Abstract

Sensor networks are used as means to monitor sensitive objects such as an animal, a soldier in battlefield and hence the privacy of monitored objects' locations becomes an important concern. When a sensor reports a monitored object by sending a series of messages through the sensor network, the route these messages take in theory creates a trail leading back to their source. By eavesdropping on communications, an attacker may be able to move from node to node to follow this trail.To address this problem we try to confuse the adversary through multiple paths that leads to the source.