

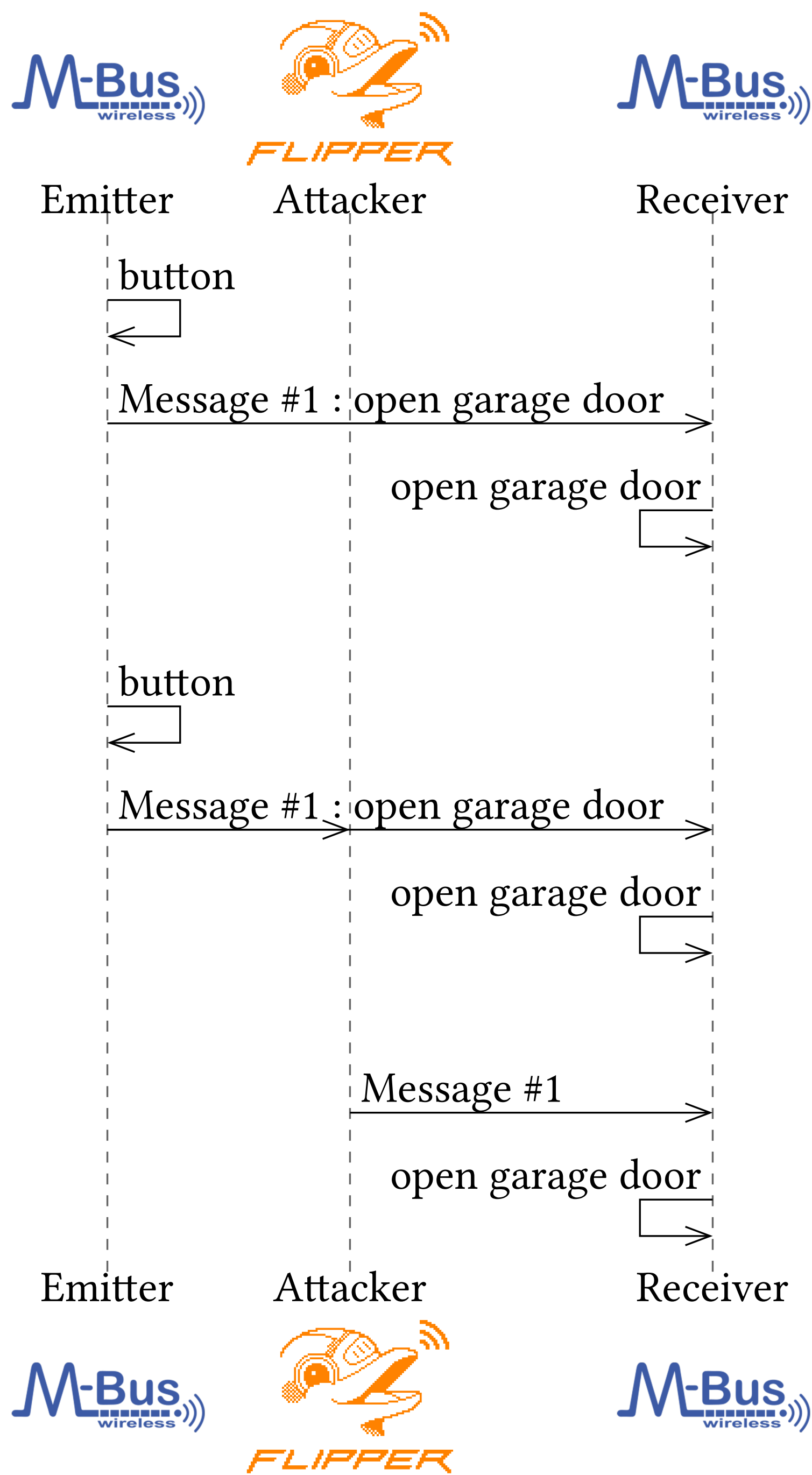
# OT Security

## Context

This thesis, exists 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.

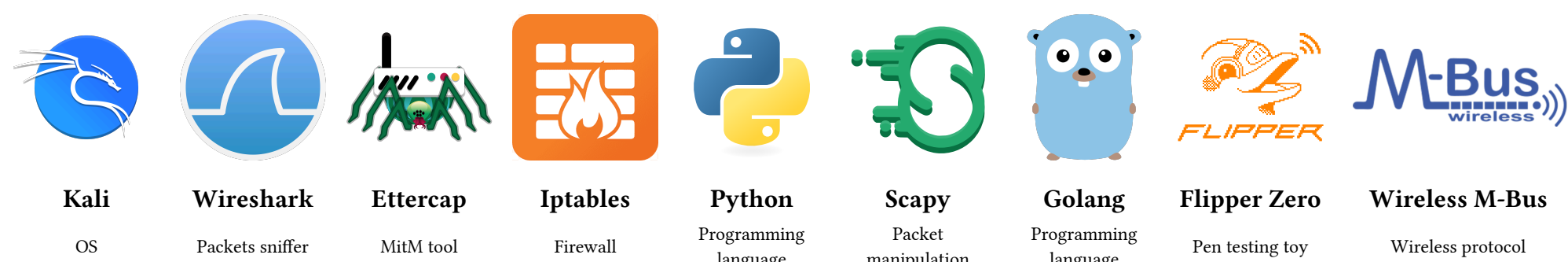
## Replay attack scenario

The replay scenario involves intercepting and resending a wireless message to produce the same effect, like a garage door opening.



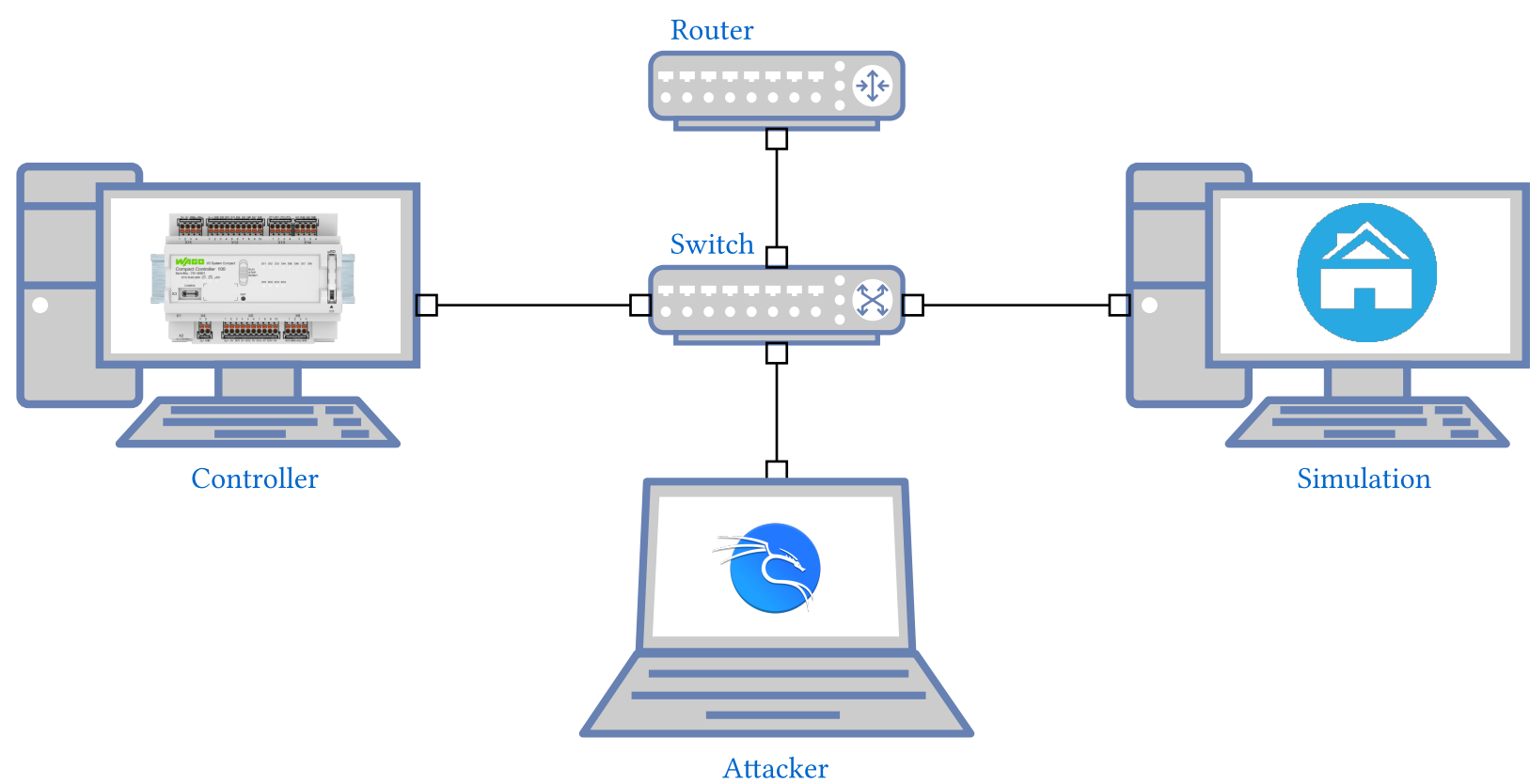
To protect against this attack, the system should integrate a security in the message, like rolling codes or an encrypted counter with a private key.

## Stack



## 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 attack is to intercept the communication between the controller and the installation. To achieve this goal, the attacker can use ARP poisoning attack (1). Once the attacker has intercepted all packets, it is possible to modify them (2). To protect against this attack, the system has to use Modbus over TLS (3).

