Università di Genova
DIBRIS DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

Electronic Attacks as a Cyber False Flag against Maritime Radars Systems

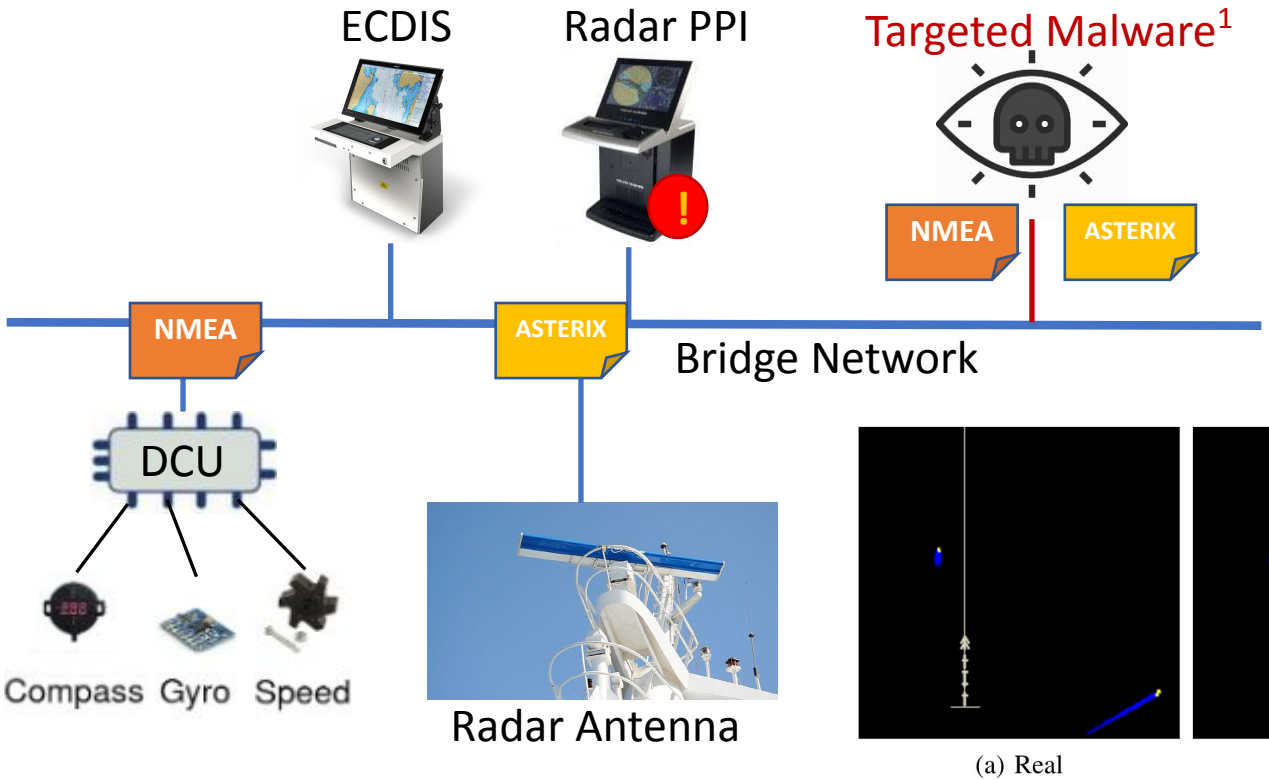
Giacomo Longo, Alessio Merlo, Alessandro Armando, Enrico Russo

5 Oct 2023, 1st IEEE LCN Workshop on Maritime Communication and Security (MarCaS)

Università di Genova
DIBRIS DIPARTIMENTO
DI INFORMATICA, BIOINGEGNERIA,
ROBOTICA E INGEGNERIA DEI SISTEMI

Background and motivation

Layout of a modern bridge



[1]Longo, G., Russo, E., Armando, A., & Merlo, A. Attacking (and defending) the maritime radar system. IEEE Transactions on Information Forensics and Security.

Elevating Sophistication to New Heights

Currently, we focus *just* on **disrupting operations**

What if we wanted an attack which:

1. Misrepresents its cyber nature
2. Has misleading attribution
3. Projects power on behalf of its attributed perpetrators

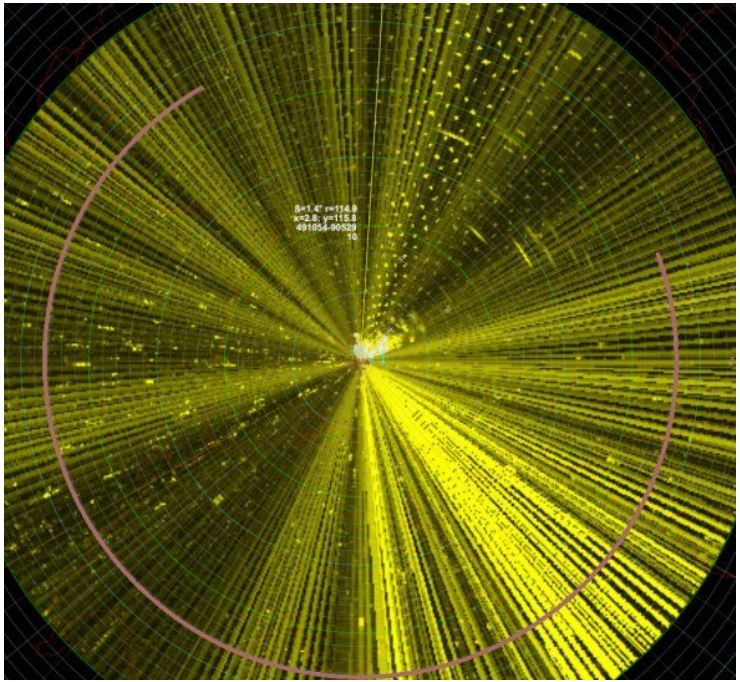
We want a **false flag attack** but in the **cyber space**

Cyber False Flags against maritime radar systems

Deceiving about their nature

Electronic Countermeasures (ECM), aim at disrupting radars, and are some of the most advanced and complex electronic warfare techniques.

Each ECM has also an associated *aesthetic* which **we can reproduce**



Cyber False Flags against maritime radar systems

Misleading attribution

W.r.t. real world ones, **cyber attacks** do not need to abide to physical laws.

There is no need for receiving or sending signals in the air.
It can be executed from **everywhere** and blame any nearby scapegoat.

Cyber False Flags against maritime radar systems

Projecting power

A **cyber attack** can write with precision everywhere.

Like an **infinitely powerful** ECM.

Università di Genova
DIBRIS DIPARTIMENTO
DI INFORMATICA, BIOINGEGNERIA,
ROBOTICA E INGEGNERIA DEI SISTEMI

Attacks

Attacks

Baseline

ASTERIX 240 from MaCySTe's default "Ligurian Sea" scenery [1].
24 rpm, 4096 sweeps, 4096 cells.

[1] Longo, G., Orlich, A., Musante, S., Merlo, A., & Russo, E. (2023). MaCySTe: A virtual testbed for maritime cybersecurity. SoftwareX, 23, 101426.

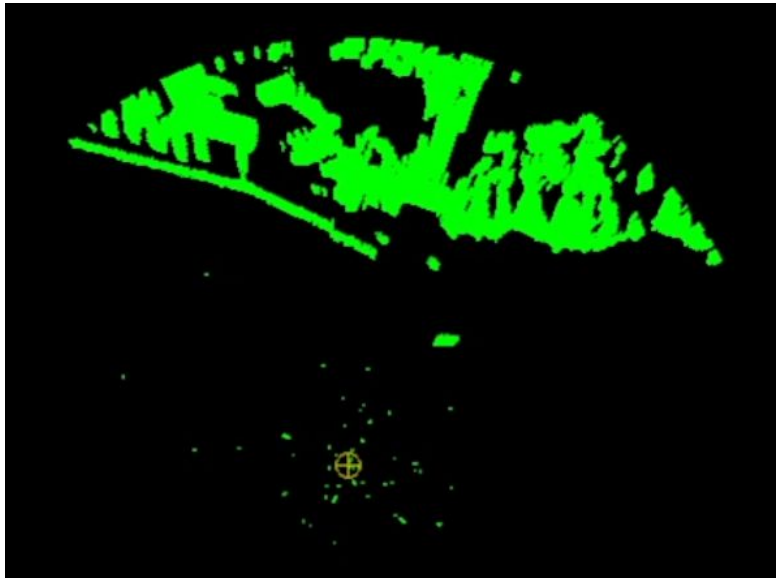
Attacks

Barrage Jamming

Flooding the display with noise.

In the real world, the radar bandwidth is filled with an high-energy noise.

Which means that it's not going to be uniform!

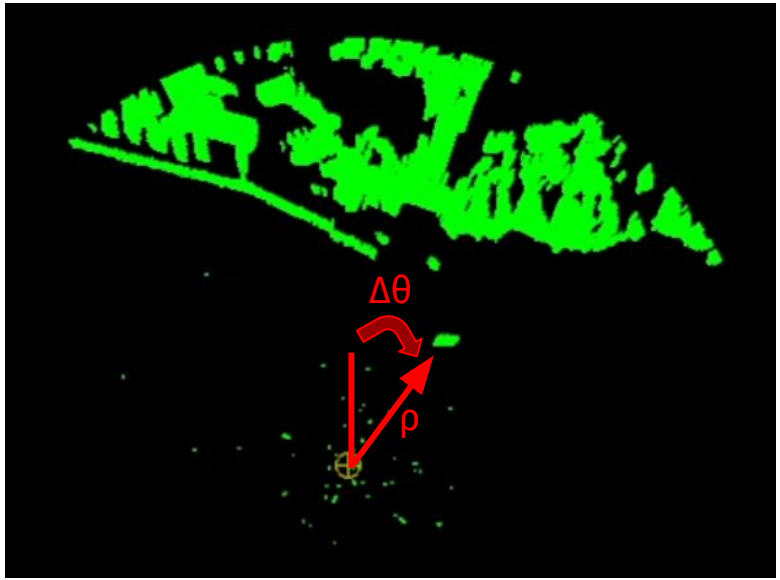


Attacks

Barrage Jamming

Scapegoat is at an angle Δθ, and at a distance ρ

To have a realistic-looking we need to emulate the physics involved. At a low computational cost.



Attacks

Barrage Jamming

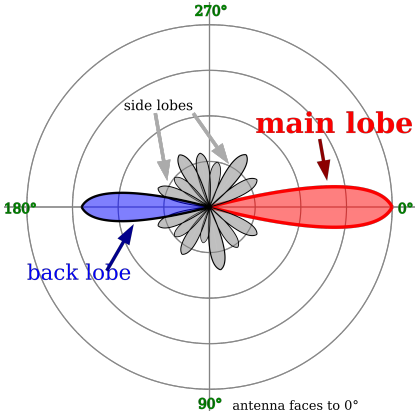
It's noise that we are adding in particular **Gaussian White Noise**

$$AI(\rho, \theta) := z \cdot S(|\Delta_\theta|) \cdot \left(1 - \min\left[1, \frac{|\rho_j - \rho|}{D}\right]\right)$$

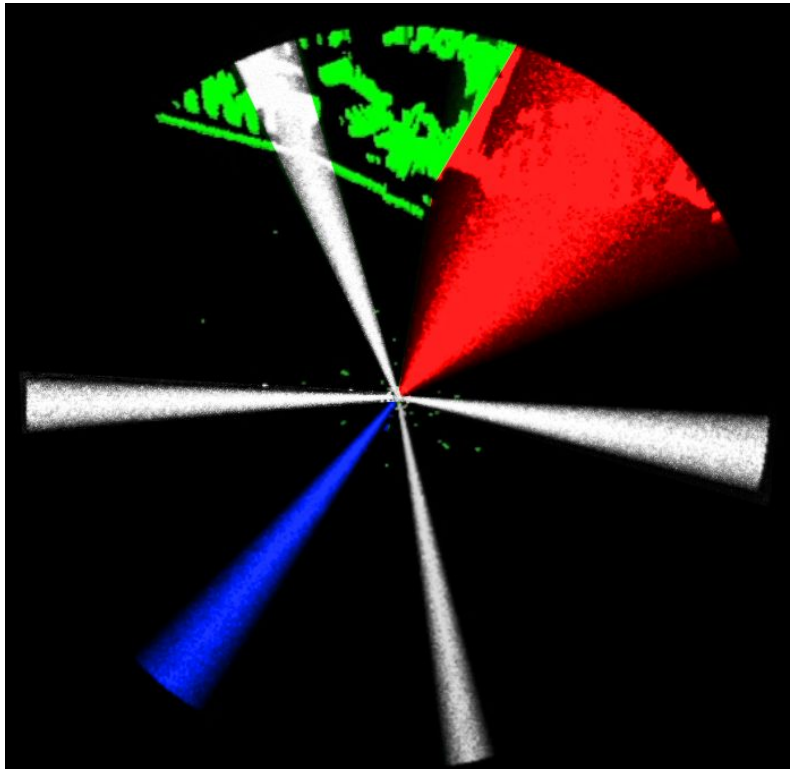
Attacks

Barrage Jamming

Antennas are **directional**



$$AI(\rho,\theta) := z \cdot \boxed{S(|\Delta_\theta|)} \cdot \left(1 - \min\left[1, \frac{|\rho_j - \rho|}{D}\right]\right)$$



Attacks

Barrage Jamming

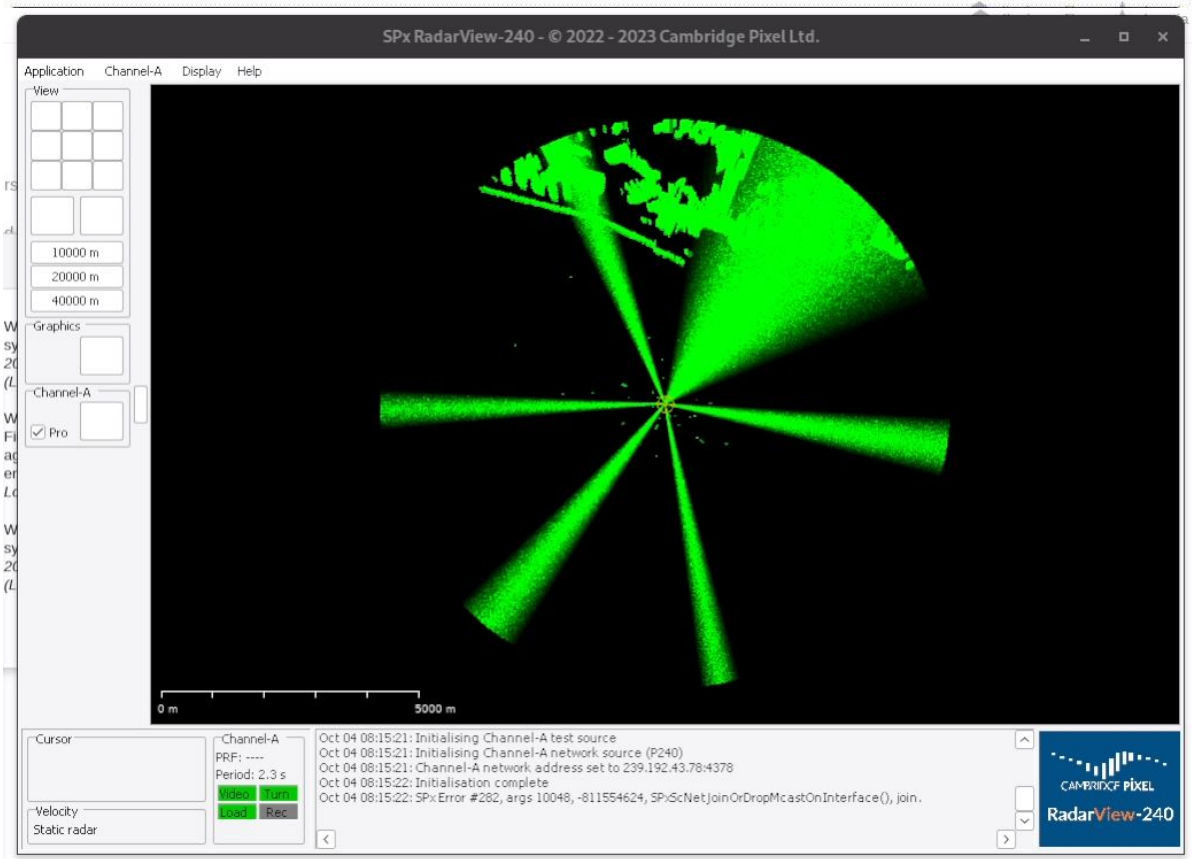
Power fades with **distance**

$$AI(\rho, \theta) := z \cdot S(|\Delta_\theta|) \cdot \left(1 - \min\left[1, \frac{|\rho_j - \rho|}{D}\right]\right)$$

Attacks

Barrage Jamming

Effect clearly denotes the scapegoat as the source, with power density reducing as it goes further away

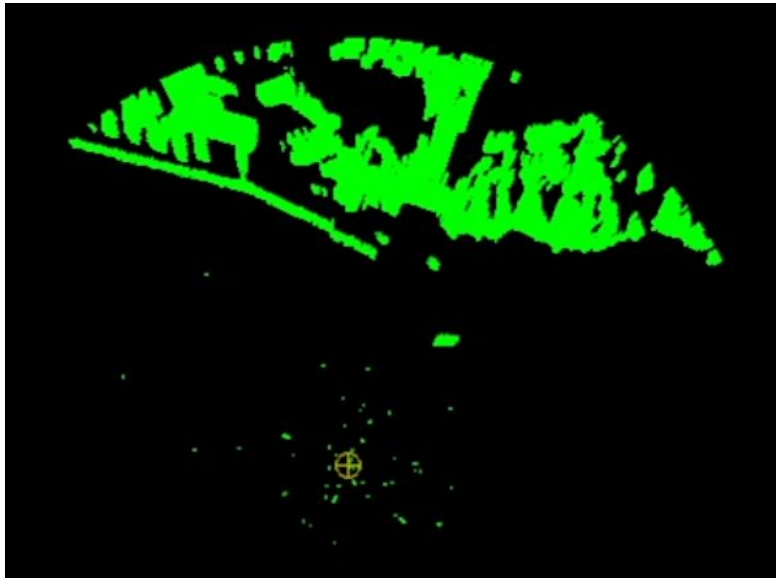


Attacks

Spot Jamming

Flooding a spot on the display with noise.

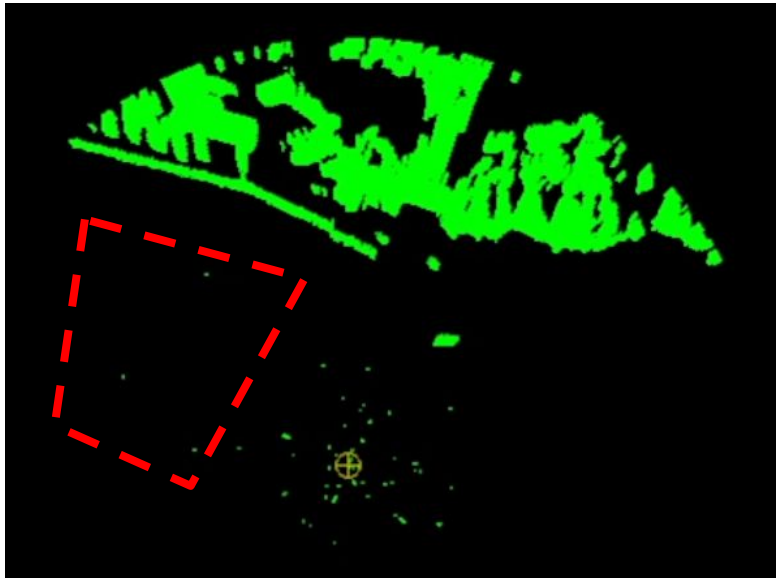
It's the sophisticated cousin of barrage jamming



Attacks

Spot Jamming

Attackers pick an area which they want to affect.

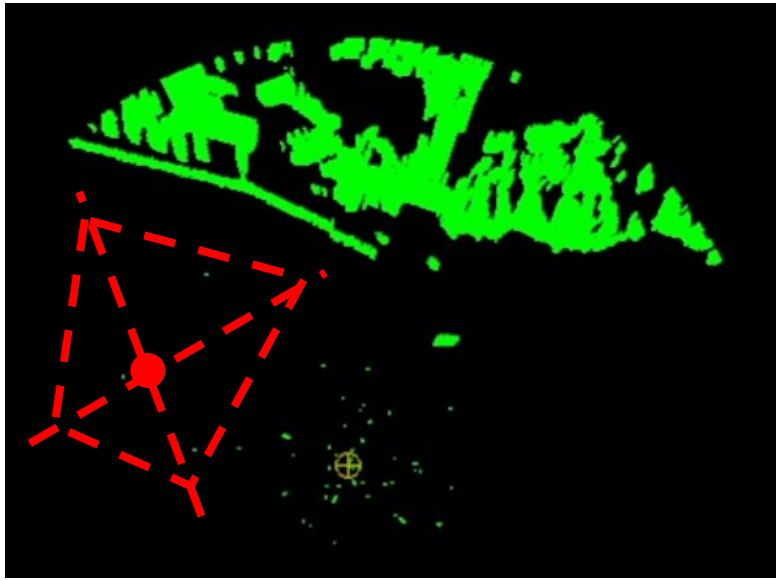


Attacks

Spot Jamming

We simulate similarly to barrage jamming but with the **center of the area as its source**

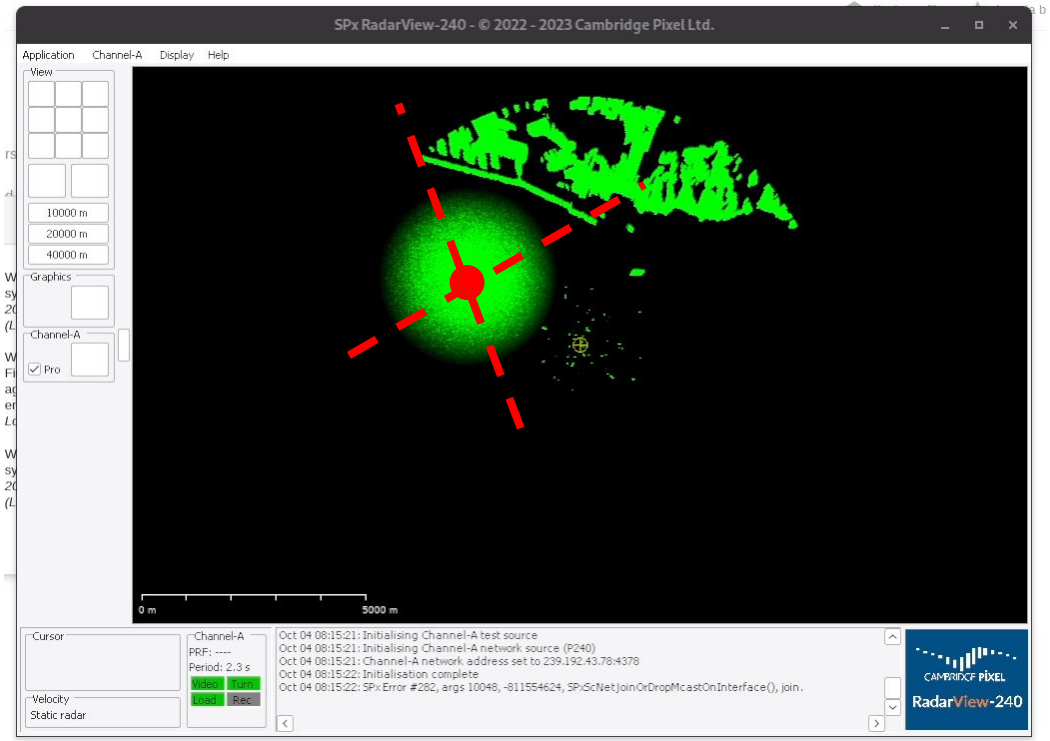
```
1 foreach Packet do
2 |  mod ← false
3 |  foreach Cell ∈ Packet do
4 |  |  if Cell.ctr ∈ Poly then
5 |  |  |  ai ← AI(Cell.ctr.ρ, Cell.ctr.θ)
6 |  |  |  if ai > ϵ then
7 |  |  |  |  Cell.illumination += ai
8 |  |  |  |  mod ← true
9 |  if mod then Send(Packet)
```



Attacks

Spot Jamming

The jamming target is easily distinguishable



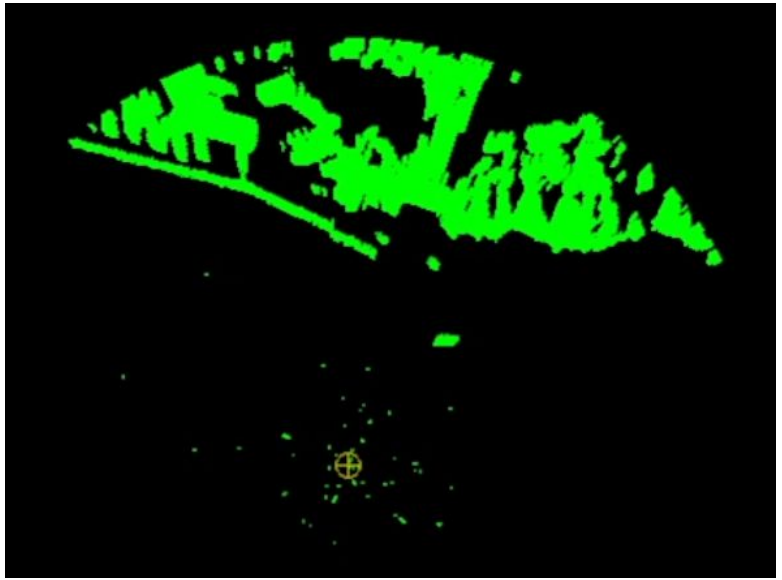
Attacks

Digital Radio Frequency Memory

Results in the duplication of existing echoes, in different positions.

In reality it consists of rapidly replaying received signals

In the cyber domain, it's an image copy operation

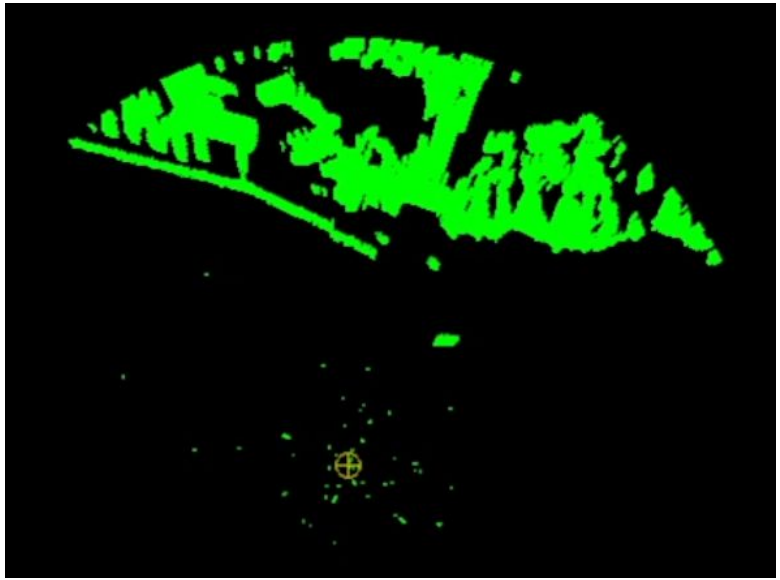


Attacks

Digital Radio Frequency Memory

Simulating DRFM involves

1. Finding which echoes are to be copied
2. Injection of the copies



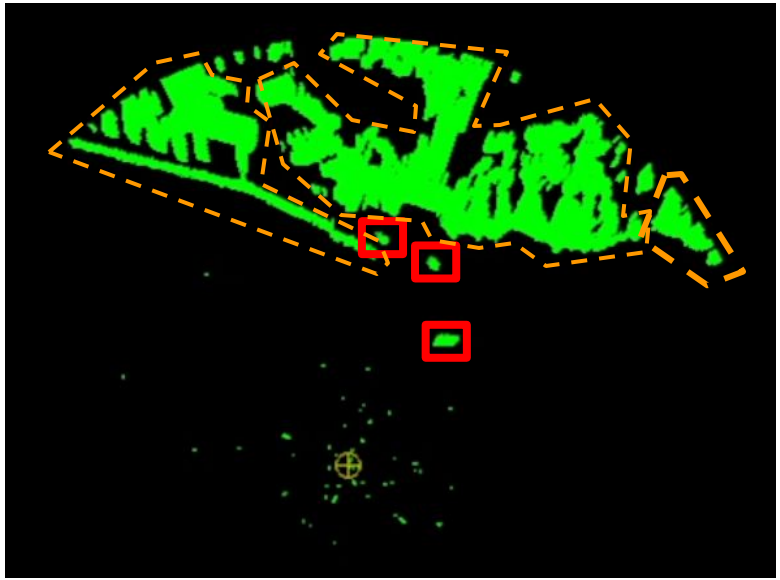
Attacks

Digital Radio Frequency Memory

Finding which echoes are to be copied can be done by applying Constant False Alarm Rate techniques to individuate blobs

Algorithm 2: Constant False Alarm Rate (CFAR)

```
Data: i, w, G
cellUnderTest ← Cells[i]
sum ← 0
for j ← 1; j <= w do
    if Cells[i-G-j] > cellUnderTest or
    Cells[i+G+j] > cellUnderTest then
        return false
    sum += Cells[i-G-j] + Cells[i+G+j]
return sum/2w < cellUnderTest
```

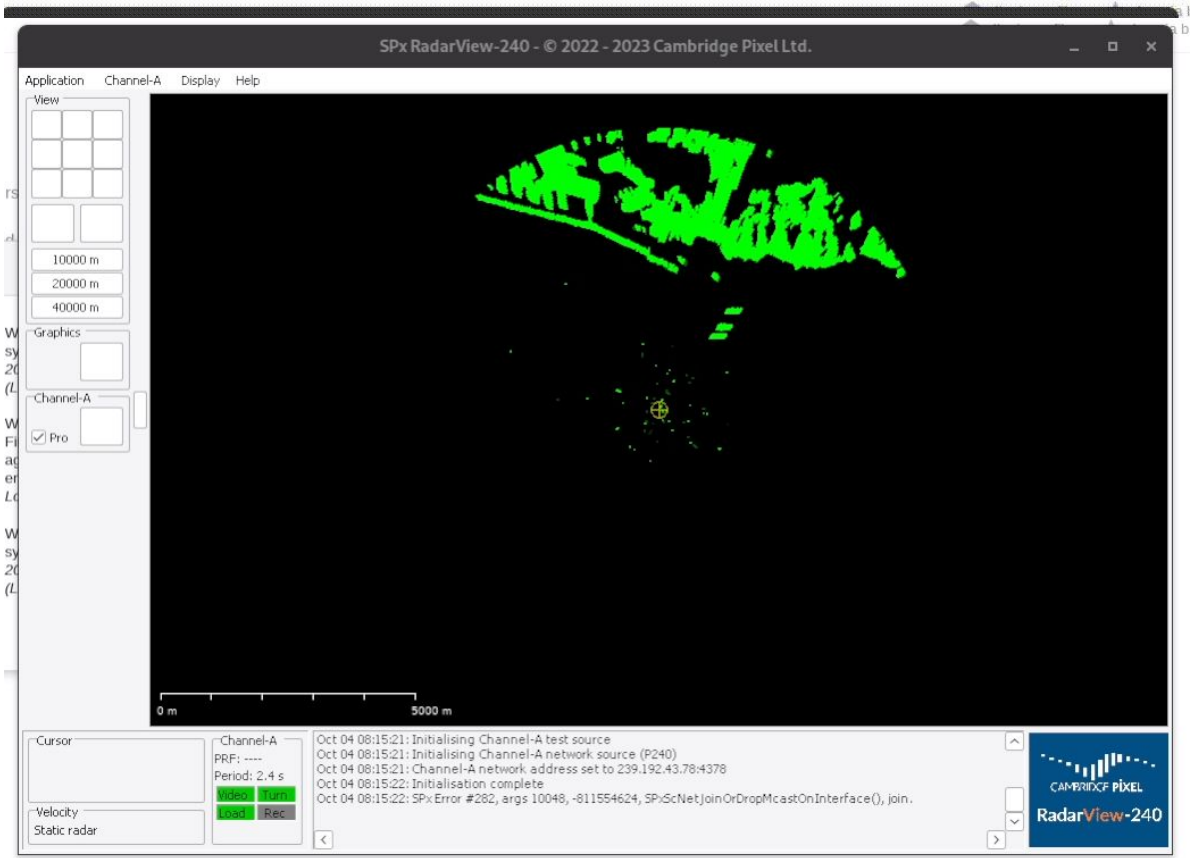


... and **discarding** those that are too big

Attacks

Digital Radio Frequency Memory

Here, two replicas are added. One ahead and one behind of the scapegoat



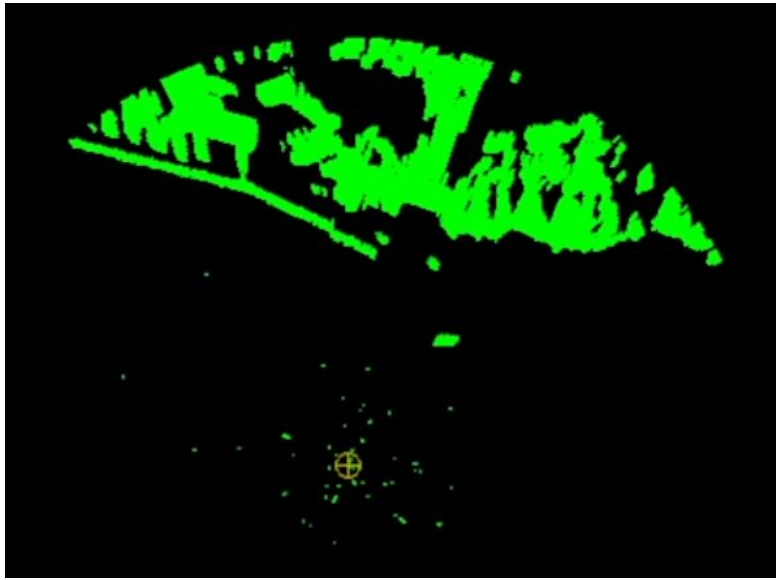
Attacks

Blip Enhancement

Blip enhancement enlarges the received blip in order to confuse about the target location, and its size

In reality, implementation varies from simple radar reflectors to DRFM-like techniques.

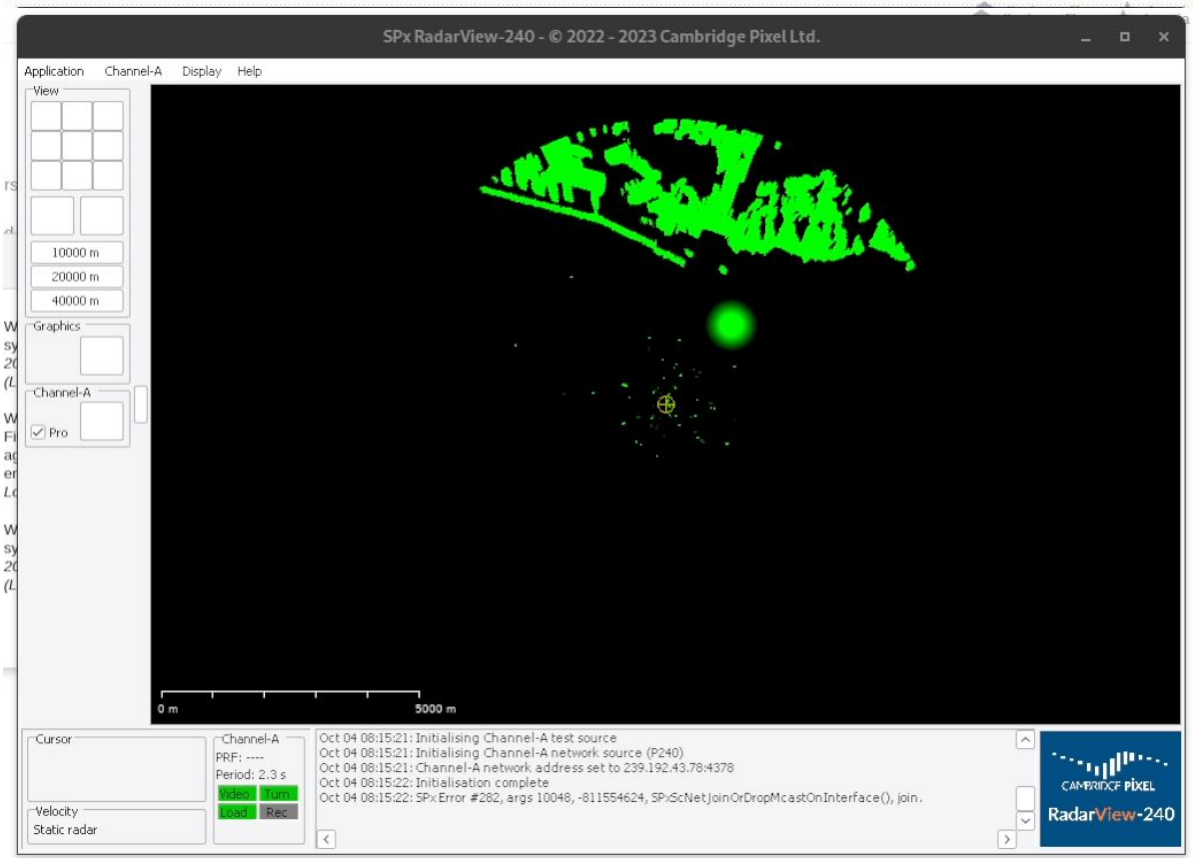
We can simulate it as a target-centered spot jamming



Attacks

Blip enhancement

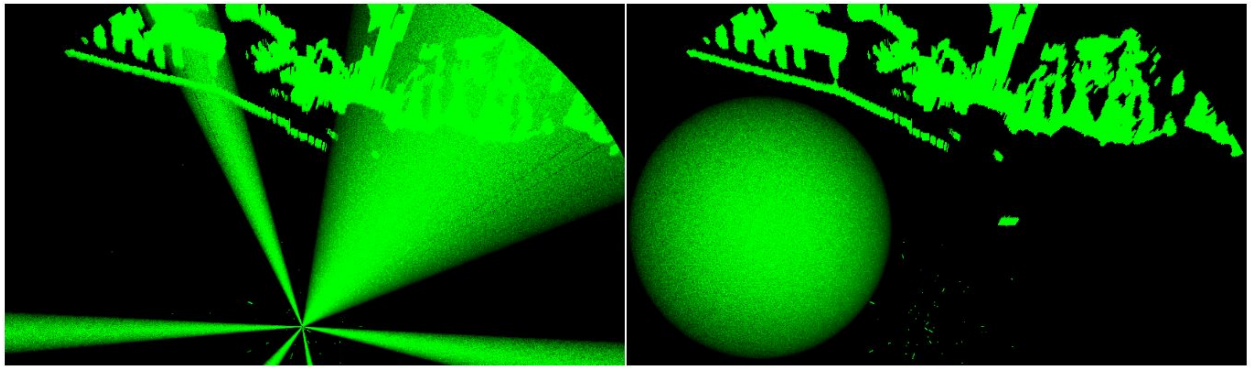
Here, the target extent and true position are concealed by the attack



Università di Genova
DIBRIS DIPARTIMENTO
DI INFORMATICA, BIOINGEGNERIA,
ROBOTICA E INGEGNERIA DEI SISTEMI

Closing remarks

Qualitative appearance considerations



(a) Barrage jamming.

(b) Spot jamming.

(c) Digital Radio Frequency Memory.

(d) Blip enhancement.

Performance considerations

Attack	Traffic increase (%)	CPU (%)	RAM (KiB)
Barrage jamming	45.42	15.1	79.6
Spot jamming	21.51	4.8	79.5
DRFM	2.25	2.9	79.9
Blip enhancement	7.83	3.8	79.6

Traffic increase considerations

Attack	Traffic increase (%)	CPU (%)	RAM (KiB)
Barrage jamming	45.42	15.1	79.6
Spot jamming	21.51	4.8	79.5
DRFM	2.25	2.9	79.9
Blip enhancement	7.83	3.8	79.6

Questions?

UniGe

DIBRIS

Errata

Barrage Jamming distance scaling

I.r.l. power scales quadratically with distance, D should be D^2

$$AI(\rho,\theta) := z \cdot S(|\Delta_\theta|) \cdot \left(1 - \min\left[1, \frac{|\rho_j - \rho|}{D}\right]\right)$$