DDoSimu5G: A Simulation-Based Study of Temporal Botnet DDoS Attack Impact on 5G+ Network KPIs

*Note: Sub-titles are not captured for https://ieeexplore.ieee.org and should not be used

1st Karim Khalil, 2nd Christian Gehrmann,4th Sara Ramezanian *Department of EIT, Lund University*, Lund, Sweden
{karim.khalil,christian.gehrmann,sara.ramezanian}@eit.lth.se
3rdJakob Sternby *Ericsson Research, Ericsson*, Lund, Sweden
jakob.sternby@ericsson.com

Abstract

Modern 5G networks are increasingly vulnerable to large-scale Distributed Denial of Service (DDoS) attacks, particularly those amplified by mobile user equipment (UE) with limited cybersecurity readiness. Telecommunication network operators often monitor traffic loads and employ strategies such as reducing cell coverage, rerouting traffic, and load balancing to manage capacity spikes. However, attacks from mobile botnets necessitate a deeper understanding of traffic behavior, as these methods may not be sufficient. Analyzing changes in key performance indicators (KPIs) is essential for effectively detecting and mitigating malicious activity. This paper introduces a simulation framework, *DDoSimu5G*, designed to support this objective by analyzing how botnet-driven DDoS adversarial traffic influences 5G+ network KPI behavior over time. By integrating Simu5G and the ONE Simulator, the framework models Device-to-Device (D2D) epidemic infection of UEs and evaluates their impact on 5G user plane functions under varying traffic conditions. Unlike prior work that examines D2D propagation and DDoS effects in isolation, our approach captures their combined influence on the network performance. The resulting open-source framework enables reproducible experimentation and supports the development of adaptive, cost-aware detection and mitigation strategies in next-generation mobile networks.

Index Terms

5G, Simulations, Malware Propagation.

Identify applicable funding agency here. If none, delete this.