Energy effective jamming attacker in wireless networks

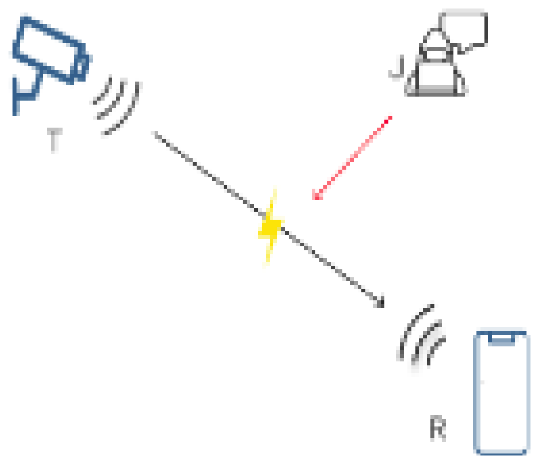
Emilie Bout

Mail: emilie.bout@inria.fr

Supervisors: Valeria Loscri, Antoine Gallais

Introduction

Jamming attack: The goal is to volontary interferences with the legitame channel



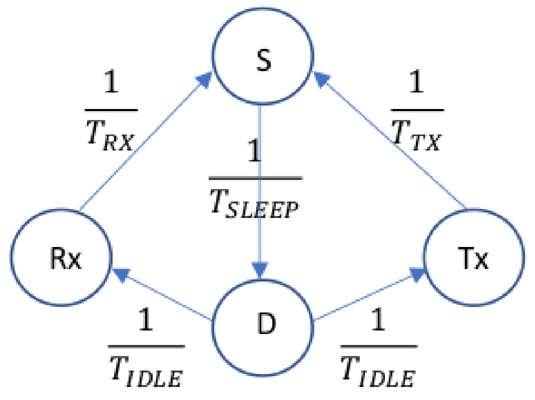
Several strategies exist:

- Constant
- Random
- Reactive

1 Model

The attacker admits 4 states

We derive a framework based on Markov Chain Theroy.



We can compute the probability of staying in each state in order to achieve the following objectives :

1. We give a limitation cost and we compute the maximun of the attack success
2. We give a probabilty of attack success and we compute the minimal associated cost

Aim of the study

Create a new intelligent jamming attack. The jammer maximizes its impact while minimizing its energy consumption

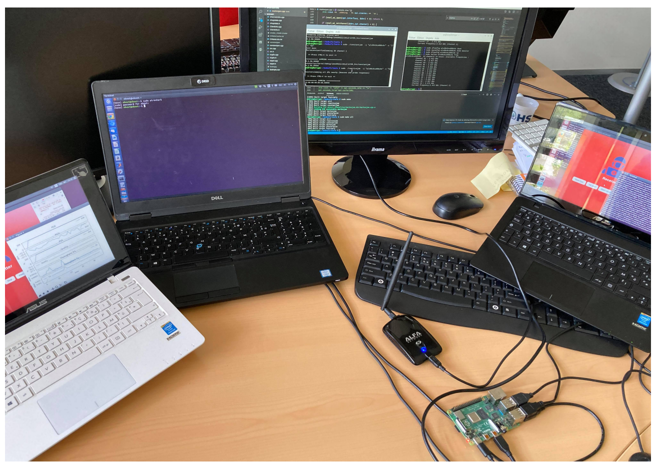
2 Experiments

First study on NS3 simulator, to evaluate several jamming attack parameters.

Then we developed a test-bed. Composed of an attacker and a transmitter / receiver .

We have implemented 3 types of jamming attack: constant, reactive and the one based on the theory of markov chains.

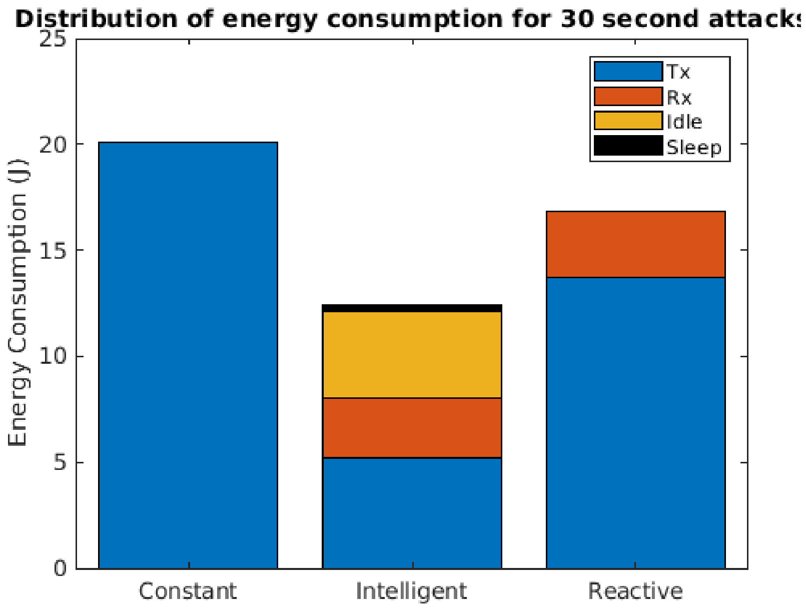
Detection system based on PDR threshold on the transmitter side.

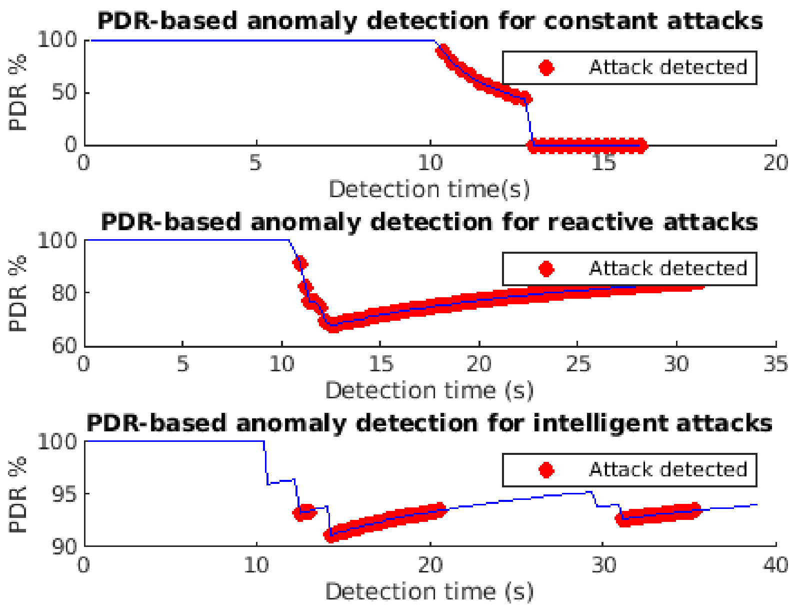


3 Results

Parameters:

- Distance transmitter/Receiver: 10 m
- Start of the attack: after 10 seconds
- Duration of the attack: 30 seconds





- For a cost limited to 60%.
- The strategy based on Markov Chain Theory consumes less energy than the others.
- This strategy is also less detectable
- Reduces the flow by 15%

4 Conclusion

- Adapt to other protocols like bluetooth
- Preliminary work: test this strategy with other configurations
- Easily to create jamming attack with a cheap device