Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

ASEM KITANA

MSc (De Paul University, 2007)
BSc (Amman University, Jordan, 2005)

“Impact of Mobile Botnet on Long Term Evolution Networks: A Distributed Denial of Service Attack Perspective”

Department of Electrical and Computer Engineering

Wednesday, March 24, 2021
9:00 A.M
Remote Defence

Supervisory Committee:
Dr. Issa Traore, Department of Electrical and Computer Engineering, University of Victoria (Co-Supervisor)
Dr. Isaac Woungang, Department of Computer Science, UVic (Co-Supervisor)
Dr. Kin Li, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Alex Thomo, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Arunita Jaekel, School of Computer Science, University of Windsor

Chair of Oral Examination:
Dr. Abdul Roudsari, School of Health Information Science, UVic
Abstract

In recent years, the advent of Long Term Evolution (LTE) technology as a prominent component of 4G networks and future 5G networks, has paved the way for fast and new mobile web access and application services. With these advantages come some security concerns in terms of attacks that can be launched on such networks. This thesis focuses on the impact of the mobile botnet on LTE networks by implementing a mobile botnet architecture that initiates a Distributed Denial of Service (DDoS) attack. First, in the quest of understanding the mobile botnet behavior, a correlation between the mobile botnet impact and different mobile device mobility models, is established, leading to the study of the impact of the random patterns versus the uniform patterns of movements on the mobile botnet’s behavior under a DDoS attack. Second, the impact of two base transceiver station selection mechanisms on a mobile botnet behavior launching a DDoS attack on a LTE network is studied, the goal being to derive the effect of the attack severity of the mobile botnet. Third, an epidemic SMS-based cellular botnet that uses an epidemic command and control mechanism to initiate a short message services (SMS) phishing attack, is proposed and its threat impact is studied and simulated using three random graphs models. The simulation results obtained reveal that (1) in terms of users’ mobility patterns, the impact of the mobile botnet behavior under a DDoS attack on a victim web server is more pronounced when an asymmetric mobility model is considered compared to a symmetric mobility model; (2) in terms of base transceiver station selection mechanisms, the Distance-Based Model mechanism yields a higher threat impact on the victim server compared to the Signal Power Based Model mechanism; and (3) under the Erdos-and-Reyni Topology, the proposed epidemic SMS-based cellular botnet is shown to be resistant and resilient to random and selective cellular device failures.