Energy effective jamming attacker in wireless network
Summary

01. Introduction
02. Strategy based on Markov Chain theory
04. Experiments
05. Results
06. Conclusion
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
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)
Strategy based on Markov Model

System model

Interaction Attacker Transmitter Model (IATM)

- Interaction between the attacker node and the transmitter node
- The transmitter alternate between the four different states
- \( F(IATM) = F(J) \times F(Tx) \)
- The matrix of the state transitions rate \( Q(IATM) \) is a matrix 16 * 16.
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
Experiments in a test-bed
Test-bed:

Composition:

- One pair of transmitter and emitter
- Raspberry Pi with Alfa device and Atheros Drivers and Firmware
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
Results
## Parameters:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance transmitter - Receiver</td>
<td>10 m</td>
</tr>
<tr>
<td>Start of the attack</td>
<td>after 10 seconds</td>
</tr>
<tr>
<td>Duration of the attack</td>
<td>30 seconds</td>
</tr>
</tbody>
</table>
Results

PDR-based anomaly detection for constant attacks

PDR-based anomaly detection for reactive attacks

PDR-based anomaly detection for intelligent attacks
Distribution of energy consumption for 30 second attacks

Energy Consumption (J)

Constant  Intelligent  Reactive

Tx  Rx  Idle  Sleep
Results:

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

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

Any questions?

emilie.bout@inria.fr