Abstract

Wireless sensor networks are now the best choice for several important applications such as monitoring disaster prone areas, surveillance and security of military operations, etc. By deploying a large number of tiny sensors (nodes) randomly over the region of interest, it is convenient to accomplish a specific task, especially in remote and hostile areas. Nodes with limited processing and communication capabilities act cooperatively in the network. For the realization of an event, it is necessary to relay the location data of the source nodes to a base station. As nodes are unaware of their location, a localization system is often desirable, which enables nodes to autonomously determine their location. State-of-the-art localization systems use a few location aware nodes with GPS receivers, called anchors. Since nodes and anchors relay data packets over a wireless medium, they are vulnerable to malicious attacks. Adversaries compromise a few nodes to tamper localization data or compromise the radio environment in a particular region, making the distance/angle estimation erroneous for the nodes located there. Eventually, the proliferation of such misinformation could mislead the plan/decision to be made at the base station. In the literature, these attacks are mitigated either by using cryptography or by detecting/eliminating misbehaviors of malicious nodes. But, cryptography remains fragile on compromised nodes because their secret keys/passwords are accessible to attackers. Non-cryptographic methods are worthwhile in the application or other inner layers. However, implementing localization systems that preserve security at the physical layer still remains a challenging task. In this thesis, we have claimed the benefits of using smart antennas to ensure greater energy efficiency and localization accuracy compared to conventional methods. By integrating smart antennas with anchors, malicious nodes were easily isolated, making the localization process as secure and robust as possible.

17/11/2023