CERIAS

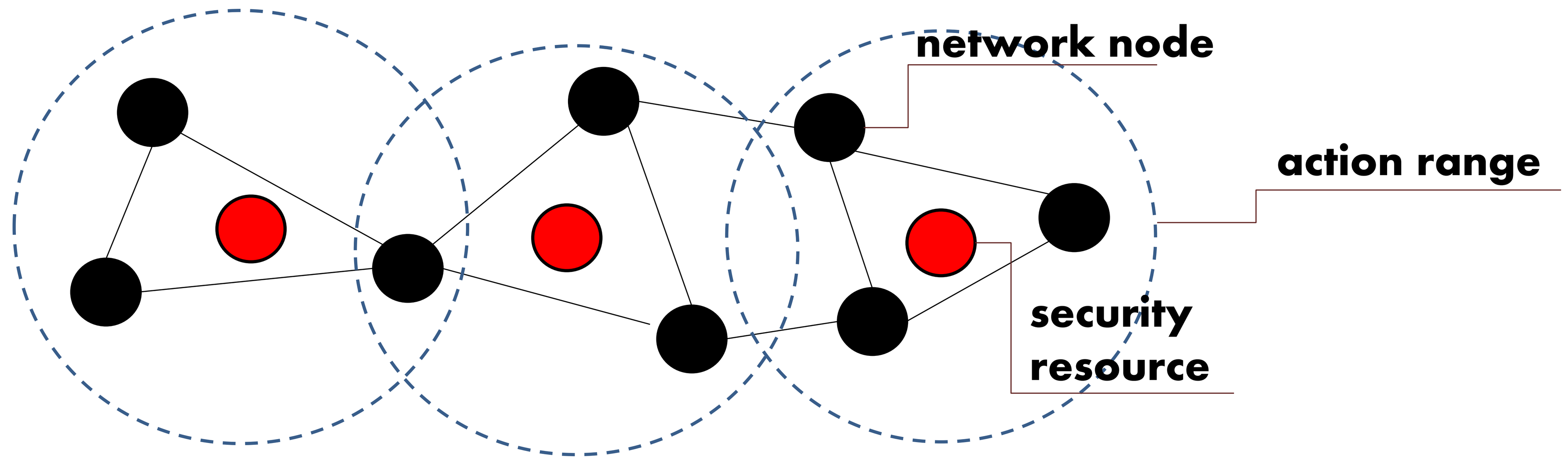
The Center for Education and Research in Information Assurance and Security

Strategic Security Resource Allocation for Internet of Things

Antonino Rullo, Daniele Midi, Edoardo Serra, Elisa Bertino

Problem

In an IoT scenario, given a set of security resources and a set of attacks to protect against, which resources should a security manager choose, and how should (s)he allocate them in the network in order to ensure protection with the minimum cost, the minimum energy consumption, and a certain degree of robustness against attacks?



SECURITY RESOURCES:

- intrusion detection systems;
- attack prevention systems;
- directional antennas and highly sensitive transceivers;
- tamper resistant hardware;
- additional nodes.

Definitions

DEFENDER STRATEGY EFFICIENCY: is based on the total **energy consumption** of the security infrastructure and the **costs of its components**.

DEFENDER STRATEGY EFFECTIVENESS: is based on two metrics: **risk**, defined as the maximum number of network nodes that are no longer protected when an attacker succeeds in taking down at least one security resource; **criticality**, a measure of how critical certain nodes are for the correct operation of the network.

SECURITY SYSTEMS: we classify security systems into two main categories: **detection and prevention systems**. Those categories correspond to two different security policies: (i) **node/link monitoring**, and (ii) **node/link hardening**.

SECURE NODE: a network node **n** is secure if at least one of the following conditions holds:

1. **n** is tamper resistant;
2. every **link** that involves **n** is secure.

SECURE LINK: a link **{n,n'}** is secure if at least one of the following conditions holds:

1. both nodes **n** and **n'** are in the action range of the same watchdog;
2. both nodes **n** and **n'** can establish a secure communication channel.

SECURE NETWORK: a network is secure if all the network nodes are secure according to the definition of secure node.

Players

DEFENDER: The defender strategy consists of a **security resource allocation plan**. The best plan is computed **in two steps**. The **first step** consists of a **Pareto analysis** which solves the optimization problem defined by the following equation:

$$\min_{AP \in \mathcal{AP}} \{ec(AP), tc(AP), \max_{sr \in AP} crit(sr, AP, N)\}$$

The **second step** computes the best allocation plan (best defender strategy), by solving the optimization problem defined by the following equation:

$$\min_{AP \in AP+} \{\max_{sr \in AP} risk(sr, AP, N)\}$$

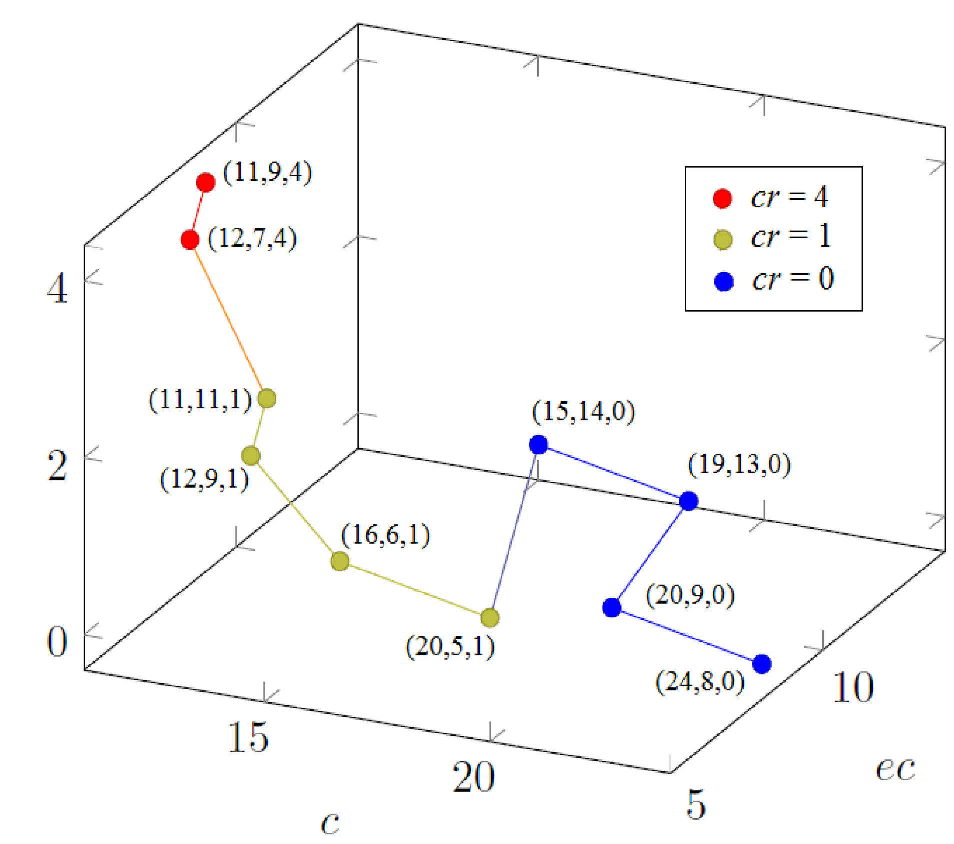
ATTACKER: can physically **tamper** with the network nodes, **capture** and **reprogram** legitimate nodes and security resources, and **add malicious entities** to **overhear** data, **inject** false data, **drop data packets**, introduce **interference**, claim **multiple identities.** The attacker needs to compromise at least one security resource in order to carry out an attack.

$$sr^* = \max_{sr \in AP} \alpha \cdot risk(sr, AP, N) + \beta \cdot crit(sr, AP, N)$$

Algorithm

Algorithm 1

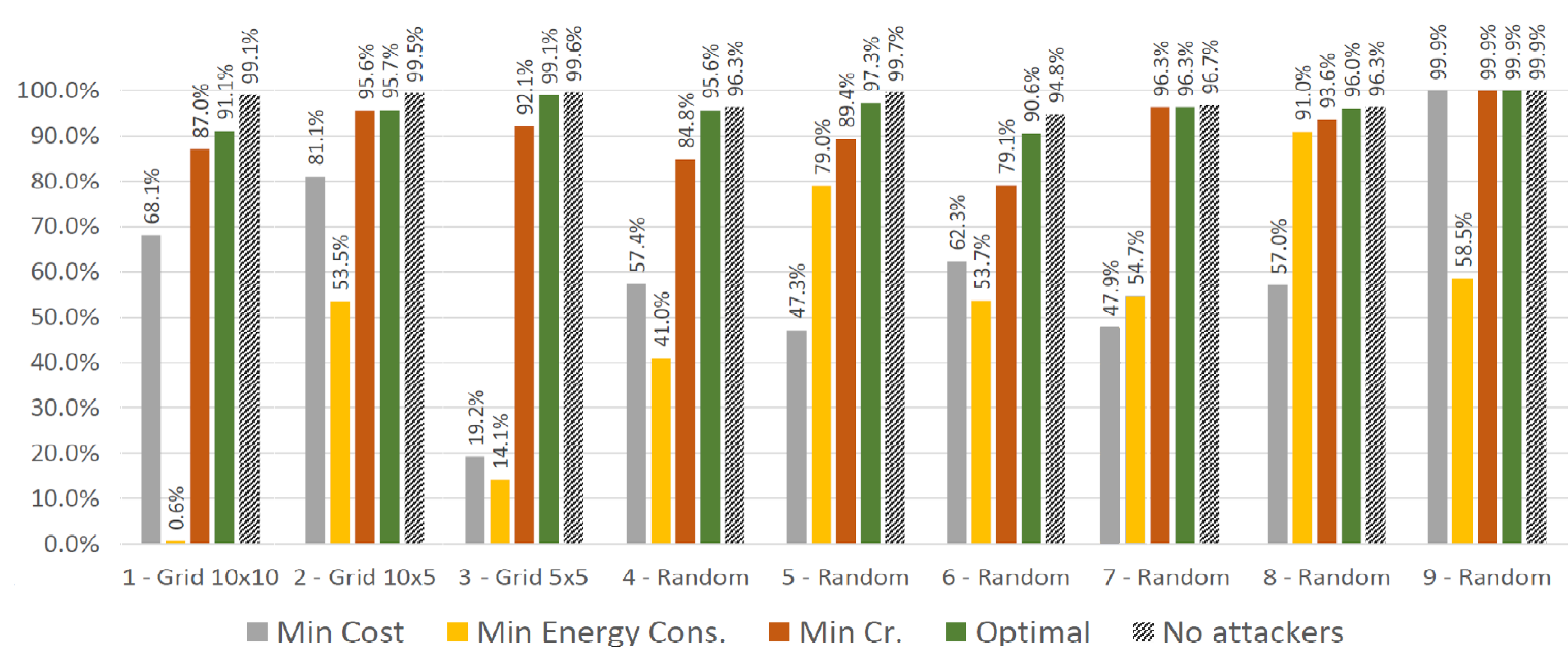
procedure ComputePC(minCR,maxCR)
  for $cr = minCR\text{-}1, \ldots, maxCR$ **do**
    $tc \leftarrow getTC(\infty, cr)$;
    while $(tc \neq null)$ **do**
      $ec \leftarrow getEC(tc, cr)$;
      $X \leftarrow X \cup (ec, tc, cr)$;
      $tc \leftarrow getTC(ec, cr)$;
    end while
  end for
  return Pareto-optimal points in X;
end procedure



$$getEC(tc, cr) = \min_{\substack{AP \in \mathcal{AP} \\ tc(AP) \leq tc \\ \max_{sr \in AP} crit(sr, AP, N) \leq cr}} ec(AP)$$

$$getTC(ec, cr) = \min_{\substack{AP \in \mathcal{AP} \\ ec(AP) < ec \\ \max_{sr \in AP} crit(sr, AP, N) \leq cr}} tc(AP)$$

Experimental Results



The best defender strategy provide a higher packet delivery rate w.r.t the most cheap strategy and the less energy consuming strategy.

Our approach provides a high quality defender strategy, for which the minimum cost is used, and that consumes the minimum amount of energy.