

IEEE/ACM DS-RT2020

Energy and Distance evaluation for  
Jamming Attacks in wireless networks

# Summary

01. Introduction
02. Objectives
03. System model
04. Results
05. Conclusion

# 01

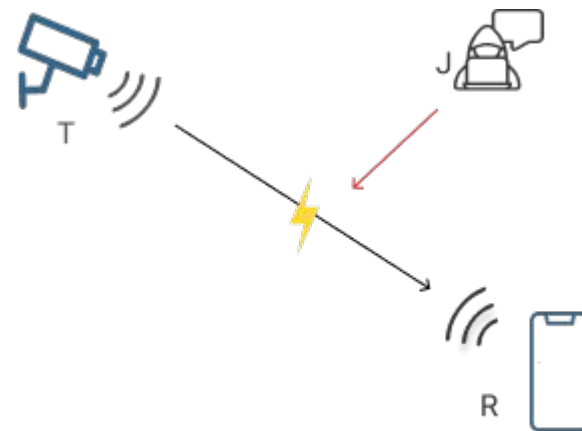
## Introduction

# Goal of Jamming Attack ?

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

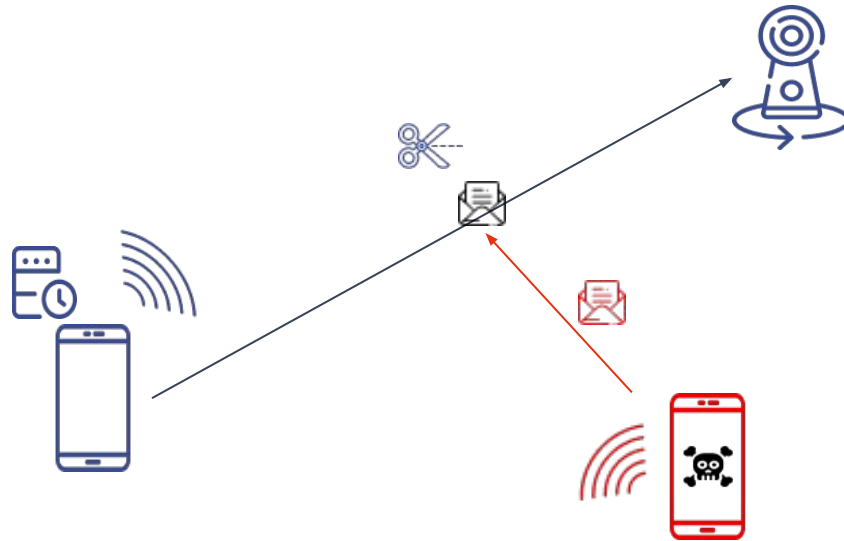
## Consequences :

- 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



# Transmission under Jamming Attack

Two potential scenarios :



# 02

## Objectives

# The objectives of this work:

## The study objectives of jamming attacks:

- Better understand vulnerabilities
- Create more robust communications protocols, effective detection and protection systems
- Better understand the location of jamming node problem.

## Related works:

- **REF1:** Ashraf, Qazi Mamoon, Mohamed Hadi Habaebi, and Md Rafiqul Islam. "Jammer localization using wireless devices with mitigation by self-configuration." *Plos one* 11.9 2016 . .
- **REF2:** Panyim, Korporn, et al. "On limited-range strategic/random jamming attacks in wireless ad hoc networks." *2009 IEEE 34th Conference on Local Computer Networks*. IEEE, 2009.
- **REF3:** Commander, Clayton W., et al. "Jamming communication networks under complete uncertainty." *Optimization Letters* 2.1 (2008): 53-70.
- **REF4:** Li, Mingyan, Iordanis Koutsopoulos, and Radha Poovendran. "Optimal jamming attacks and network defense policies in wireless sensor networks." *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*. IEEE, 2007.

# Hypothesis:

## Jammer node assumptions:

- Constrained in energy and resources consumption
- Optimize its impact while minimizing its energy consumption.

## Evaluation of many parameters together:

- energy consumption spent
- jamming efficiency
- probabilities of being detected



# 03

## System model

# Simulation Details



## Strategies of Jamming attacks:

Parameters	Constant Jammer	Random Jammer	Reactive Jammer
Send interval(ms)	1	Between 100 and 1	Send interval of the legitimate node

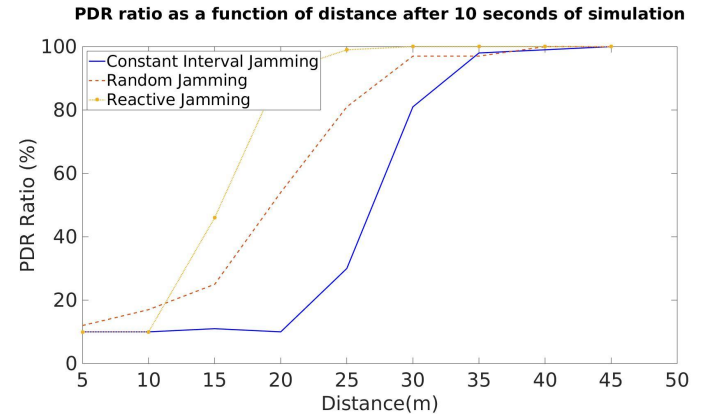
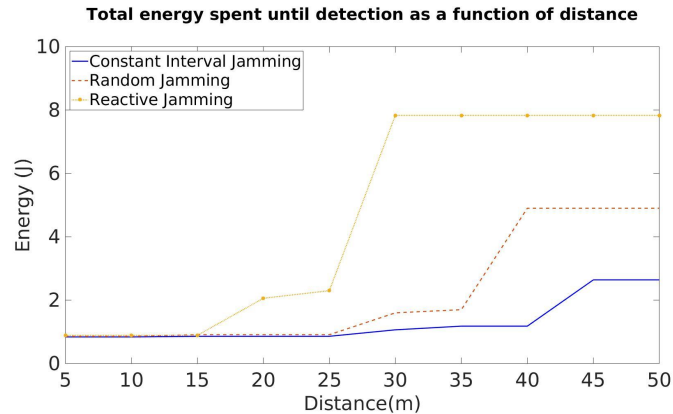
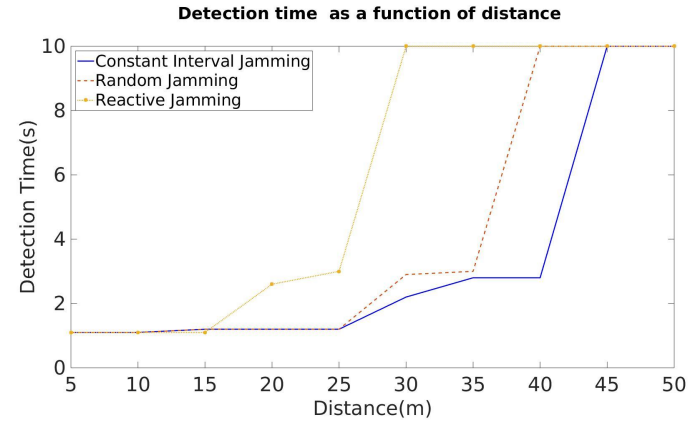
## Factors taken into account:

- energy
- detection time
- impact on the networks
- the distance between the transmitter and the attacker
- the distance between the transmitter and receiver.

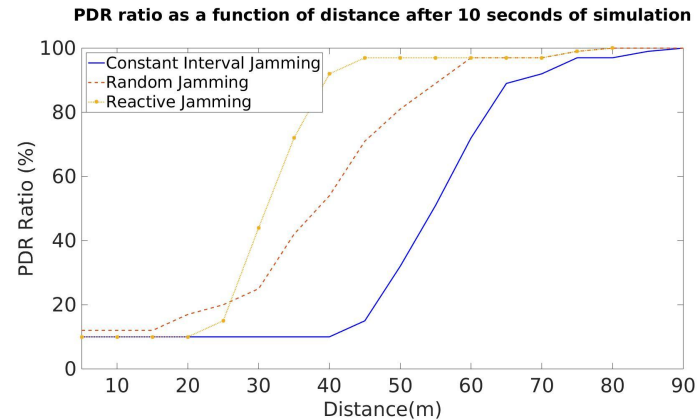
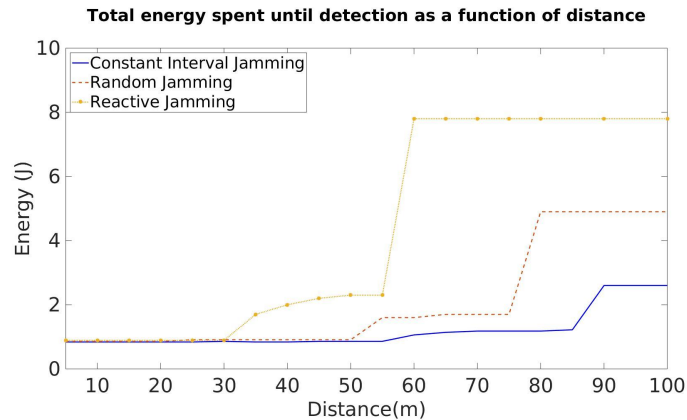
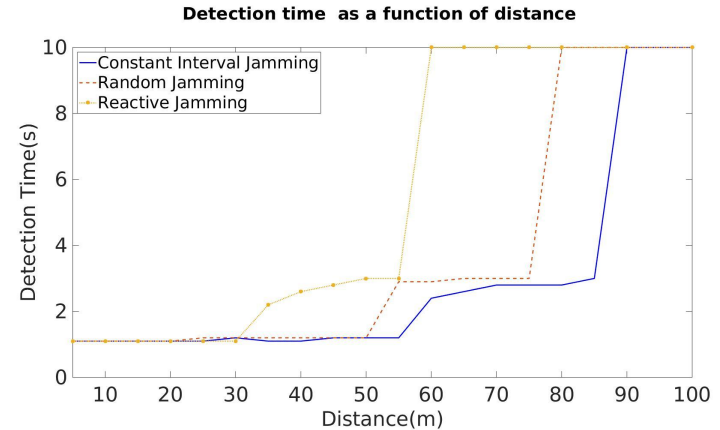
# 04

## Results

Distance between transmitter and receiver	20 m
Detection threshold	99%
Start time of detection and jamming attack	1 s



Distance between transmitter and receiver	60 m
Detection threshold	99%
Start time of detection and jamming attack	1 s



# Results:

**The choice of optimal strategy depends on many parameters:**

- Position of the jammer
- Energy consumption
- Detection probability

# 06

## Conclusion

# Discussion & Conclusion

## Work completed:

- The choice of optimal strategy depend on several parameters evaluated together

## Future works:

- Simulation performed under optimal conditions: detection threshold 99%.
- Conduct the same evaluation with a multitude of victim nodes
- Creation of “intelligent” jammer which chooses strategy according to evaluated parameters



# Thank you !

Any questions ?

[emilie.bout@inria.fr](mailto:emilie.bout@inria.fr)

Distance between transmitter and receiver	40 m
Detection threshold	99%
Start time of detection and jamming attack	1 s

