Security Training Introduction

Hands-on Security Simulation

- This tutorial describes the way in which security training will be conducted using Cooja
- The key element of our approach is to run first a "**reference simulation**", so that trainees understand the scenario
- This is followed by the deployment of malicious nodes in the reference network to create the "**attack simulation**"
    - The attacks are achieved by modifying RPL-related files, thus resulting in an alteration of the node behavior

Reference and Attack Scenarios

- IoTrain-Sim includes already several security training scenarios, and for each of them both the reference and the attack scenarios are provided
- Each of them can be started via the corresponding menu entries in the IoTrain-Sim command-line interface
- For reference purposes, in the following slides we provide an overview on how to create a reference simulation via the Cooja GUI, and the preparation steps needed before the implementation of different attacks, so that the training content can be extened

1. Reference Simulation

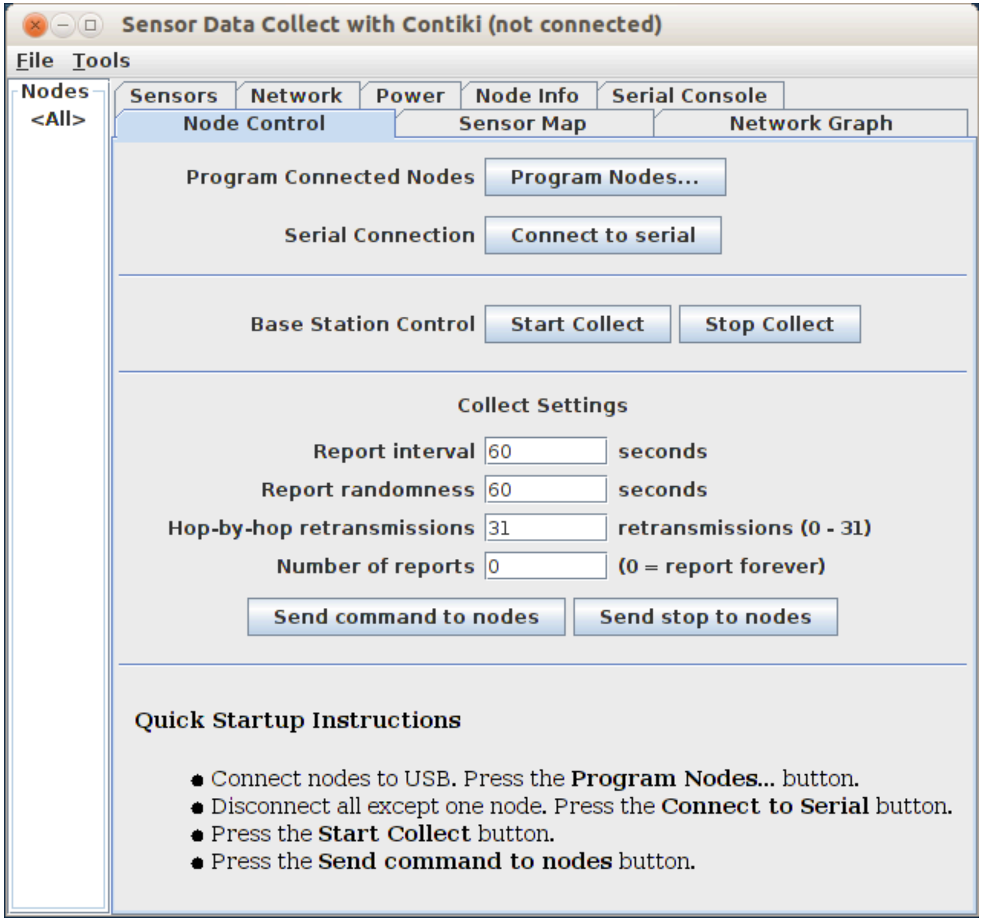
- Open Cooja and click on File > New simulation
- Create the mote types that will make up the network
  - Typically, the reference network will have two types of motes
    - One sink mote, which would function as an LBR and DODAG router
    - Several leaf motes, functioning as mere sensor data collectors
  - Motes will be based on the following firmware files
    - Sink more → "contiki/examples/ipv6/rpl-collect/sink.c"
    - Leaf motes → "contiki/examples/ipv6/rpl-collect/udp-sender.c"
- After starting the simulation, use the "Collect-view" tool on the sink node to collect internal data
- Save the simulation as an CSC file

What is Collect-view

- Collect-view is a Java based application in Contiki used for internal mote information visualization
- A mote is acting as a SINK, while the other motes are acting as sources
    - Source motes send important parameters to the SINK
- Collect-view uses a Graphical User Interface (GUI) for visualizing mote parameters
- In an attack simulation, this tool will be used frequently to observe the impact of malicious nodes on the network

Running Collect-view

- To manually open Collect-view, run the following commands
  - cd contiki/tools/collect-view
  - ant run
- The interface with the Node Control panel selected will be displayed, as illustrated in the screenshot on the right



Report interval 60 seconds

Report randomness 60 seconds

Hop-by-hop retransmissions 31 retransmissions (0 - 31)

Number of reports 0 (0 = report forever)

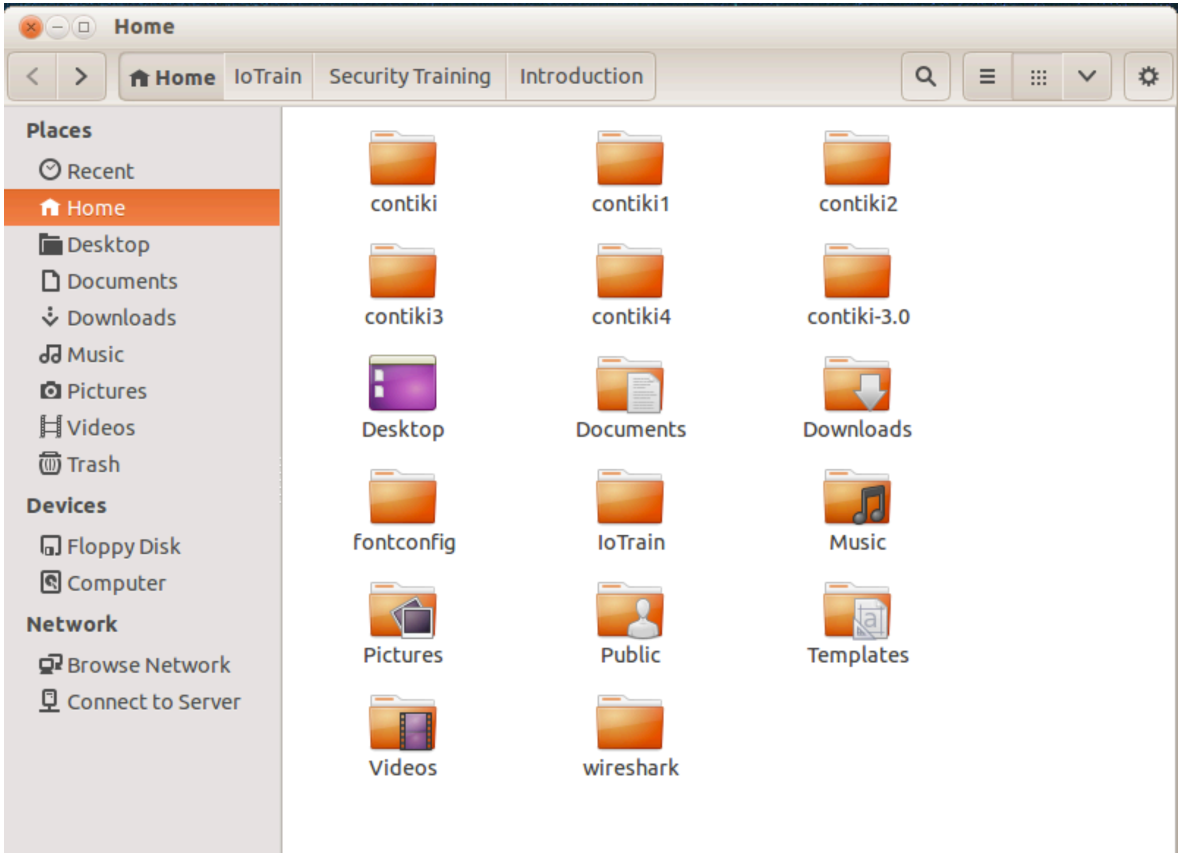
Quick Startup Instructions

- Connect nodes to USB. Press the **Program Nodes...** button.
- Disconnect all except one node. Press the **Connect to Serial** button.
- Press the **Start Collect** button.
- Press the **Send command to nodes** button.

2. Attack Simulation

- Attack simulation is done by modifying the behavior of one or more motes, without altering the normal behavior of the other network nodes
  - Thus, one can assess network changes during security attacks
- The recommended method to achieve this is
  1. Duplicate the “contiki/” folder to create a new Contiki instance (for example, you can use “contiki1/” for flooding attack, “contiki2/” for version number attack, etc.)
  2. Modify the necessary files in the new Contiki instance according to the specificities of the attack
  3. Open the target reference simulation file in Cooja
  4. Create a new malicious mote as a leaf and compile the node firmware within the new Contiki instance
  5. Add the malicious mote(s) to the reference network

Attack Simulation Folders



Home

Home | IoTrain | Security Training | Introduction

Places
- Recent
- Home
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Trash

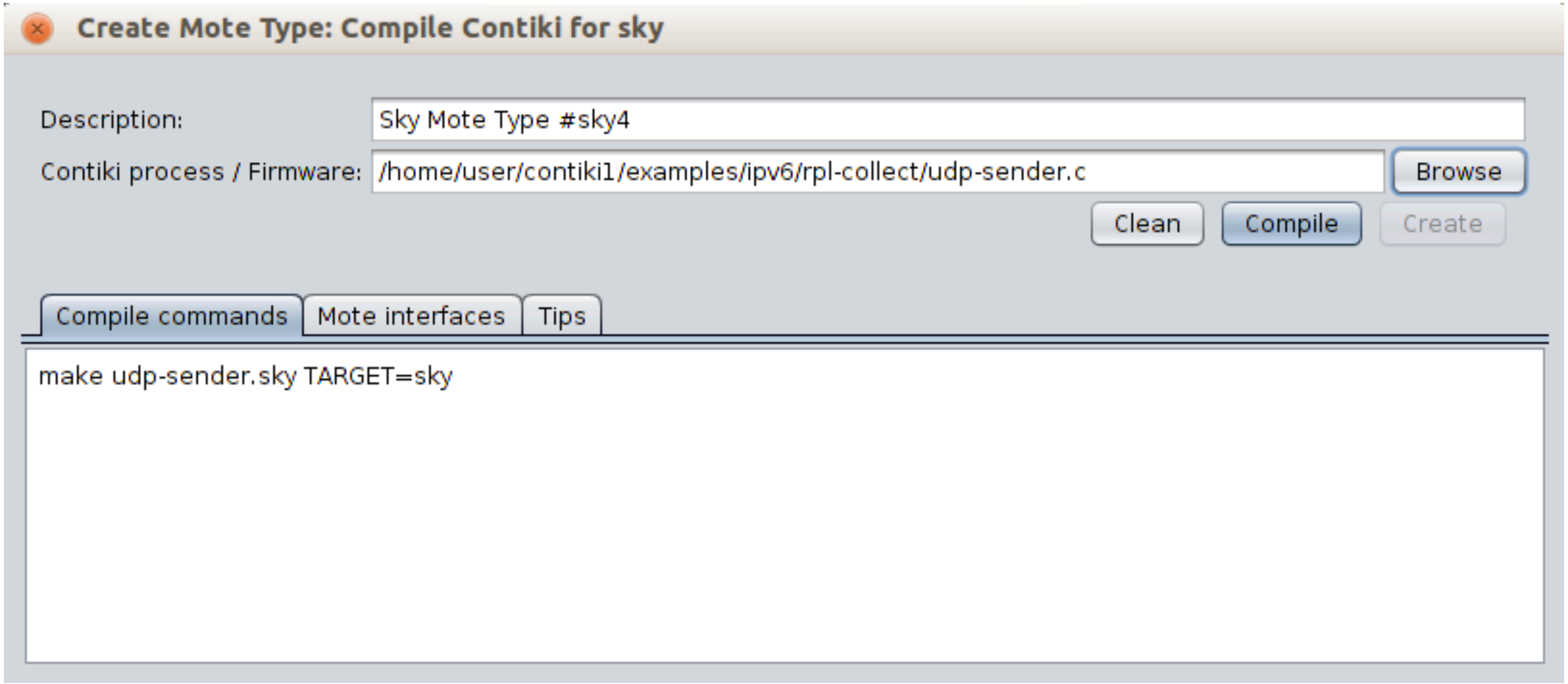
Devices
- Floppy Disk
- Computer

Network
- Browse Network
- Connect to Server

contiki
contiki1
contiki2
contiki3
contiki4
contiki-3.0
Desktop
Documents
Downloads
fontconfig
IoTrain
Music
Pictures
Public
Templates
Videos
wireshark

Several Contiki folders as needed to create different types of malicious motes

Attack Simulation Implementation



Description: Sky Mote Type #sky4

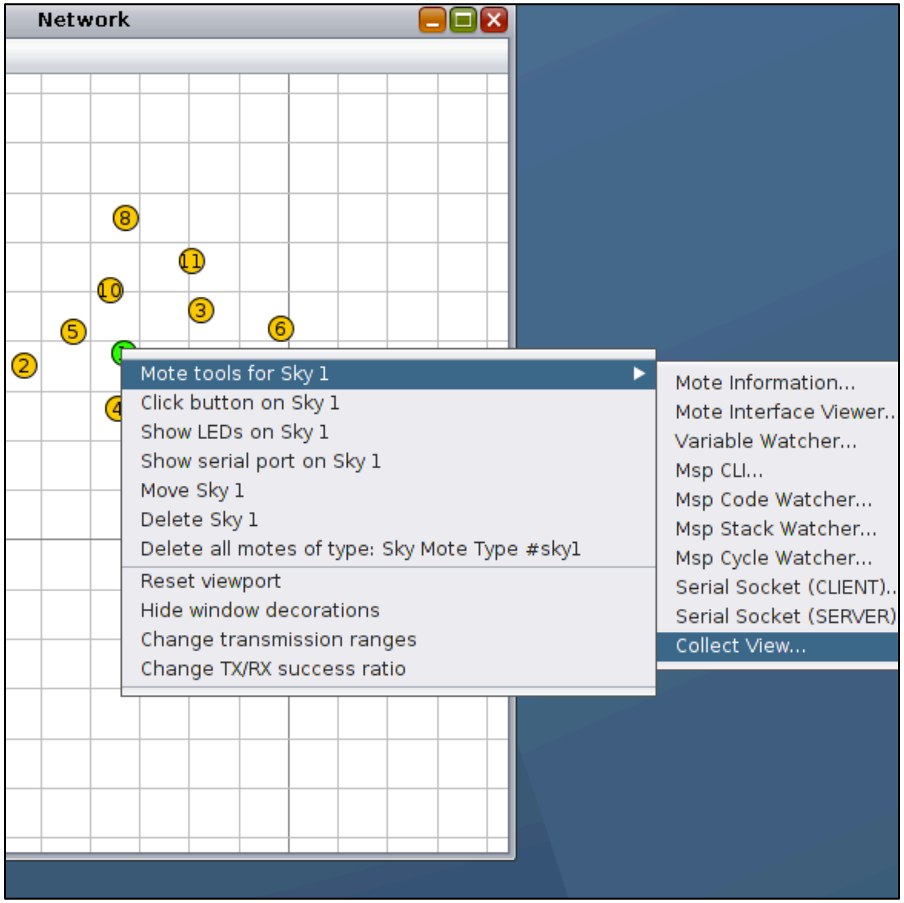
Contiki process / Firmware: /home/user/contiki1/examples/ipv6/rpl-collect/udp-sender.c

```
make udp-sender.sky TARGET=sky
```

Creating a malicious mote with source code from another Contiki instance

Collect-view in Attack Simulation

- In an attack simulation, do the following to use Collect-view
  - Find the SINK node
  - Right click on the SINK node, then select Mote tools for … > Collect View
  - In the Node control panel, click on "Start Collect", then click on "Send command to nodes"


Network
8
11
10
3
5
6
2
1
4
Mote tools for Sky 1
Click button on Sky 1
Show LEDs on Sky 1
Show serial port on Sky 1
Move Sky 1
Delete Sky 1
Delete all motes of type: Sky Mote Type #sky1
Reset viewport
Hide window decorations
Change transmission ranges
Change TX/RX success ratio
Mote Information...
Mote Interface Viewer..
Variable Watcher...
Msp CLI...
Msp Code Watcher...
Msp Stack Watcher...
Msp Cycle Watcher...
Serial Socket (CLIENT)..
Serial Socket (SERVER)
Collect View...