Malware Propagation in Complex Networks

Charlotte Felius Nikolaos Chatzis Viviane Desgrange

Overview

I. Introduction

II. HIRED Model

III. ABM Mesa model

IV. Cellular Automata Game

V. Conclusion

Introduction


MALWARE

Different types of Malware and assumptions

Main focus: Ransomware like infections (e.g. WannaCry):

Infected node can die or infect other neighbors

Neighboring nodes of an infected node are notified and can go offline to prevent infection

No (easy) antivirus

Some nodes cant go offline, this is dependent on their importance

Spyware Assumptions:

Nodes don’t notice their infection immediately

Antivirus software can make nodes resistant

Every Timestep there is a small probability that Antivirus Software is created

This probability increases as more nodes are infected

Hypothesis

Research questions

- How severe is the spread of Malware under different circumstances?
  - Does Malware leads to immutable change in the complex system?
  - Can cascading failure (avalanche) been observe in the network?
- How long until an Antivirus for Malware (Spyware) is created?
- In the SOC model what is the Avalanche and Output energy distributions?
- In the CA : what insights can we get by changing the grid and probability and of spread?

Hypothesis

Eventually a disturbed network (i.e. threatened by malware) will reach some steady state. Different actions can result in the prevention of wide malware spread

Model 1

H-I-R-E-D Model

In this model we explore 5 transition states:

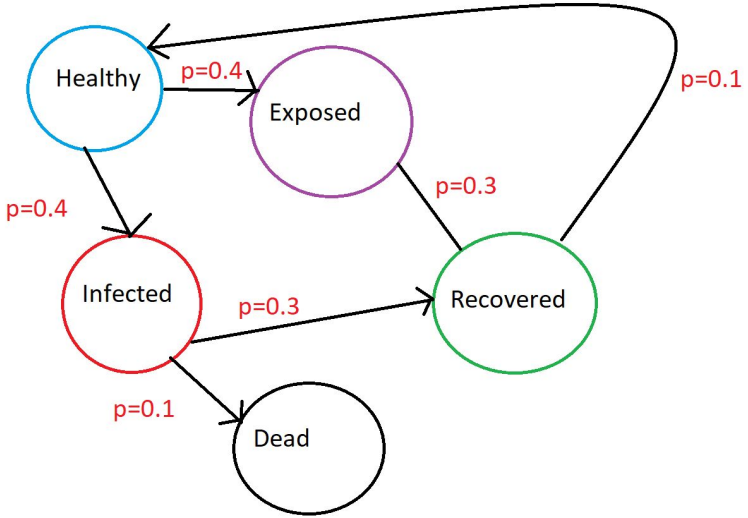
-Healthy can get Exposed or Infected

-Exposed can Recover

-Infected can Die or Recover

-Recover can become Healthy

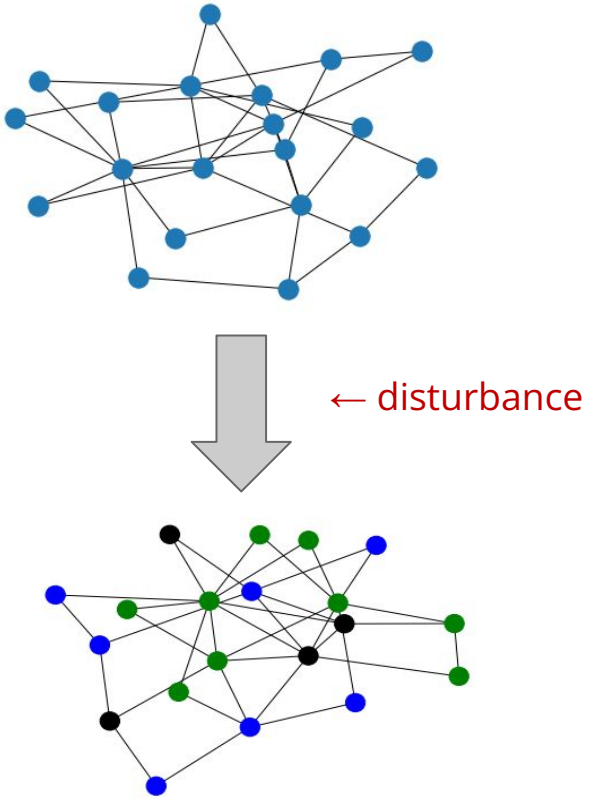
-Dead stays Dead



Experiments & emergence of phenomena

Self organised criticality

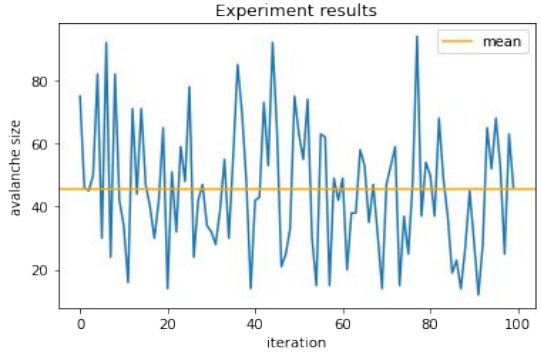
- System starts at a stable state
- Introduction of infected nodes
- Things move around
- New steady state

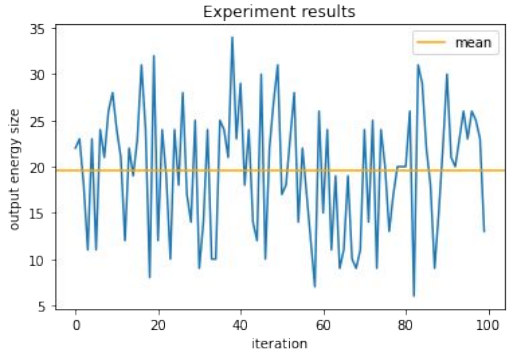


Terminology:

- Avalanche: time to new steady state
- Output energy: #dead at the end

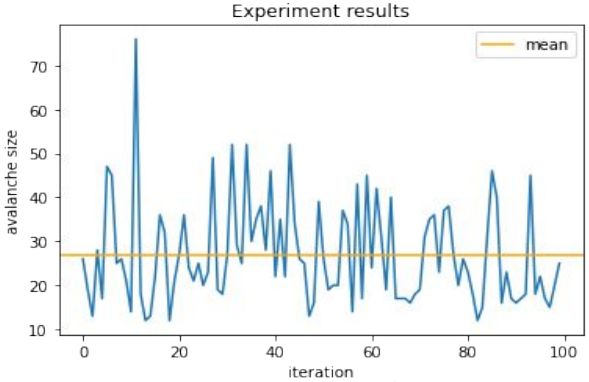
Warm Up

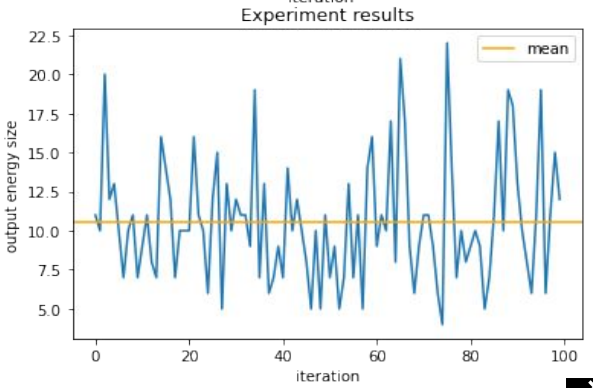




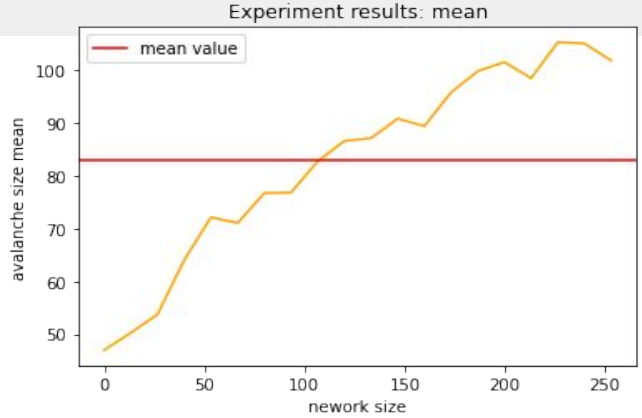
← Albert-Barabasi(53,3)

Random Graph(53,3/53) →

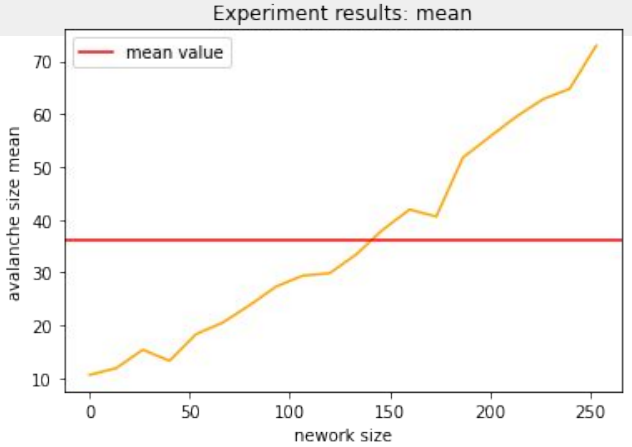




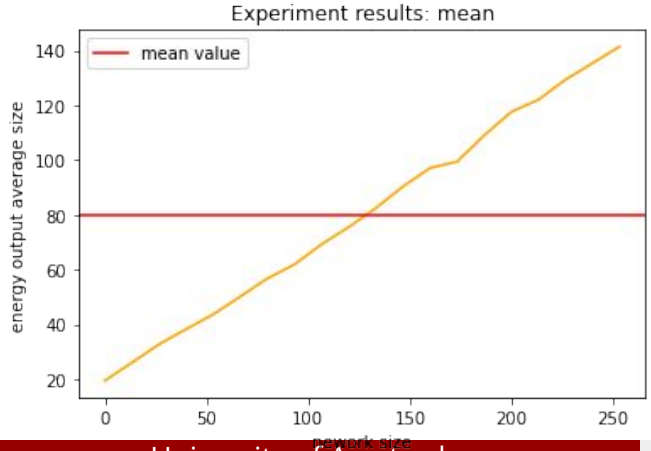
Increase network size

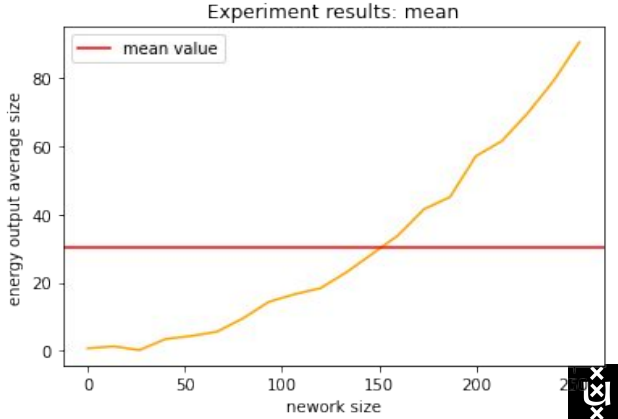


← Albert-Barabasi(253,3)



Random Graph(253,3/253) →





Logarithmic relation

Extrapolate network to 1000 nodes

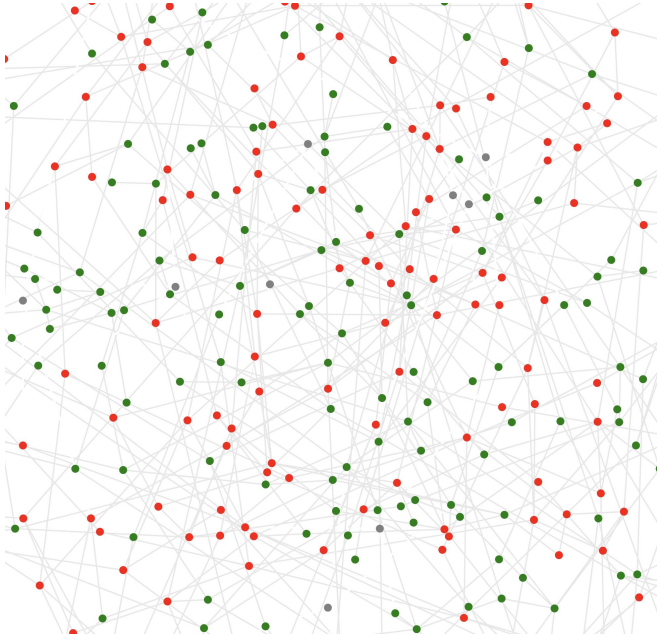
	Albert-Barabasi:	Random graph:
Avalanche mean:	162.3	203.5
Output energy mean:	651.6	811.8

Model 2

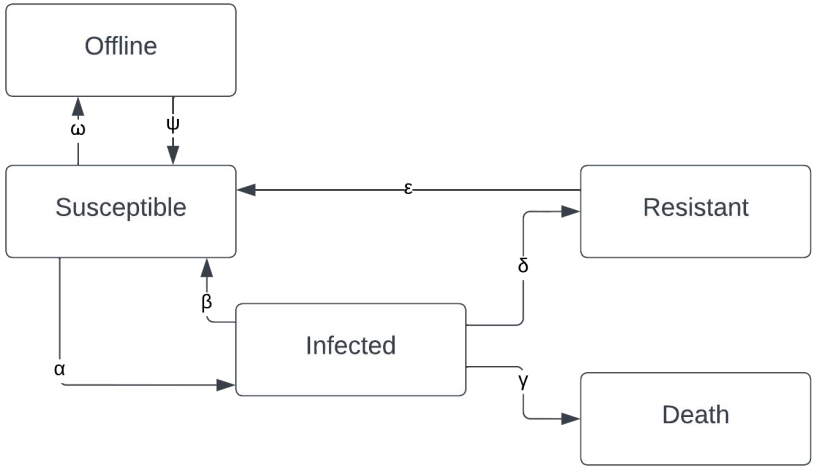
SIROD - An agent-based model

A complex system based on compartmental models from epidemiology

Type	• Agent-based model • Complex network from scratch
Framework	• Mesa (Netlogo based on Python networkX)
Agents	• Malware Agent
Network	• Erdos-Renyï • Barabasi Albert
States	S (Susceptible) I (Infected) R (Resistant) O (Offline) D (Death)



Methods & parameters

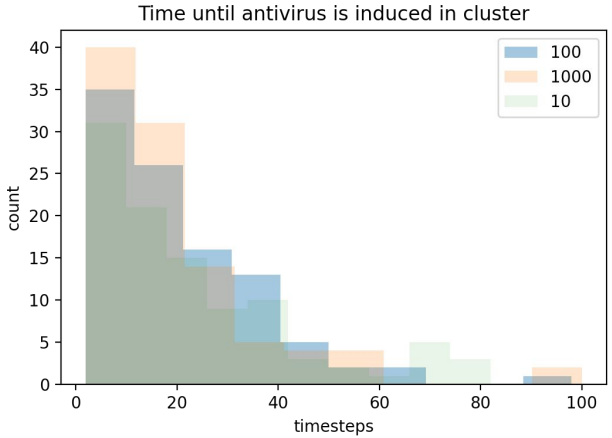


Demonstration

Experiments & emergence of phenomena

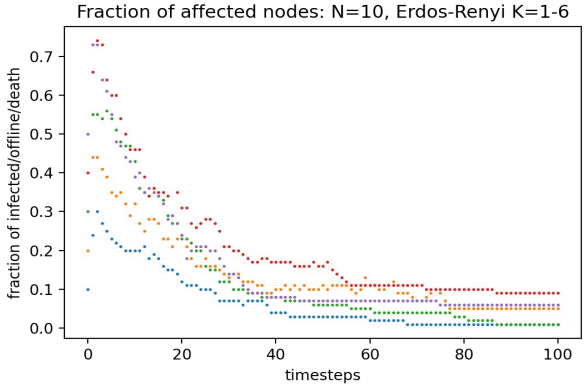
Antivirus Adoption (Spyware)

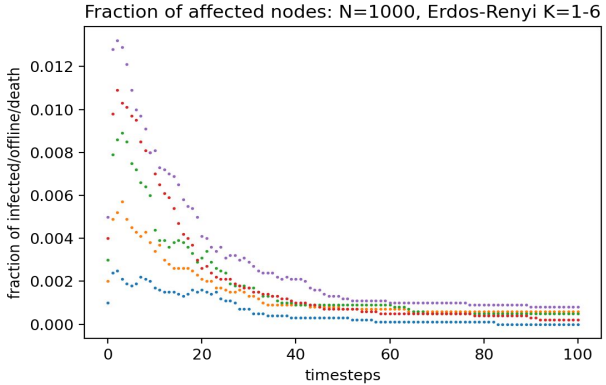
- Specific case where Malware cannot induce death but gets unnoticed for a larger period of time (Spyware)
- 100 simulations

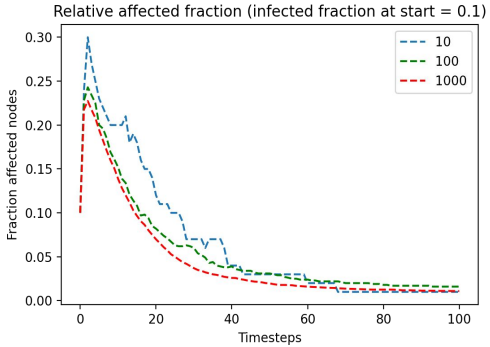


Initial results

- Avg of 10 simulations per timestep
- For different initial infections outbreak [1,2,3,4,5,6]
- 10, 100, 1000 Nodes, 100 timesteps
- ER Random Network
- Affected fraction = Infected + Offline + Death

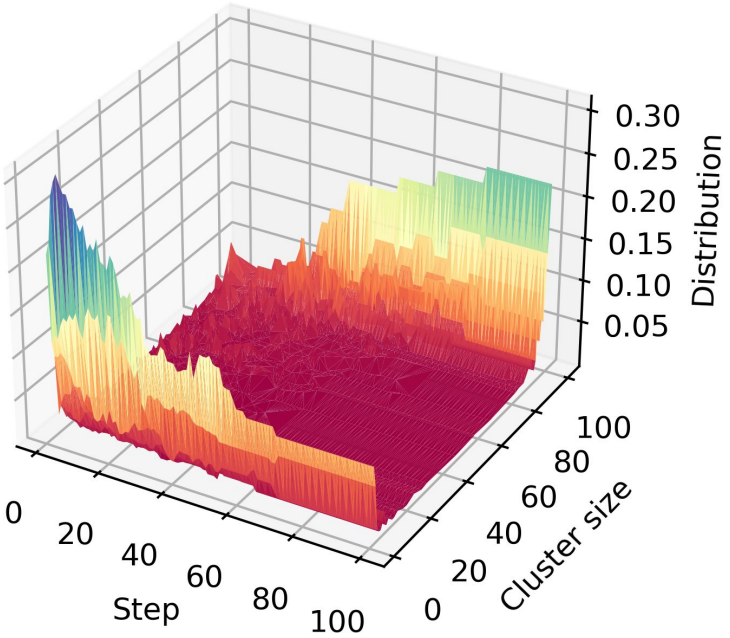






Immutable change - cluster analysis

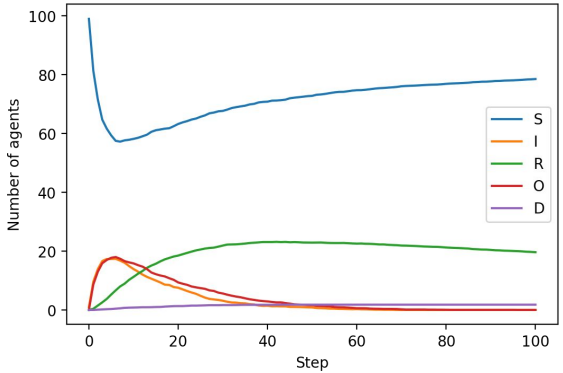
Evolution w.r.t time t → Emergence of giants components in Barabasi-Albert network



- Barabasi Albert
- 100 simulations
- [100, 1000] nodes
- Infection node centrality per degree
- Optimistic scenario (low death - offline - high check)

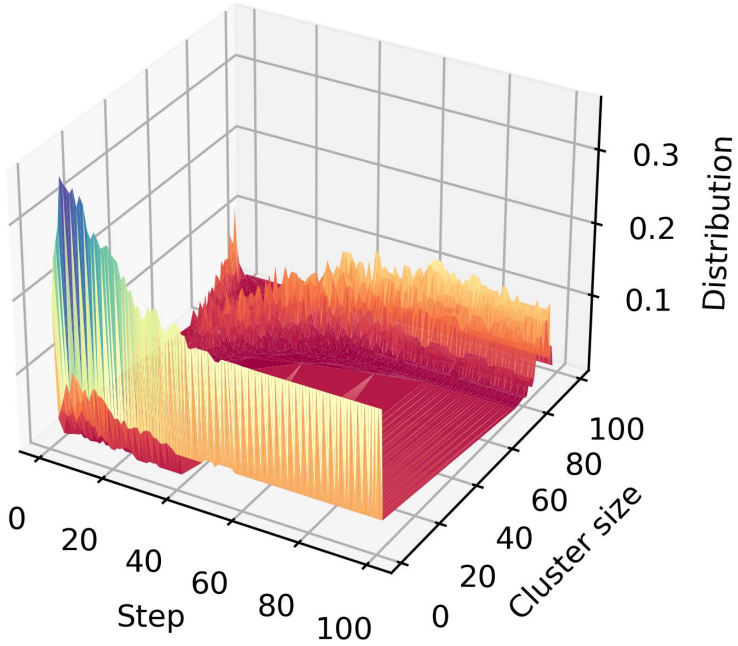
To compare with agent state evolution

Barabasi Albert → malware stop fast → giant components



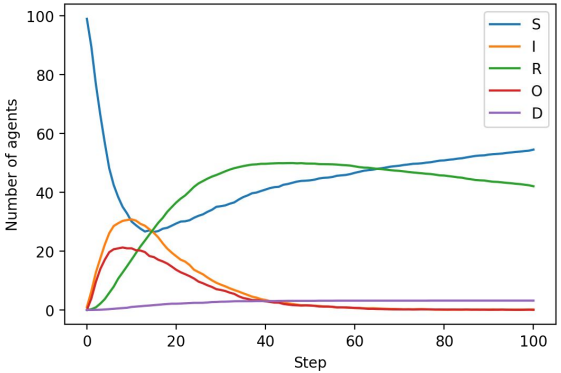
Immutable change - cluster analysis

Evolution w.r.t time t → Less obvious with random network



- Erdos-Renyï
- 100 simulations
- 100 nodes
- Infection node centrality per degree
- Optimistic scenario (low death - offline - high check)

To compare with agent state evolution

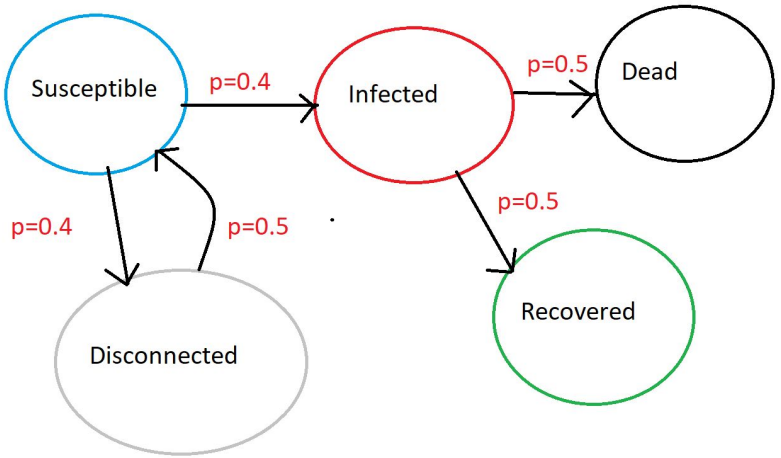


A cellular automata game

Cellular Automata game

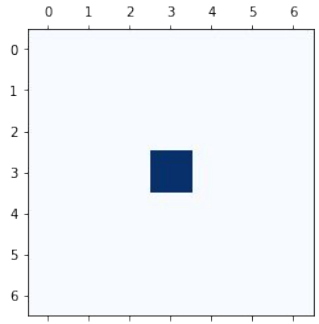
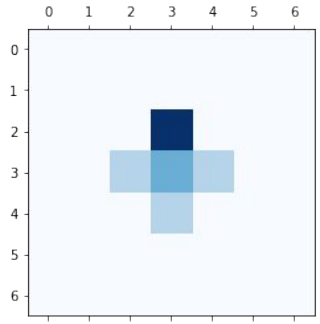
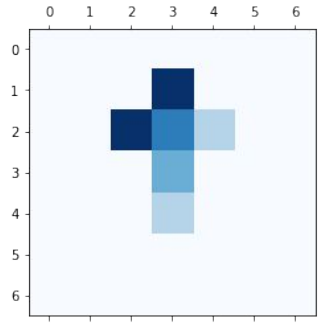
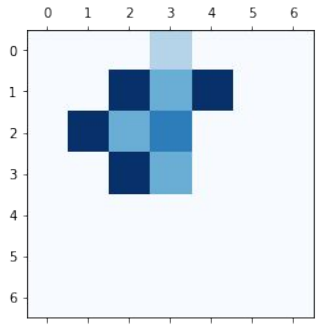
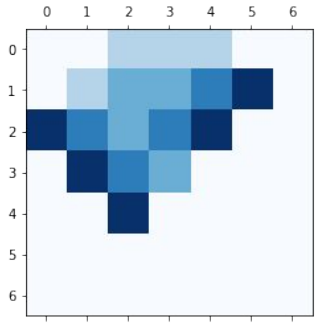
Game rules:

- 5 states of Von Neumann model (Diamond)
- The very middle site starts as infected
- Win if:
  - reach a set amount of steps &
  - spread has not reached the edge



Warm Up

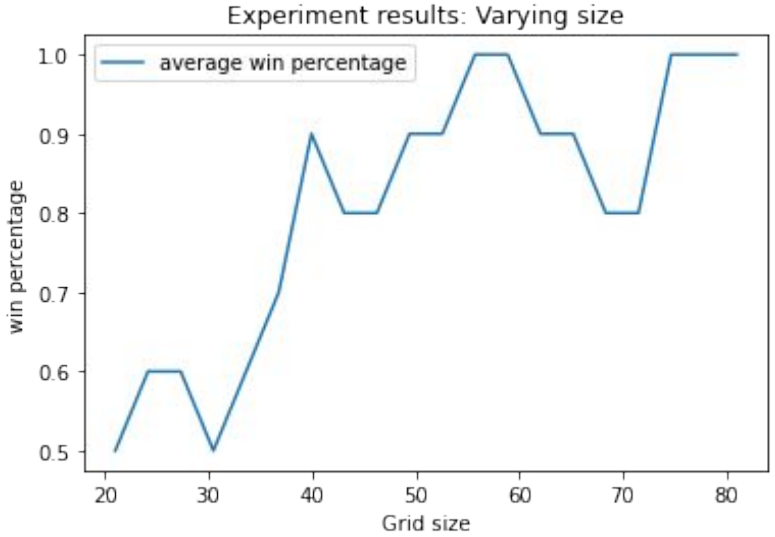
5x5 grid:

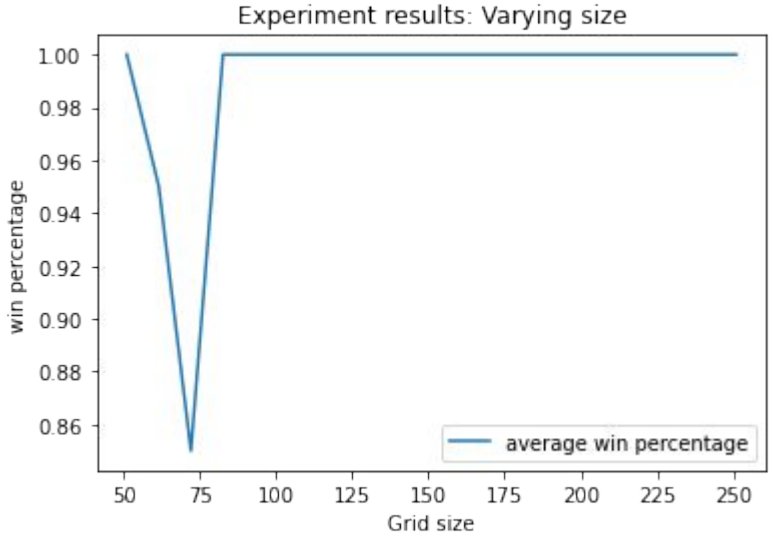
White = Susceptible → Offline → Dead → Recovered → Infected = Dark blue

Increase grid size

Start 21x21 and increase side length by 2 each step:

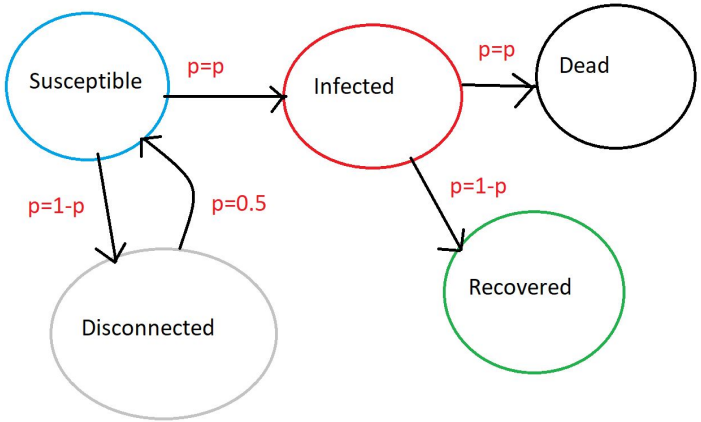


Start 51x51 and increase by 10 each step:

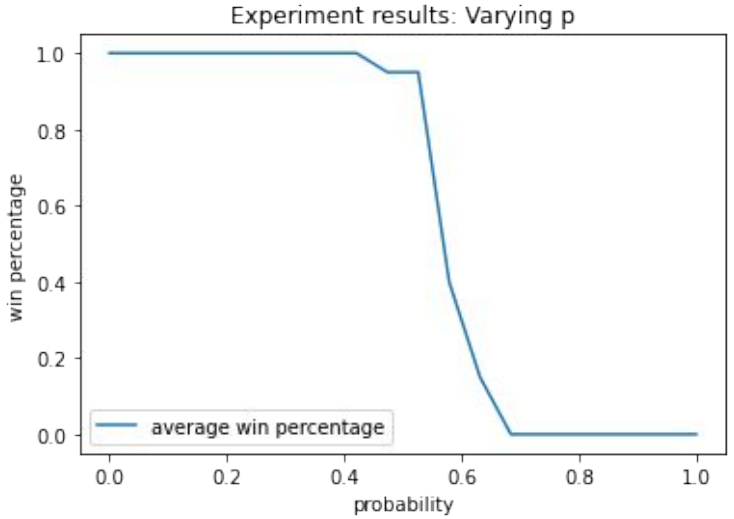


51x51 grid, varying probability:

New Model:



Results:



Conclusion:

Plot suggests a phase transition from “all win” to “all lose”, rather than a data collapse

Conclusion

- Does Malware leads to immutable change in the complex system? It depends!
  - Optimistic scenario (low death - offline - high check) leads to remission of the system.
  - Pessimistic scenario (high death - low check) leads to collapse of the system
  - We can observe emergence of giant components

- In the SOC system we noticed a difference in distribution of Avalanche and Output Energy depending on the network model:
  - Random Graph: Avalanche => linear, Output Energy => exponential
  - Albert-Barabasi: Avalanche => logarithmic, Output Energy => linear

- In the cellular automata model:
  - Increasing the grid size makes us win with probability 1
  - Fixing the grid size and varying the spread probability behaves like a phase transition from “always win” to “always lose”

References

[1] A New Individual-Based Model to Simulate Malware Propagation in Wireless Sensor Networks
Farrah Kristel Batista, Ángel Martín del Rey, Araceli Queiruga-Dios. March 2020.

[2] Advanced malware propagation on random complex networks
A.Martín del Rey, G.Hernández, A.Bustos Tabernero, A.Queiruga Dios. 2020

[3] An agent-based model to simulate coordinated response to malware outbreak within an organisation
Jonathan Pan, Chun Che Fung. January 2012

[4] Power Laws in Superspreading Events: Evidence from Coronavirus Outbreaks and Implications for SIR Models

Questions ?