Detection denial of service attacks in SDN with an evaluation model based on fuzzy decision

ALI AKBAR RANJBAR EMAMZADE HASHEMI*,GholamHossein EKBATANIFARD,

Software-defined networking (SDN)is a new network architecture that separates the control page the data page, And logically, it provides a centralized control over the entire network. Because the SDN controller combines the high-applied layer and the underlying structure layer, this controller may encounter a one-point failure problem. If this controller becomes inaccessible to DDoS (Distributed Service Prohibition) attacks, the entire network may no longer function normally, Specifically, in the case of SDN wireless controllers, since the control protocol, the secure channel for communication between the wireless SDN controller and wireless SDN devices is exposed to the attacker's sight, the attacker's attack range will extend to SDN. In order to reduce the impact of this threat, a solution based on the fuzzy hybrid decision-making model has been proposed, which is an effective and lightweight solution in terms of resource efficiency, This solution uses factors for detecting DDoS attacks and makes comprehensive judgments based on these factors, In this research, three types of DDoS attacks for the SDN network and two DDoS attacks on the traditional and old network are considered for testing the solution. The results show that the proposed method is well-suited to detect most DDoS attacks.

Keywords : Software-defined networking (SDN), DDoS attacks, Fuzzy hybrid assessment decision making model.

Islamic Azad University, Rasht Branch - Thesis Database
دانشگاه آزاد اسلامی واحد رشت - سامانه بانک اطلاعات پایان نامه ها