Denial-of-Sleep Attacks

#IotSec

Emilie Bout

Inria Lille-Nord Europe

Mail: emilie.bout@inria.fr

Address: 40 avenue Halley
59650 - Villeneuve d'Ascq - France

WebSite: https://emilie-bout.netlify.app/

Research Interests: Internet-of-things, Security, Routing protocols for Wireless Networks, Machine Learning

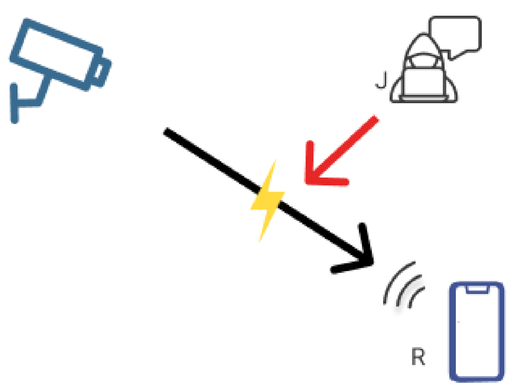
Denial-of-Sleep Attacks on IoT Networks

2 main goals:

Experiment and **create** denial-of-sleep **attacks** to find new vulnerabilities in IoT devices and communication protocols

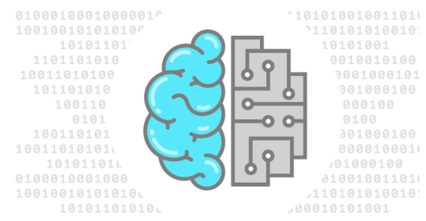
Improve the communication protocols and make them more **robust** against denial-of-sleep attacks

Study on "intelligent" jamming attacks



Current idea:
Creating a jamming attack using machine learning algorithms

If you are expert in these fields:

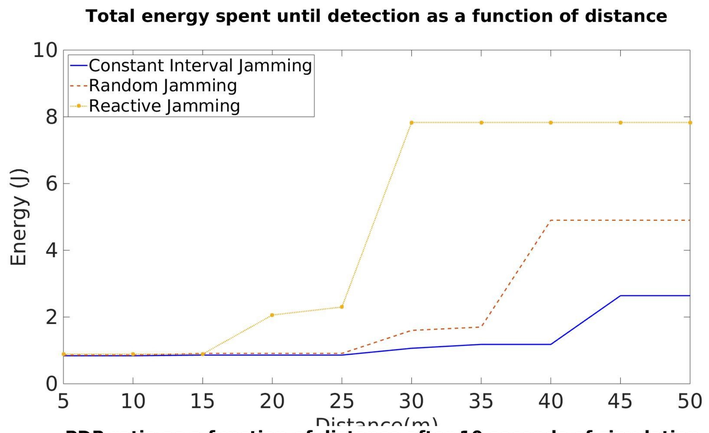


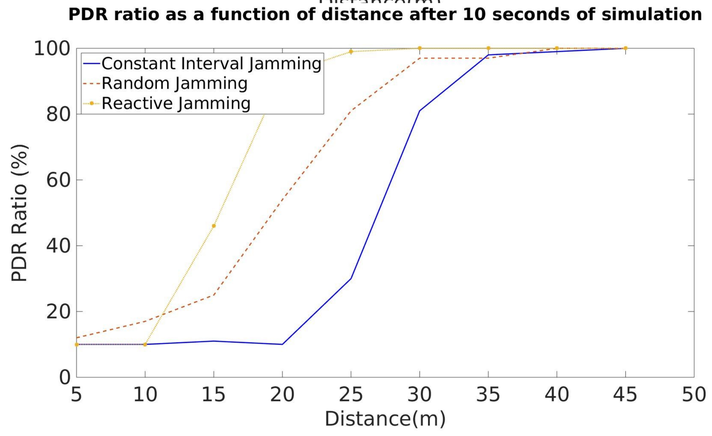
Machine learning

Wifi protocols

ns-3

Preliminary results :





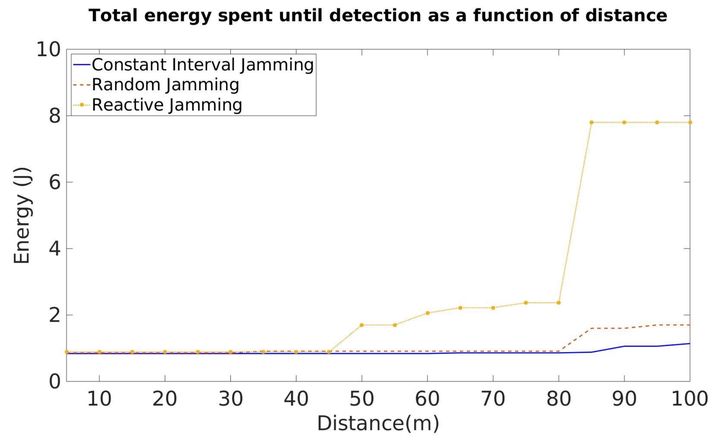
Distance between transmitter and receiver at 20m

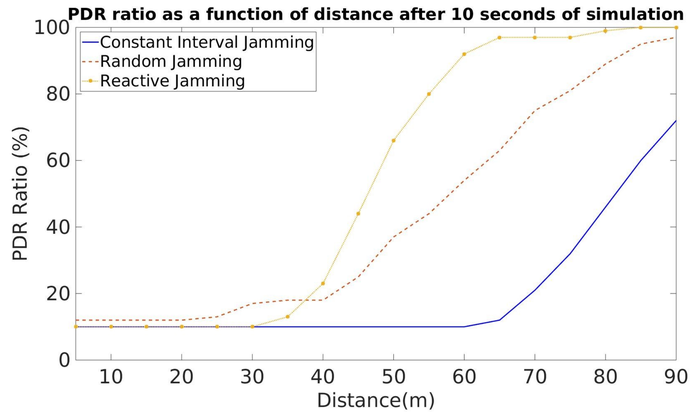
First goal: Evaluate the impacts of jamming attacks according to several parameters taken into account together

3 types of jamming attacks:

- *Constant* Interval Jamming
- *Random* jamming attack
- *Reactive* jamming attack

Conclusion : The choice of optimal strategy depend on several parameters evaluated together





Distance between transmitter and receiver at 60m

IEEE/ACM DS-RT 2020: Bout, E., Loscri, V., & Gallais, A. (2020, September). Energy and Distance evaluation for Jamming Attacks in wireless networks.