Locating Sensors among Adversaries – SeRLoc to the Rescue

LOUKAS LAZOS, GRADUATE STUDENT (EE)

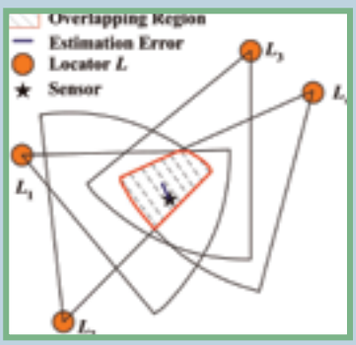
Wireless sensor networks monitor physical properties in a Field of Interest (FoI) such as temperature, humidity and motion. In order to extract meaningful information from the collected observations, the sensed data must be correlated with space. When sensors are stochastically deployed, they must estimate their location via a process known as localization. This research focuses on the problem of providing secure localization services for wireless sensor networks.

While sensor localization has been extensively explored for benign environments, enabling position estimation for sensors in the presence of adversaries has not been addressed. Attacks against the localization process not only disassociate the collected observations from the true location of sensors, but also inflict cross-layer vulnerabilities to location-dependent protocols of higher layers.

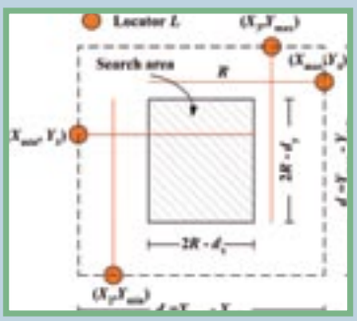
To ensure robust location estimation, a secure range-independent localization algorithm called SeRLoc was developed. SeRLoc relies on a two-tier network architecture. The network consist of a set of sensors of unknown location, and a set of nodes equipped with directional antennas called "locators," with known location and orientation. Both the sensors and nodes are randomly deployed in the FoI. In SeRLoc, sensors passively estimate their position based on beacons transmitted from the locators. Each beacon contains localization information that defines the sector antenna where the beacon transmission took place. The center of gravity of the convex intersection of the sectors heard is chosen as the sensor location.

By analyzing the space of possible attacks against SeRLoc, we showed that cryptography alone is not sufficient to secure the localization process. Instead, lightweight cryptography was combined (such as hashing and symmetric encryption/decryption with deployment statistics) to allow sensors to detect attacks on the localization like the wormhole and Sybil attack. We also analytically evaluated the level of security achieved by SeRLoc using Spatial Statistics theory.

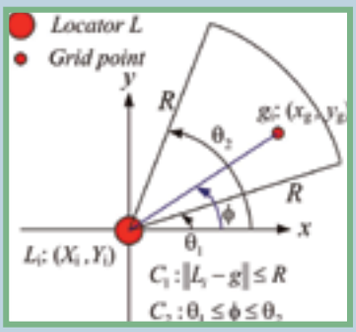
Securing the localization process is an essential requirement for providing secure network services. As the size of the sensor devices decreases, computational and energy resources become limited, so security becomes a challenging problem. To address this, secure localization methods that combine cryptography with multiple consistency checks on invariant physical properties must be developed. EE



THE SENSOR DEFINES A SEARCH AREA WHERE IT WILL ATTEMPT TO LOCALIZE ITSELF BASED ON THE COORDINATES OF THE LOCATORS IT HEARS, AND THE COMMUNICATION RANGE R OF EACH LOCATOR. IT THEN PLACES A FINE GRID OF EQUALLY SPACED POINTS WITHIN THE SEARCH AREA.



THE SENSOR PERFORMS A GRID-SECTOR TEST FOR EACH POINT OF THE SEARCH AREA AND FOR EACH LOCATOR. IF A POINT IS INCLUDED INSIDE A SECTOR, ITS VALUE ON A CORRESPONDING TABLE IS INCREASED BY ONE. THE DEFINED REGION OF INTERSECTION IS BASED ON MAJORITY VOTE.



EACH LOCATOR BROADCASTS A BEACON CONTAINING THE COORDINATES AND SLOPES OF THE LINES THAT DEFINE THE SECTOR WHERE THE TRANSMISSION TAKES PLACE. THE SENSOR HEARS LOCATORS L_1 - L_4 AND ESTIMATES ITS LOCATION TO BE THE CENTER OF GRAVITY FOR THE REGION OF INTERSECTION.

FACULTY ADVISOR: PROFESSOR RADHA POOVENDRAN
RESEARCH AREA: SECURITY IN WIRELESS SENSOR NETWORKS
GRANT/FUNDING SOURCE: DEPARTMENT OF DEFENSE (DOD)