A transparent and scalable anomaly-based DoS detection method

О. Јолџић, З. Ђурић, Р. Vuletić

Abstract:
Intrusions and intrusive behaviour can be aimed at different parts of the system, ranging from lower-level network attacks intended to disrupt the flow of data in general, to higher-level attacks targeted against specific applications or services. Due to the constant growth of network traffic and the need to inspect the traffic thoroughly, intrusion detection and prevention are becoming increasingly complex and require significant computational resources. This paper presents a distributed, scalable solution for the detection of lower-level Denial-of-Service (DoS) attacks which are executed by transmitting overwhelming amounts of data with the intention of disrupting regular network service. Scalability is achieved by active traffic balancing among multiple traffic processors, exploiting the flexibility and network programmability that Software Defined Networking paradigm brings and packet processing based on device polling. Traffic processors can be elastically added into the pool depending on the traffic volume. The whole system is completely transparent to the external observers. The paper shows that the implemented balancing algorithm further improves the reliability of the intrusion detection.

Keywords:
Intrusion detection; Intrusion prevention; Distributed processing; Load balancing; Security