Fault Tree Reliability Analysis of Network Configurations in Cybersecurity Intrusion Detection Systems

By Egarievwe, Stephen

Intrusion detection and protection systems are used to prevent attacks in neighborhood area networks of infrastructures such as smart grids. Real time Intrusion Detection and Prevention Systems (IDPS) serve as a promising solution to detect and possibly prevent a broad range of security related violations. This study focuses on communication network configurations with IDPS placed at the nodes. The goal is to analyze and compare the reliability of four basic configurations of collector communication networks: ring, star, tree, and mesh topologies. The analysis includes the development of fault tree for each network topology, finding the minimum cut-sets, and calculating the exact top event probability. In this study, each node in the network was assigned the same failure probability for all configurations. The results where each network configuration has 4 nodes show that the full mesh and star network topographies tie at best with the lowest top level fault probability. The tree network has the worst fault probability. Scalability analysis showed that the full mesh network is the best while the ring network is not scalable.

Biography

Stephen Egarievwe has PhD in Applied Physics. He serves as Director of the Nuclear Engineering and Radiological Science Center Alabama A&M University. His research areas include nuclear radiation detectors; data analytics for homeland security applications; and reduction of cybersecurity vulnerability and attacks at nuclear power plants.