Abstract

While mobile ad hoc networks offer significant improvements for tactical communications, these networks are vulnerable to node capture and other forms of cyber-attack. In this paper, we evaluated via simulation the impact of a passive attacker, a denial of service (DoS) attack, and a data swallowing attack. We compared two different adaptive network responses to these attacks against a baseline of no response for 10 and 20 node networks. Each response reflects a level of trust assigned to the captured node. Our simulation used a responsive variant of the ad hoc on-demand distance vector (AODV) routing algorithm and focused on the response performance. We assumed that the attacks had been detected and reported. We compared performance tradeoffs of attack, response, and network size by focusing on metrics such as "goodput", i.e. percentage of messages that reach the intended destination untainted by the captured node. We showed, for example, that under general conditions a DoS attack response should minimize attacker impact while a response to a data swallowing attack should minimize risk to the system and trust of the compromised node with most of the response benefit. We show that the best network response depends on the mission goals, network configuration, density, and network performance, attacker skill, and degree of compromise.