MITIGATION OF CONTROL AND DATA TRAFFIC ATTACKS IN WIRELESS AD-HOC AND SENSOR NETWORKS

Recently we have seen increasing adoption of wireless ad-hoc and sensor networks (WAHAS) for security critical applications in military and civilian domains, such as battlefield surveillance and emergency rescue and relief. However, they are often exposed to a wide-range of control and data traffic attacks. Control attacks are directed to control traffic in the network, such as routing and localization. Examples are wormhole, Sybil, and rushing attacks. Control attacks are often easy to launch even without the need for any cryptographic key and can be used to subvert the functionality of the network by disrupting data flow. Data traffic attacks include selective forwarding and misrouting attacks.

We have pursued two lines of defense to secure WAHAS networks. The first is attack prevention using low-cost key management for encryption and authentication. Our protocol SECOS provides the guarantee that communication between any two nodes remains secure despite compromise of any number of other nodes. The second line of defense is control and data traffic attack detection, diagnosis, and isolation through *local monitoring* and *response*. Each node oversees the traffic in its one-hop neighborhood and maintains state for the behavior of each neighbor. We develop a suite of three protocols for respectively static networks, mobile networks, and energy efficient sleep-awake aware local monitoring. To demonstrate the protocols, we perform analysis and simulation in *ns-2*. The metrics for evaluation include fraction of data received at the destination, coverage and delay of isolation, likelihood of false positives, and overhead in terms of resource consumption.