When jamming attacks in wireless networks become (too) smart!

Bout Emilie - Loscri Valeria - Gallais Antoine

Summary

01. Introduction

02. Objectives

03. A new smart Jamming Attack

04. Test-bed

05. Demonstration

06. Results

07. Conclusion

01

Introduction

Iot Networks

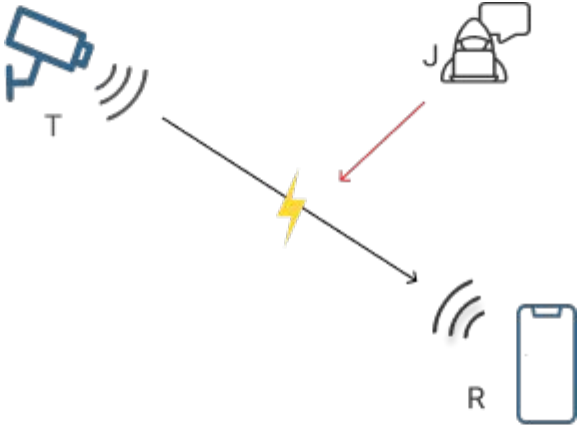
- **Omnipresent** in your live
- Essential roles :
  - Security element: camera, alarm
  - Health object: Pacemaker, insulin pump
- **Constrained in energy** and resources

What is a Jamming Attack ?

“Prevent the exchange of packets between the legitimate nodes of the network”

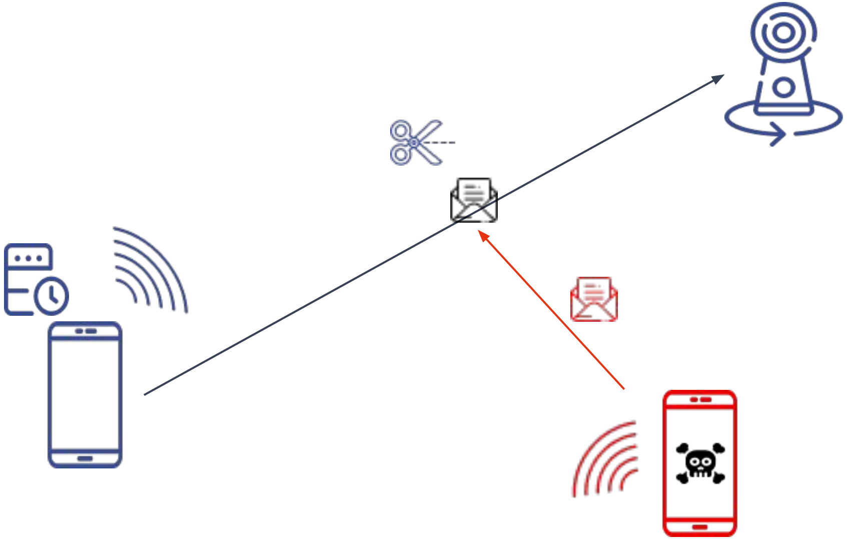
Consequences :

- **Loss** of crucial **information, communication**.
- The **lifetime of a device is reduced.**
- **Decrease in the Quality of Service**.
- Denial-of-Services - Denial-of-Sleep



Transmission under Jamming Attack

Two potential scenarios :



Consequences in Real life ?

- In daily life: your car keys, your home security camera

- **Basis of other attacks**: Spoofing attack, Man in the middle attack ...

02

The objectives

The Objectives

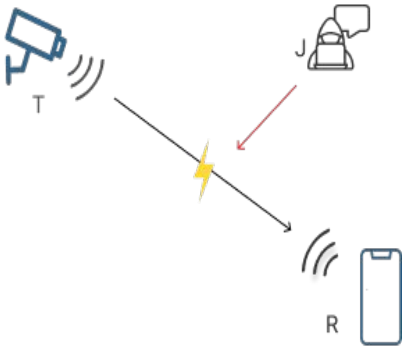
- New solutions based on Machine Learning: more autonomous, more efficient
- More and more attacks based on Machine Learning algorithms
- Study, create this type of attack to better understand them
- Find vulnerabilities in machine learning algorithms to circumvent these attacks
- Jamming attacks can also be an interesting defense.

03

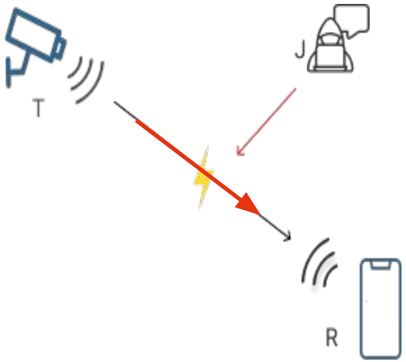
A new smart jamming Attack

Several attack strategies

Constant



Reactive



Successful attack = t_detect + t _jam < t_transmission

Hypothesis:

Jammer node assumptions:

- The attacker has the same WI-FI configuration
- Constrained in energy and resources consumption
- Admits 4 states: Transmission, Receiver, Sleep, Idle

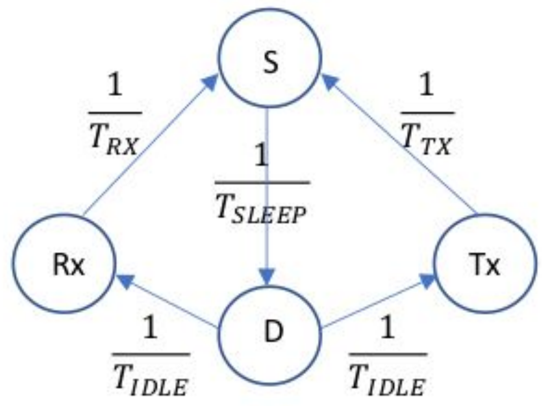
Goals:

- Optimize its impact while minimizing its energy consumptior

- Be as undetectable as possible

System model

- Derive an analytical framework based on Markov Chain Theory
- Attacker Node Model and Transmitter Node Model



$$Q_J = \begin{pmatrix} \frac{-1}{Ts} & \frac{1}{Ts} & 0 & 0 \\ 0 & \frac{-2}{Tidle} & \frac{1}{Tidle} & \frac{1}{Tidle} \\ \frac{1}{Trx} & 0 & \frac{-1}{Trx} & 0 \\ \frac{1}{Ttx} & 0 & 0 & \frac{-1}{Ttx} \end{pmatrix}$$

System model

Goals:

- **Compute the probability of staying in each state in order to achieve the following objectives:**
  - Maximization of the attack effectiveness by minimizing the energy consumption

    Given a certain limitation cost , the maximization of the probability that the attack is occurring in a certain time interval
  - By imposing a threshold in terms of probability the attack occurs in a certain interval time, we minimize the associated cost

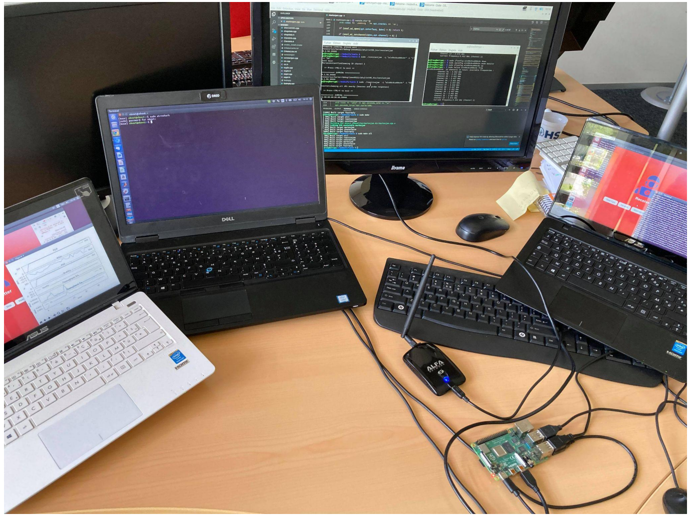
04

The test-bed

Description of the test bench :

Composition:

- One pair of transmitter and receiver
- Raspberry Pi with Alfa device and Atheros Drivers and Firmware.



The attacker system :

- **3 types** of jamming attack implemented:
  - Constant
  - Reactive
  - Markov

- Compute the **energy consumption** for each attack.

The Detection system

Metric used :

- Packet Delivery Ratio(**PDR**) on the transmitter side with ACK packet:

$$\text{PDR} = \frac{\text{Total packets successfully received}}{\text{Total packets send}}$$

Detection Method:

- **Detection using a threshold :**
  - If the PDR metric is lower than the defined threshold, an attack is detected
  - Number of observations

05

Demonstration

Demonstration

Demonstration

Demonstration

06

Results

Parameters:

Distance transmitter -Receiver	1 m
Start of the attack	after 20 seconds
Duration of the attack	30 seconds

Number of corrupted packets

Type of Attack	Packet Error Rate
Constant	0%
Reactive	6%
Markov	31%

Detection time

Type of Attack	Detection time (seconds)
Constant	9
Reactive	-
Markov	13

Energy Consumption

Type of attack	Energy Consumption (Joules)
Constant	20.1
Reactive	13.5
Markov	10.5

Results:

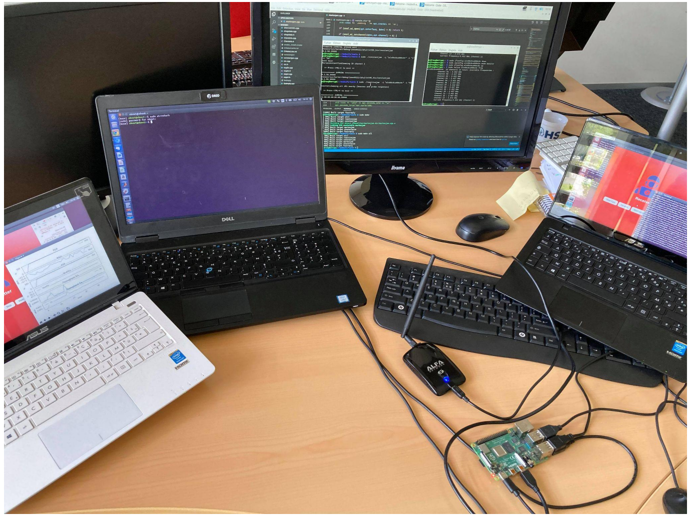
- Consumes less energy than other attacks
- Greatest impact on the PDR and PER
- Reduce the flow by 15%

07

Conclusion

Discussion & Conclusion

- Adapt to other protocol
- Easily to create jamming attack



Thank you !

Any questions ?