Title:
Science-Based Metrics for Network Topology Resilience against Attacks

Abstract:
Defining meaningful security metrics, which are needed to quantify security risks, is one of the most frequent and urgent calls addressed to security researchers. Unfortunately, the adversarial nature of security has resisted to traditional methods of quantifying risk and only ad hoc solutions are available in individual domains. We still are desperately in need of well-grounded security metrics that are developed using proven mathematical models.

In this talk, I will introduce a game theoretic framework to derive metrics for network topology resilience in adversarial environment. Game Theory models provide a principled way to understand the security problem and to capture its adversarial nature. I will first introduce the notion of network blocking games and discuss how it can be used to derive metrics for the vulnerability of network topologies in adversarial environments. A network blocking game takes as input the communication model and the topology of a network and models the strategic interactions between an adversary and the network operator as a two-player game. The Nash equilibrium strategies are then used to predict the most likely attacker’s actions and the attacker’s Nash equilibrium payoff serves as a quantification of the vulnerability of the network.

I will show how the theory of blocking pairs of polyhedra can be used to derive a formula for the Nash equilibrium payoff of the game. This Nash equilibrium payoff is proposed as a metric for vulnerability. Using a series of illustrative examples, I will discuss properties of the proposed metrics and show how they can be related to well-known graph theory notions. I will also show how the metrics can be used to design robust networks and/or strengthen the robustness of existing ones. Finally, I will show how the metrics can be used to identify the most critical links in a network.

This is joint work with Dr. Vladimir Marbukh (NIST), Aron Lazska (Budapest University of Technology and Economics), Prof. Jean C. Walrand and Prof. Venkat Anantharam (UC Berkeley),

Bio:

Dr. Assane Gueye is a postdoctoral researcher jointly at the National Institute of Standards and Technology (NIST) and the University of Maryland, College Park. He received his Ph.D. in Electrical Engineering and Computer Sciences (March 2011) from the University of California at Berkeley and his Master of Engineering (September 2004) in Communication Systems from the Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland. Assane’s current research focuses on network science and cybersecurity, the security of large-scale interconnected systems, and cybersecurity metrology. His past research includes bottleneck identification in complex network, performance evaluation of wireless cellular networks and sensor network deployment in unknown environment.