Power-Efficient Jamming attacks in wireless network

Emilie Bout - Valeria Loscri - Antoine Gallais

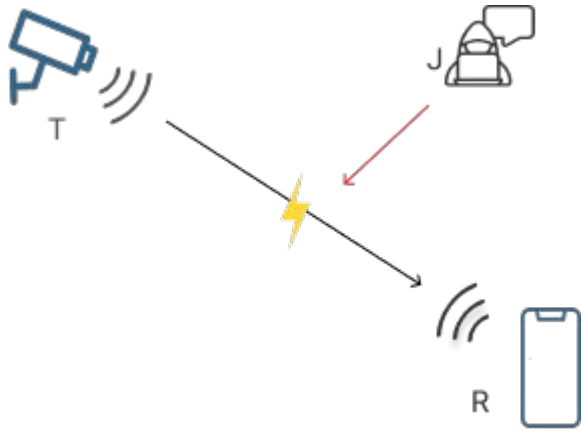
Summary

01

Introduction

Goal of Jamming Attack ?

“Prevent the exchange of packets between the legitimate nodes of the networks.”

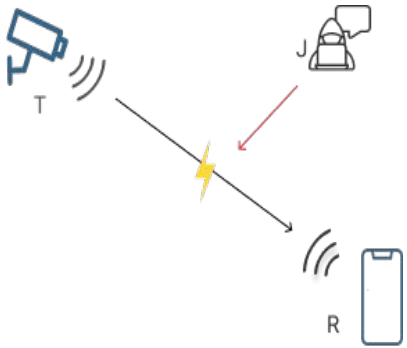


Consequences :

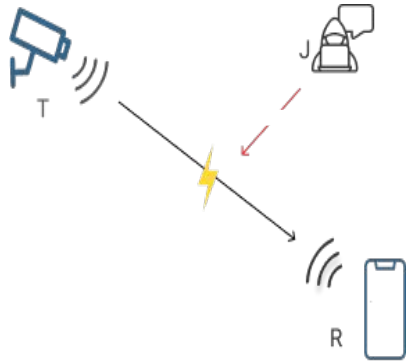
- A **loss** of crucial **information**, **communication**.
- The **lifetime of a device is reduced.**
- A **decrease in the Quality of Service**.
- Denial-of-Services, Denial-of-Sleep

Several attack strategies

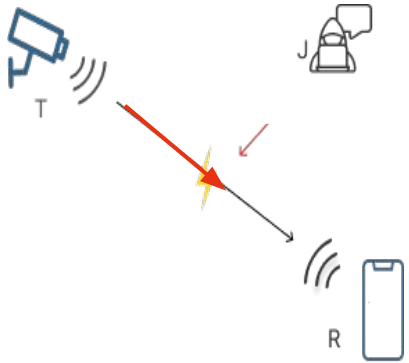
Constant



Random



Reactive



02

Strategy based on Markov theory

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

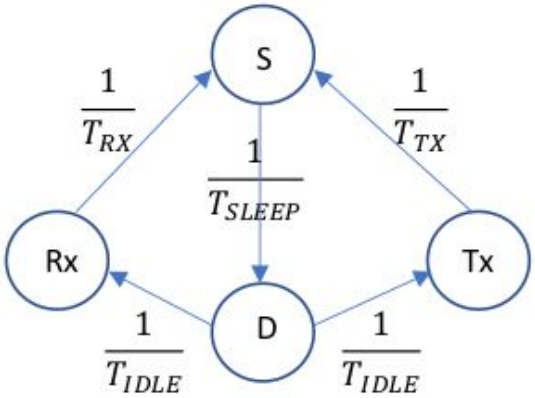
Goal:

- Optimize its impact while minimizing its energy consumption.

- Be as undetectable as possible

System model

- Derive an analytical framework based on Markov Chain Theory
- Attacker Node Model (ANM)



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

System model

Interaction Attacker Transmitter Model (IATM)

- Interaction between the attacker node and the transmitter node
- The transmitter alternate between the four different states
- F(IATM) = F(J) * F (Tx)
- The matrix of the state transitions rate Q(IATM) is a matrix 16 * 16.

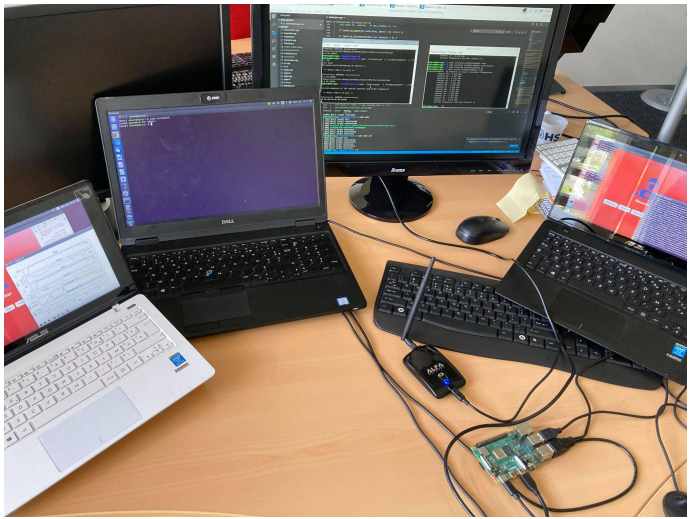
04

Experiments in a test-bed

Test-bed:

Composition:

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



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

Detection system

Detection system:

Detection system based on PDR threshold in transmitter side

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

Attacker System

- Compute the energy consumption

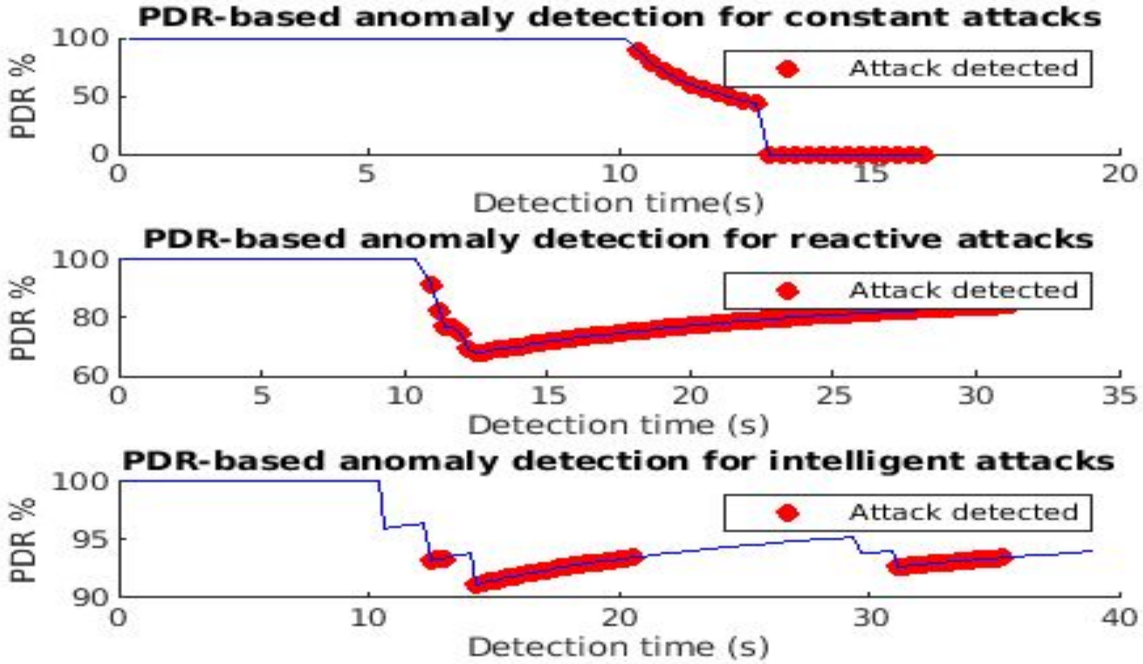
- 3 types of attack implemented:
  - Constant
  - Random
  - Markov

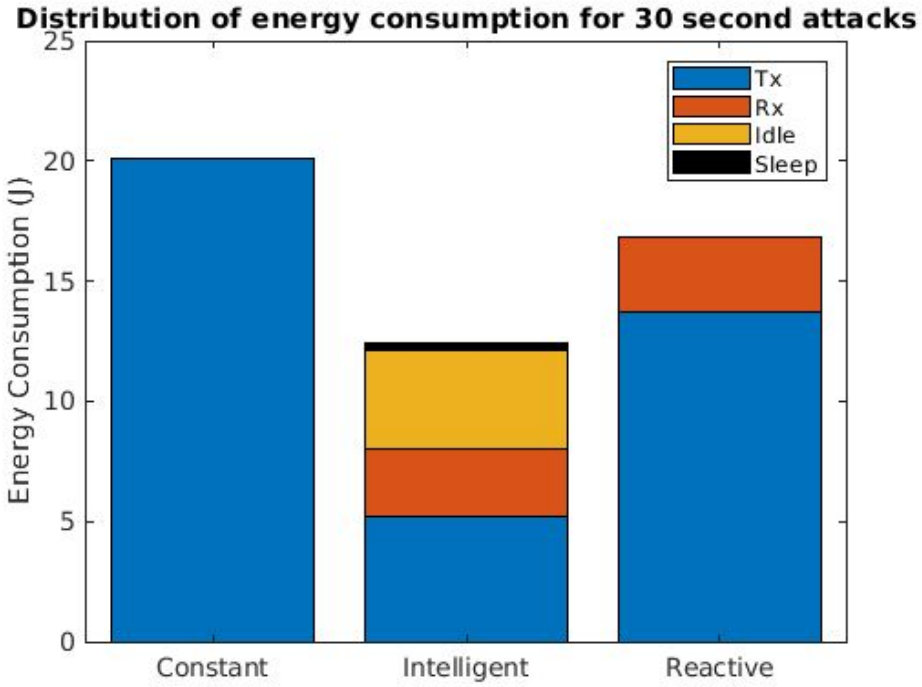
04

Results

Parameters:

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


PDR-based anomaly detection for constant attacks
PDR %
100
50
0
0
5
10
15
20
Detection time(s)
Attack detected
PDR-based anomaly detection for reactive attacks
PDR %
100
80
60
0
5
10
15
20
25
30
35
Detection time (s)
Attack detected
PDR-based anomaly detection for intelligent attacks
PDR %
100
95
90
0
10
20
30
40
Detection time (s)
Attack detected


Distribution of energy consumption for 30 second attacks
Energy Consumption (J)
0
5
10
15
20
25
Tx
Rx
Idle
Sleep
Constant
Intelligent
Reactive

Results:

- Consumes less energy than other attacks
- Impact of the PDR
- Reduce the flow by 15%

06

Conclusion

Discussion & Conclusion

- Preliminary work: other configurations
- Adapt to other protocol
- Easily to create jamming attack

Thank you !

Any questions ?

emilie.bout@inria.fr