# A Rule-based Approach to Detect Botnets based on DNS

**Kamal Alieyan, Ammar Almomani, Rosni Abdullah, Mohammed Anbar**

Botnets inflict serious problems on the global computer network (the Internet). They can result in serious economic damages for both organizations and individuals. Botnets comprise thousands of hosts being infected. Latest developed modes of the botnet utilize other channels of communication like domain name server (DNS) between C&C servers and the hosts that are infected (the bots). Using substitute channels of communication enable the botnets to make a detour around the common network filters. Accordingly, a new rule-based method is introduced in this study. This method aims to detect the botnet based on DNS called Rule Botnet Detection (RBD). It can enhance the accuracy of detecting botnets based on DNS traffic. RBD uses a rule based on DNS query and response behaviors. Based on RBD, a higher accuracy level achieved with a lower false positive compared with other approaches. The findings, which were obtained based on the proposed approach, significantly increased the network's security situation awareness in the network's community. The findings concluded that the accuracy of the RBD in detection is (99.97 %) compared with approach named (PsyBoG), this approach can detect the malicious behavior that is caused by DNS traffic.