Modelling Challenges and Attacks to Wireless Networks

Dongsheng Zhang, Santosh Gogi, Egemen Çetinkaya, and James P.G. Sterbenz

Understanding network behaviour under perturbations can improve today's networks performance, as well as lead to a more resilient and survivable Future Internetwork. Therefore, it is essential to have a thorough understanding of the network behaviour when exposed to challenges, such as component failures, attacks, large-scale disasters, and effects of the mobile wireless communication environment. Recognition of network disruptions and their causes is crucial for planning and designing networks. We cannot thoroughly study the effects of challenges in live networks without impacting users. Testbeds are useful, but do not provide the scope and scale necessary to understand the resilience of large, complex networks, although progress is being made in this direction. Simulations arguably provide the best compromise between tractability and realism to study challenges, however this is nontrivial. We develop the KU Challenge Simulation Module (KU-CSM) to evaluate network dependability and performability in the face of challenges. We utilise ns-3 network simulator as the main component of our framework and KU-CSM consists of four distinct steps: challenge specification, network topology, ns-3 C++ code, simulation and post-processing. As a result, we can study the impact of challenges on networks in a cost-efficient way.

The Wireless Challenge Simulation Module (WCSM) extends the previous work of KU-CSM. The mobile ad hoc network (MANET) environment has a dynamic and intermittent network connectivity due to channel fading and the mobility of the nodes; hence, it is be more complex and difficult to model these networks and their challenges. We begin by applying a maximum range propagation model to our simulation and then extend to more sophisticated radio models. We model MANETs as time-varing graphs represented as a weighted adjacecy matrix, in which the weights refer to the link availability during a period of time. A wide range of network attacks are modeled including several attacks models used for wired network. We concentrate on malicious attack scenarios, in which we model attacking the most significant nodes in the network, based on clustering coefficient and several centrality metrics such as degree, betweenness, and closeness. Our ultimate goal is to provide a comprehensive network challenge framework incorporating both wired and wireless networks.