ATTACK TOOL FOR WIRELESS SENSOR NETWORKS

Thanassis Giannetsos
Athens Information Technology
Peania, Athens, Greece
agia@ait.edu.gr

Tassos Dimitriou
Athens Information Technology
Peania, Athens, Greece
tdim@ait.edu.gr

Ioannis Krontiris
Athens Information Technology
Peania, Athens, Greece
ikro@ait.edu.gr

1. Demo Overview

The pervasive interconnection of autonomous sensor devices has given birth to a broad class of exiting new applications in several areas of our lives, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. At the same time, however, their unattended nature and the limited resources of their nodes have created equal number of vulnerabilities that attackers can exploit in order to gain access in the network and the information transferred within.

Motivated by the growing use of sensor networks, we will demonstrate a tool that allows both *inspection* of their functionality by analyzing overheard radio messages and *discharge* of various attacks against them. This tool can identify common applied protocols and use this information for performing attacks such as *Sinkhole attack, Replay attack, or Injecting malicious code* in order to take control over the network. Also, it can extract useful network information such as node crashes, reboots, routing problems, network partitions, and traffic analysis (overall network traffic or overheard traffic by each sensor node).

The presented tool is an implementation of our Sensor Network Attack Tool, which consists of a network sniffer for overhearing network traffic, a packet description database to decode overheard messages, a data stream framework to construct messages for launching attacks, and a graphical user interface to visualize and display the network topology, network traffic and node states.

The network sniffer is based on packets that are overheard in a sensors node neigh- borhood. These packets are forwarded to a computer where they are processed in order to extract vital network information such as node IDs or traffic data. Essentially, this sniffer allows to construct a directed graph of all neighboring nodes. Overheard packets flow along the edges of the graph and are provided with a number of operators for manipulating them.

The network attack tool, at its current state, gives the user the opportunity to launch three different kind of attacks:

- **Sinkhole attack**: The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. Through the attack tool, the user will start transmitting “routing packets” specially constructed for attracting all or as much traffic as possible from the nodes neighborhood.

- **Replay attack**: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated. Since, all overheard messages are stored into a database (work done by the network sniffer), the user is able to change them and re-transmit them at a later time.

- **Inject malicious code**: By taking advantage of memory overflows in sensor nodes, the user may send crafted data to trigger a stack overflow and execute arbitrary code on the target system.

The graphical user interface of the demonstrated tool shows, in real time, all the above described network information and the state of the performed attacks.

The demo will consist of a deployed sensor network and one laptop computer with a connected sensor device for overhearing sent messages and displaying collected data in an appropriate GUI. The transmission power of the sensor nodes will be reduced to obtain a true multi-hop sensor network. Finally, the motes will run a typical data gathering appli- cation, like Delta, which is based on the MultiHopLQI routing protocol.