**Introduction**

Wireless Sensor Network (WSN), as a subset of ad-hoc networks is one of the most resource-limited environments. The major concerns in sensor networks are the scarcity of energy, memory and processing power. Providing security with such limited resources is a challenging task.

Cryptography has been known to be an efficient tool in providing seamless security. However, the application of cryptographic primitives in WSN incurs noticeable cost. For public key primitives, this cost is so high that has made its application in WSN rather impossible.

For specific threats it is possible to take advantage of the WSNs characteristics in order to provide security in expense of accepting some level of imperfectness. What is earned is a great reduction in costs and simplicity of implementation.

The following figure shows three types of protocols reaction to greedy-type attacks. If an attacker spends more resources (x-axis), in a secure protocol it will not gain more than what it could gain if it behaved like a benign node. In the insecure profile the more the adversary spends, the more it gains. However, in the robust profile, although the maximum gain of the adversary is higher than the secure profile, but it is well limited.

![Graph showing Secure, Insecure, and Robust Profiles](image)

**Statistical Security Model**

Statistical security works for certain type of attacks in which the potential victims are numerous. Thus WSNs are good test beds for implementation of the statistical countermeasures.

The designer has to define the security goal and cost function first. Depending on the goal, the designer might need to modify or manipulate the protocols structures so that the gain profile turns into a generic robust type for the greedy adversaries. Then in an optimization phase the designer minimizes the maximum achievable payoff of the adversaries.

1. Define the Security Goal
2. Define the Security Cost Function
3. Design/Modify the Rules & Parameters
   - Normal Behavior
   - The Boundaries
4. Optimization

Usually there is no rigid boundary for separation of benign and malicious behaviors.

- **Benign Behavior**
- **Malicious Behavior**

The amount of guard band the designer considers for efficient operation of the network corresponds to the penalty paid in this approach which can be seen as an overshoot in the robust profile. Usually this band is imposed by the network characteristics, e.g.:

- The variation in the number of neighbors in neighbor discovery scenarios of WSNs
- The hardness of the optimal code assignment in CDMA WSNs

**Examples of Application**

- **Hello Flooding Attack**: In this attack, a compromised node advertises the Hello request which is used for neighbor discovery with very high power so that many nodes are convinced that the adversary is their neighbor. By modifying the protocol and adding an information-carrying reply to the Hello request, the nodes cause collisions at the receiver of the adversary preventing the correct decoding of the information (see the figure). Here $R$ is the attack range and $r$ is the benign carrier sense range. The optimization shall be done on the timing parameters of the nodes MAC layers.

- **Eavesdropping in CDMA WSNs**: In CDMA WSNs, code reusing is necessary. Assume that the network has sparse traffic (green arrows) and an eavesdropper tries capturing as much as information possible from the ongoing transmissions. Transmissions with similar codes in the eavesdropping range $R$ will significantly reduce the SIR. The better the code assignment is done (i.e. less codes are used), the less the information will leak. The optimization is done on the code assignment algorithm in this case.

---

**Learn More about Statistical Security**


