet scalability; Address resolution protocol (ARP); Dynamic host configuration protocol (DHCP); ARP storm; Spoofing attack