Detection and mitigation of ARP storm attacks using software defined networks

ABSTRACT

Attention to security aspects has increased rapidly in the current century by both academic researchers and companies offering security services and solutions, as a result for an increased attacks number on network infrastructure worldwide. Therefore, some techniques have emerged that can mitigate the effects of the attack and improve the ability of networks to detect attackers and prevent attacks. Software Defined Network (SDN) is considered one of the prominent techniques in general. SDN is emerging to enhancement existing protocols and networks architecture, in addition, to adding more simplicity for managing the networks. The proposed approach is depending on SDN features to detect and mitigate ARP storm attacks in Local Area Networks (LAN) without needing to change ARP packet, change the existing hardware or forcing hosts to install specific patch or application. Several scenarios applied to demonstrate the ability of the proposed approach in detecting the sources of storm attacks and protect both network devices and hosts from the effect of ARP storm attacks.

Keyword: SDN; ARP; Flooding; ARP storm; ARP flood