A methodology that allows the design of secure WSNs from the first steps of the development process

Dr. Fidel Ibrahim

Head of Department of Information Engineering, Al Hawash Private University

Abstract

Current wireless sensor networks (WSNs) require effective network simulation methodologies and embedded software performance analysis because of the increasing complexity and low power constraints imposed on these networks, as well as the security feature they should have for using sensitive data in undesirable and hostile environments.

This article includes a methodology for security analysis in wireless sensor networks through the design of a built-in firewall or a set of countermeasures. This is done by modeling the attacker and simulating the attack with the performance analysis (node execution time and power consumption estimate taking into account the spread of the network components and the topology) after examining three different types of attacks that mimic most attacks on wsn, It is capable of designing hardware devices, software programs, and basic wireless channels.

The planned simulation provides developers with necessary information about the effects of a single attack or a series of multiple attacks on the network, helping them develop more secure wireless sensor systems, and the WSN attack simulator is an essential element of the built-in anti-malware development strategy Of the attack put forward in this research.

About scientific research.

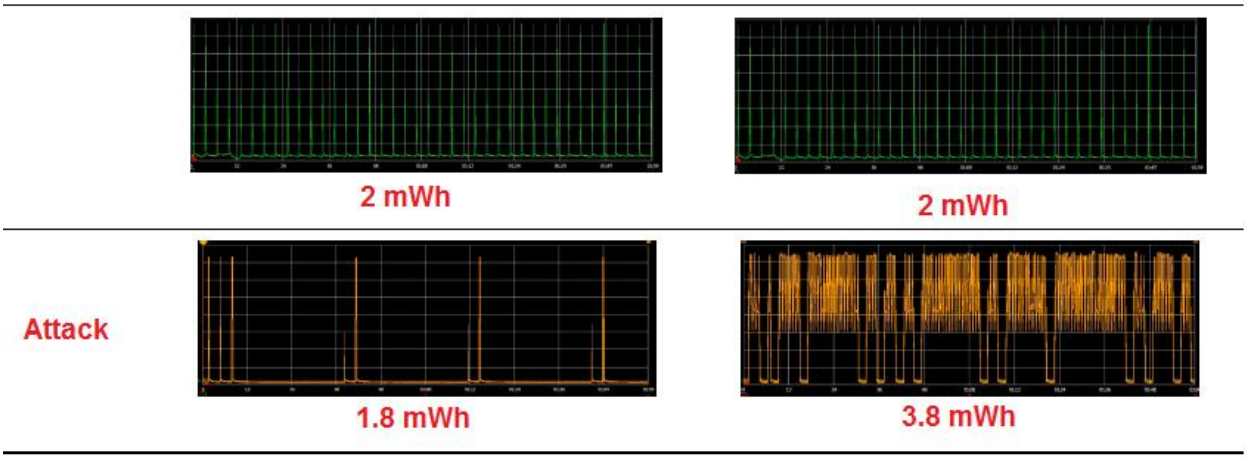
Smart environments (building, health, industry ...) are primarily based on smart devices that get real-world data processed and delivered to information processing centers to generate some information-based services, sometimes to produce certain services in the environment.

Information used by intelligent environments is provided by wireless sensor networks (WSNs), which are responsible for monitoring and physical recording of environmental conditions, and delivering collected data to its central location.

WSNs include a set of scattered nodes that relate to actuators and display information supplied to the environment. These nodes are multifunctional, with limited resources, low cost and energy, and are often operating in undesirable environments with limited sensitivity.

Common requirements for WSNs in previous years were in the security assessment first, especially because attackers could disable the network, access and modify information, access to the nodes, influence them, and modify their behavior. It was therefore necessary to identify WSNs security vulnerabilities within the early stages of the design process, as well as to understand the impact of the most common attacks on the node or the entire network, especially the energy consumption effect.

This article presents a methodology for simulating WSNs under different attack conditions, allowing the effects of these attacks to be determined on each node and on the network in full by identifying the most harmful attacks to help design countermeasures to prevent these attacks. This methodology is very effective before deploying network components during the software and hardware design phase, allowing developers to design safer systems and introduce anti-attack measures to avoid the effects of the most serious attacks that we have integrated into only four categories. Each category is represented by relevant attackers Facilitate their implementation in any WSN Simulator.



Energy Consumption results