Student : Rémi Heredero
Professor : Prof. Medard Rieder
Expert : Rico Steiner (HOOC AG, Visp)

Hes·so VALAIS WALLIS
School of Engineering

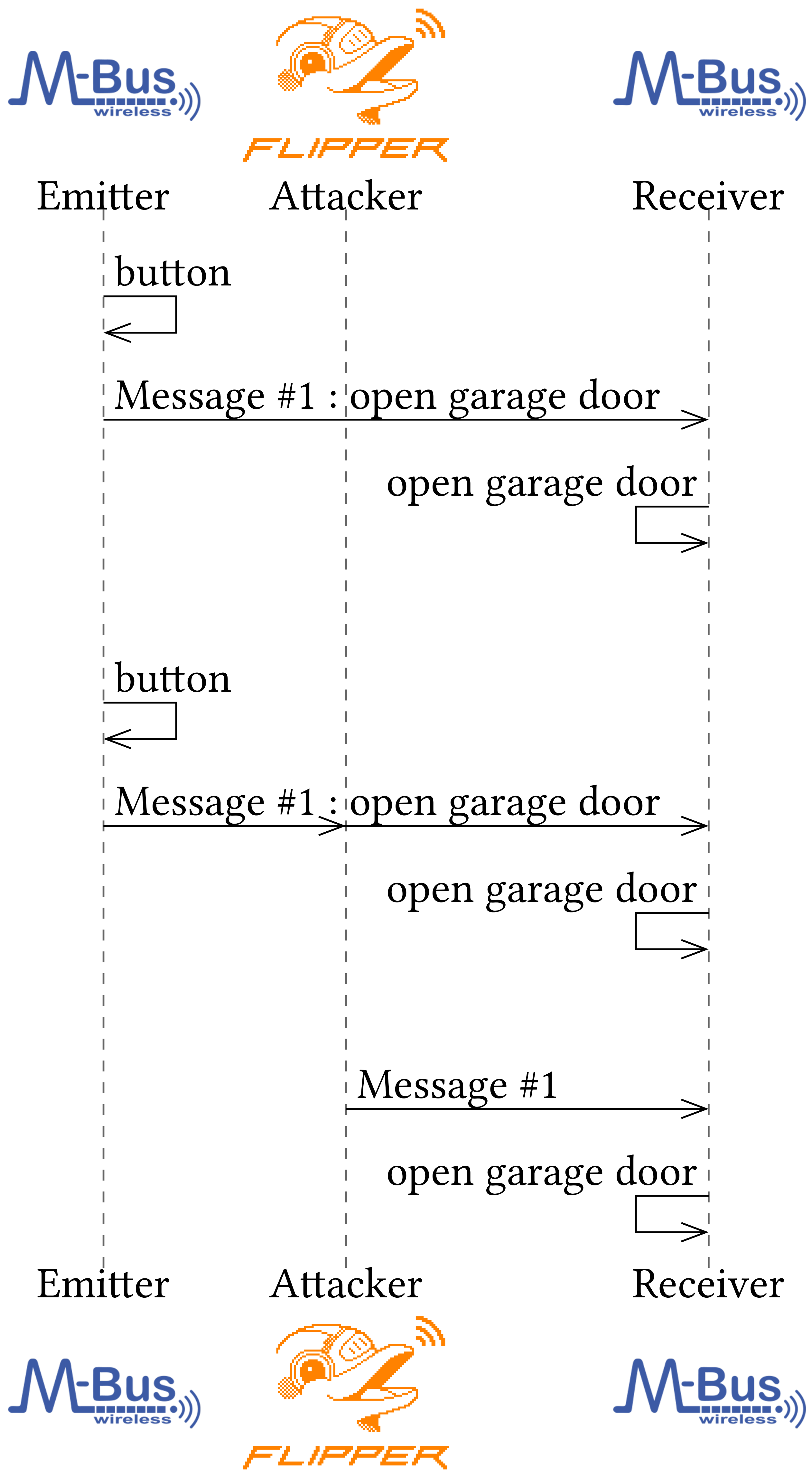
OT Security

Context

This thesis, existe in the context of the rework of the embedded systems security course at HEI-VS. The aim is to come up with several attack scenarios which can be used as the basis for a laboratory module for students. These scenarios could also serve in industrial training partnerships with HEI-VS.

Replay attack scenario

The replay scenario involves intercepting and re-sends a wireless message for replay same effect, like a garage door opening.


Emitter
Attacker
Receiver
button
Message #1 : open garage door
open garage door
button
Message #1 : open garage door
open garage door
Message #1
open garage door
Emitter
Attacker
Receiver

To protect against this attack, the system should integrate a security in the message, like rolling code or an encrypted counter with a private key.

Stack

Kali
OS

Wireshark
Packets sniffer

Ettercap
MitM tool

Iptables
Firewall

Python
Programming language

Scapy
Packet manipulation

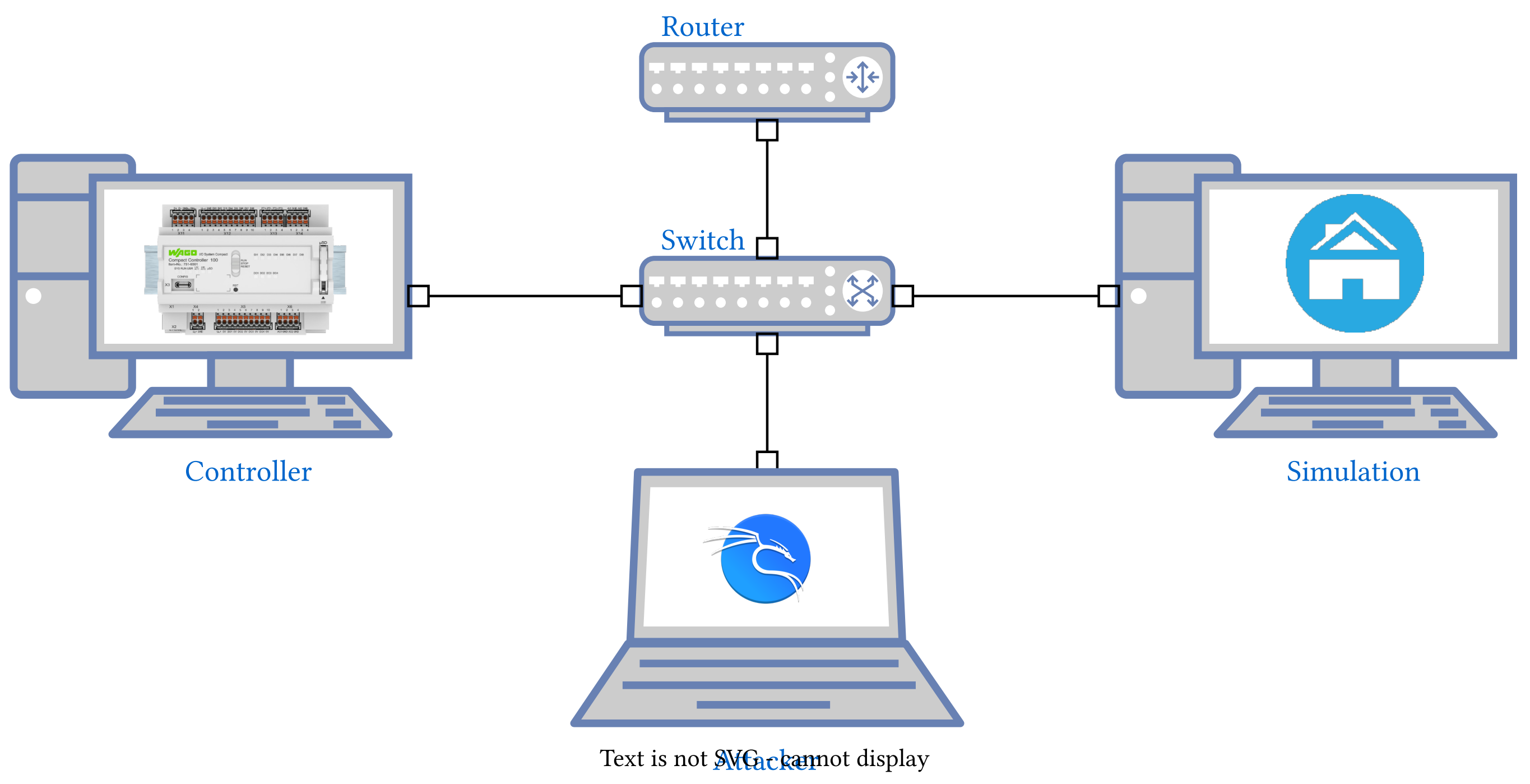
Golang
Programming language

Flipper Zero
Pen testing toy

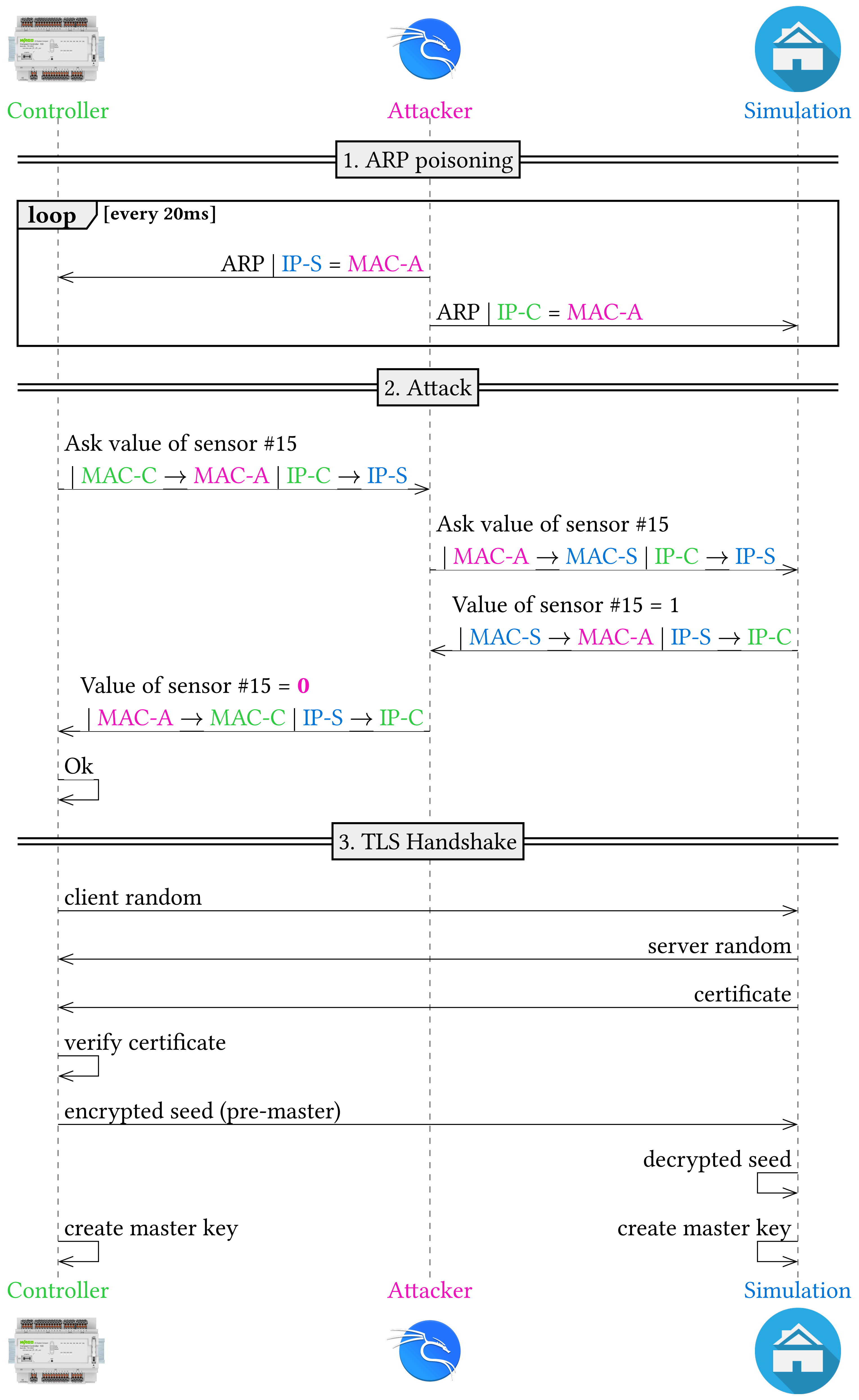
Wireless M-Bus
Wireless protocol

Man in the middle

The Man in the Middle scenario involves intercepting, modifying and sending packets to take control of a Modbus/TCP installation.



The first step of the attacker is to intercept the communication between the controller and the installation. To achieve this goal, the attacker has to do an ARP poisoning attack (1). Once the attacker intercepts all packets, it is possible to modify them (2). To protect against this attack, the system has to use Modbus over TLS (3).


Controller
Attacker
Simulation

1. ARP poisoning

loop [every 20ms]
ARP | IP-S = MAC-A
ARP | IP-C = MAC-A

2. Attack

Ask value of sensor #15
| MAC-C → MAC-A | IP-C → IP-S
Ask value of sensor #15
| MAC-A → MAC-S | IP-C → IP-S
Value of sensor #15 = 1
| MAC-S → MAC-A | IP-S → IP-C
Value of sensor #15 = **0**
| MAC-A → MAC-C | IP-S → IP-C
Ok

3. TLS Handshake

client random
server random
certificate
verify certificate
encrypted seed (pre-master)
decrypted seed
create master key
create master key

Controller
Attacker
Simulation