Peer-to-Peer (P2P) botnet is one of the major threats in network security for serving as the infrastructure that is responsible for various cyber crimes. Enterprises routinely collect terabytes of security-relevant data. This work exploits such data to propose a novel large-scale P2P botnet detection that fuses big data behavioral analytics in conjunction with graph theoretical concepts.

P2P botnet lifecycle consists with the following stages: (a) Infection stage, during which the bot spreads, via email attachments, drive-by downloads, malicious software installation, etc.; (b) Rally stage, where the bot connects with a peer list and form P2P network; (c) Waiting stage, where the bot waits for the botmaster’s command; and (d) Executing stage, in which it actually attack carries out, such as a DDoS attack, generate mass of spam emails, etc. In this proposed work, we are focusing on detecting P2P botnet in last two stages. Future directions will also be discussed.