Game Theoretic Vulnerability Assessment of Transportation Networks

Lance Fiondella, *Department of Computer Science & Engineering, University of Connecticut*

Abstract: Transportation networks are vulnerable to disruptions from natural disasters and terrorist attacks. Due to the size and complexity of these networks, a quantitative method to identify the most vulnerable links is necessary. This talk presents a two player game to assess the vulnerability of the links comprising a network. The traffic management authority seeks to route travelers on the safest most convenient paths, while an attacker conspires to disable the links that will maximize network disruption. The realism of the router's play is enhanced with concepts from transportation engineering, including a traffic assignment algorithm that considers the impact of congestion on travel time. We also define an *interest function* to capture the attacker's desire to target crowded areas that possess high intrinsic value and are poorly defended. The approach is demonstrated on the cities of Anaheim, California and Chicago, Illinois. To simplify analysis, we visualize the results of the game by coloring roads according to their criticality.

Lance Fiondella completed his Ph.D. at the University of Connecticut (UConn). In 2007, he received a scholarship from the IEEE Reliability Society for his research on system and software reliability. He also conducts network vulnerability research for UConn's Department of Homeland Security (DHS) National Transportation Security Center of Excellence (NTSCOE). He was an invited speaker at the 2011 DHS Student Day, where he presented his research on the optimal deployment and protection of high-speed rail.