Discrete Modeling Simulation of Worm Propagation

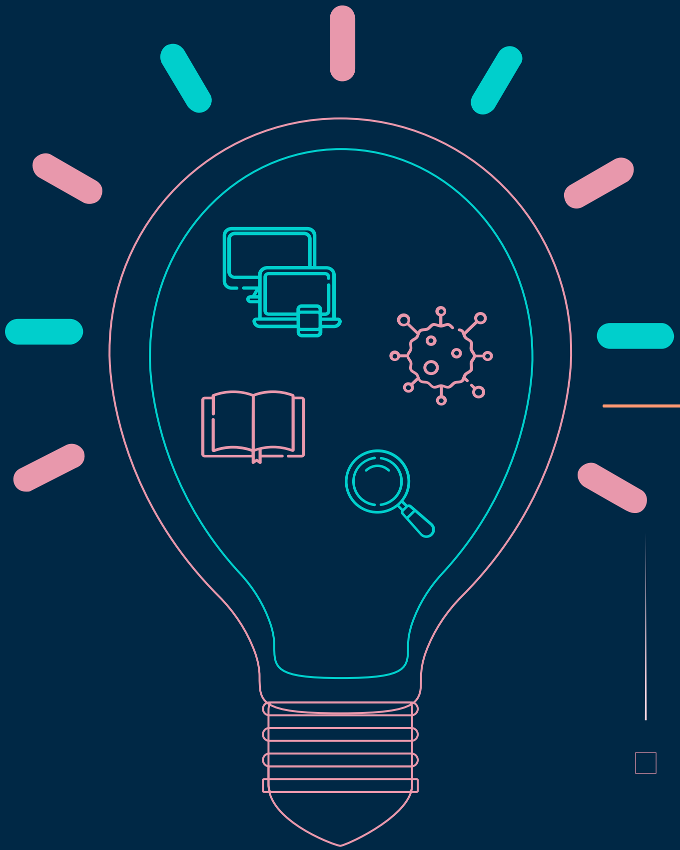
and Comparing Worm Infection Using Random Scanning and Local Preference Scanning

Avinash Khetri 2K18/IT/035
Shreoshi Roy 2K18/SE/120

ABSTRACT

One of the most malicious malware infecting computer systems in today's time, are worms. Our project addresses the need for simulating worm propagation in medium-scale networks by taking inspiration from [1] so that it is easier to understand how exactly a worm infects computers and what are some of the factors affecting its spread.

Malware analysis can be done statically or dynamically, but we have chosen simulation as research has shown that visualization and simulation have proven to be the best techniques for educational and research purposes [2].



[1] Jyotsna Krishnaswamy, Wormulator: Simulator for Rapidly Spreading Malware, in San Jose State University SJSU ScholarWorks, 2009

[2] Madihah Mohd Saudi, Kamaruzzaman Seman, Emran Mohd Tamil and Mohd Yamani Idna Idris, Worm Analysis through Computer Simulation (WAtCoS), The International Journal of Learning Annual Review, 2008

[3] Legal Job Site, 44 Must-Know Malware Statistics to Take Seriously in 2020, 2020

$2.4 million

Worth of damage is incurred by the average US company every year due to worms [3]

What are Worms?

As defined by [4], worms are a type of malware that is **independent** and does not require any software to attach to

They take advantage of computer or network **vulnerabilities** to creep into a system and cause damage.

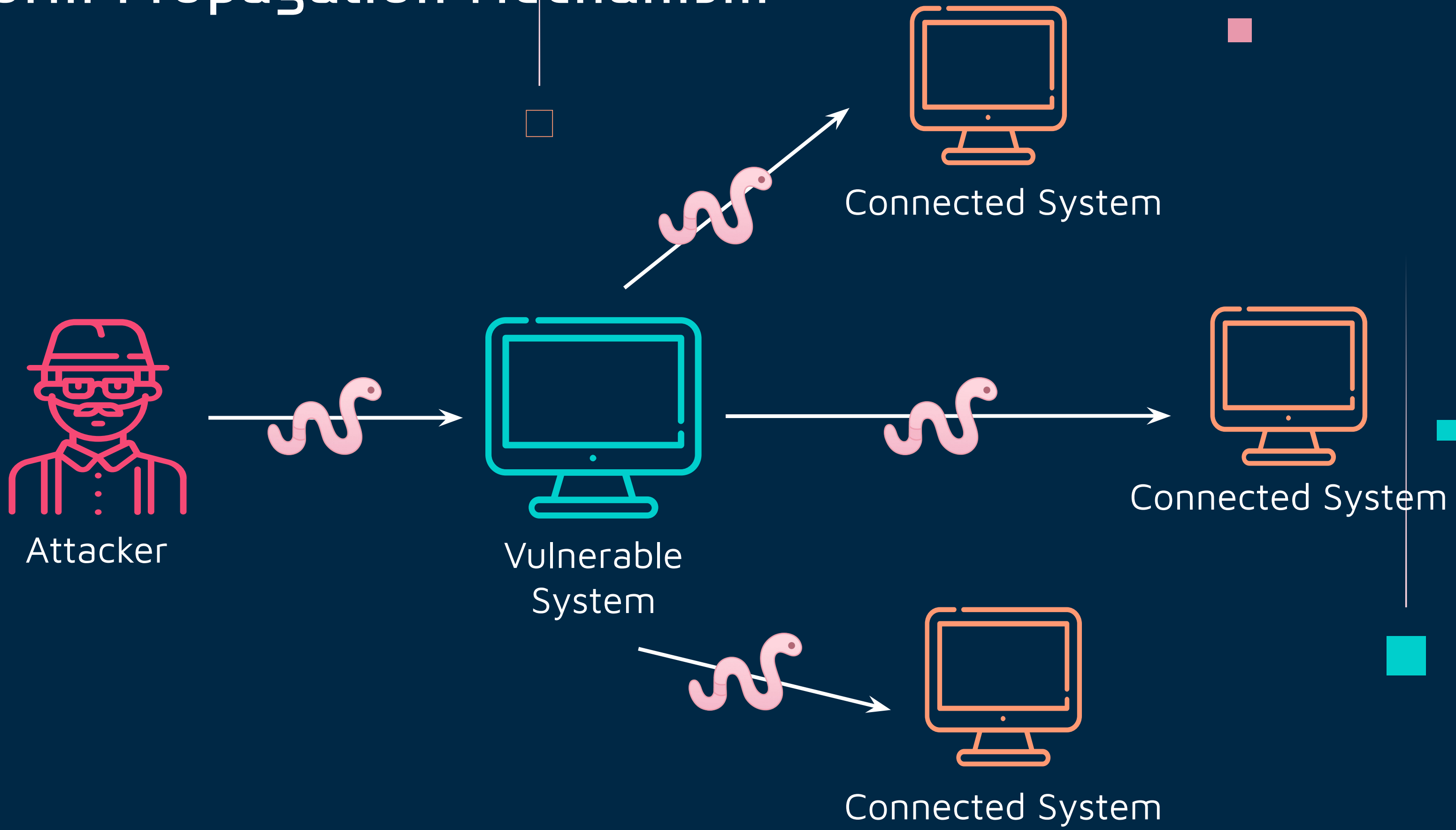
They **replicate very fast** and can infect all the computers present in a network in a very short time.

Once a worm enters a system, it will **scan all computers on its network** to find more potential victims.

[4] Wikipedia, Computer Worm, 2020. https://en.wikipedia.org/wiki/Computer_worm

[5] B. Rajesh, IIY.R. Janardhan Reddy, IIIB. Dillip Kumar Reddy, A Survey Paper on Malicious Computer Worms, International Journal of Advanced Research in Computer Science & Technology, 2015

Worm Propagation Mechanism



OBJECTIVE

01

Use Discrete Event Simulation Model and Epidemic Model to create a tool that shows how worms propagate in a medium-scale network

OBJECTIVE

02

Compare simulation results obtained when a worm propagates through random scanning vs local preference scanning

MODELS

Discrete-event simulation model

Considers time to be **discrete** instead of continuous

Time is sliced into **equal**-sized intervals

State of every variable can change only when the next time interval occurs

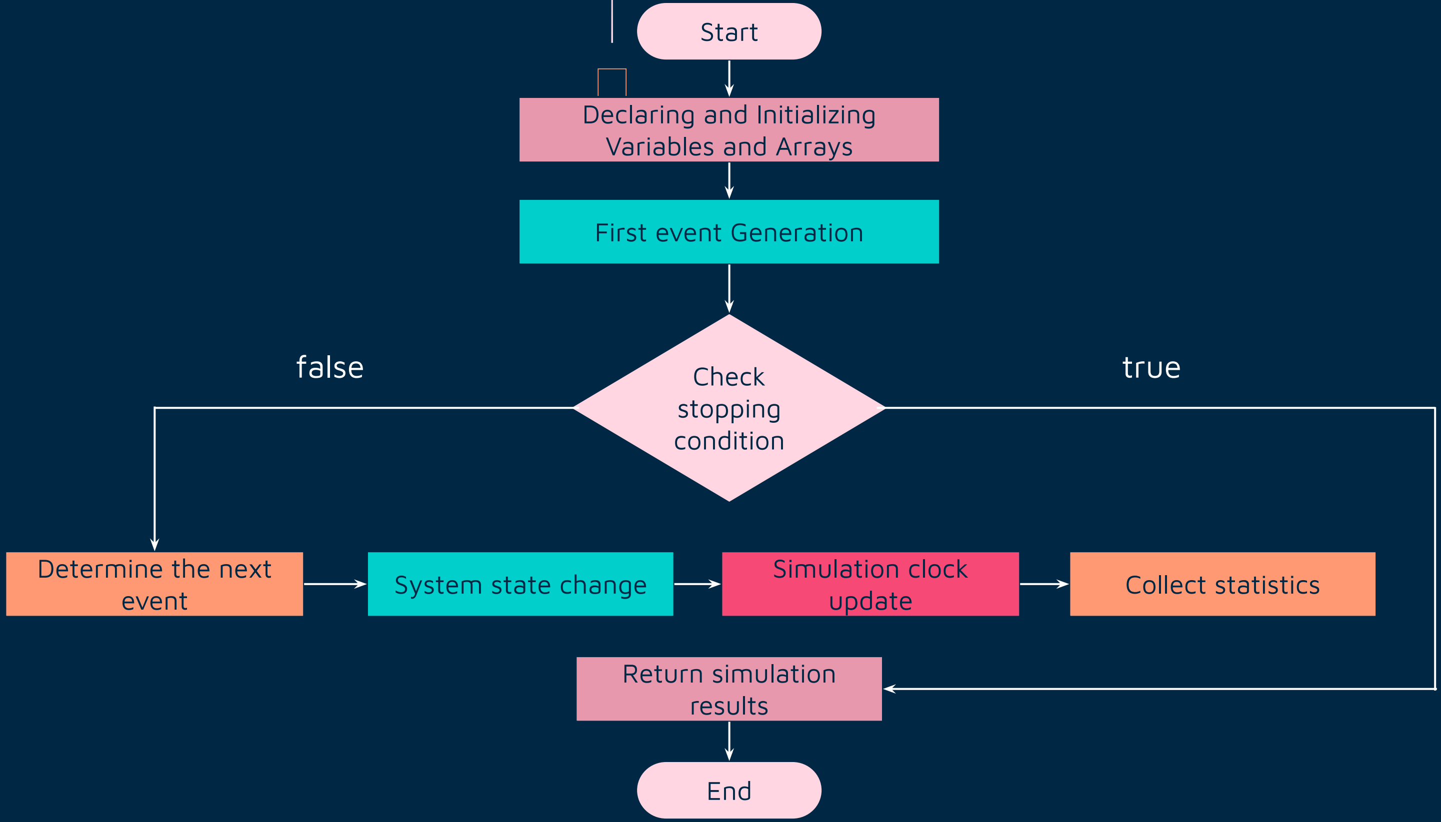
Any change in the state of a variable is called an **event** [6]

No event can occur between two consecutive timestamps

The system can **jump** to various events instead of occurring continuously

[6] TutorialsPoint, Discrete system simulation. https://www.tutorialspoint.com/modelling_and_simulation/modelling_and_simulation_discrete_system_simulation.htm

FLOWCHART : Discrete-event simulation model



[7] Dmitry Kozyrev, Vladimir Rykov, Statistics and Simulation, 2018

EPIDEMIC MODEL

01

Superset of the SIR Model

Used to study the transmission of infectious epidemics

02

Homogeneous networks

All hosts are considered to be identical in design

03

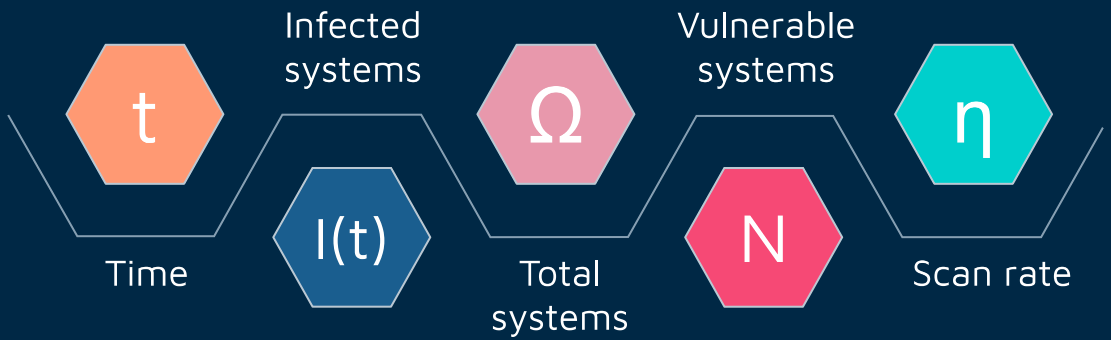
Completely Connected Graph

Any infected host can infect **any** vulnerable host in the system [8]

[8] Cliff C. Zou, Don Towsley, Weibo Gong, Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm, University of Central Florida.

According to this model [8], the worm propagation at any given time can be represented by the equation:

$$\frac{dI(t)}{dt} = \frac{\eta}{\Omega} I(t)[N - I(t)]$$



[8] Cliff C. Zou, Don Towsley, Weibo Gong, Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm, University of Central Florida.

METHODS OF SCANNING

RANDOM

The host selects a computer at random by generating a random IP address [9]

All computers have an equal probability of getting scanned

Example - Slammer and Code Red

LOCAL PREFERENCE

The host selects a computer having an IP address closer to itself within its sub-network [10]

Computers nearer to the host have a higher probability of getting scanned

Example - Sasser worm and Blaster worm [11]

[9] Zesheng Chen, Worm Propagation Models, Georgia Institute of Technology
[10] Cliff Changchun Zou, Don Towsley, Weibo Gong, On the Performance of Internet Worm Scanning Strategies, Univ. Massachusetts, Amherst
[11] Markos Avlonitis, Emmanouil Magkos, Michalis Stefanidakis, Vassileios Chrissikopoulos, Exploring Scalability and Fast Spreading of Local Preference Worms via Gradient Models, 17th EICAR Annual Conference, 2008

DESIGN

IMPLEMENTATION ENVIRONMENT

Programming Language

Python 3

Library Packages

Numpy, Pandas, Matplotlib, Streamlit

Interface Design

GUI using Streamlit

IMPLEMENTATION DETAILS

IP address space in our network ranges from 1 to 100,000.

$\Omega = 100{,}000$

The host can scan 3 IP addresses at each time step

$\eta = 3$

$N = 1{,}000$

1,000 computers are vulnerable to the worm in the network

$1(0) = 1$

When the simulation starts, only one computer is infected

PROCESS

STEP 01

Initially, when the simulation starts, only one computer is worm infested

STEP 02

The host scans 3 more computers. If they are vulnerable, they get infected

STEP 03

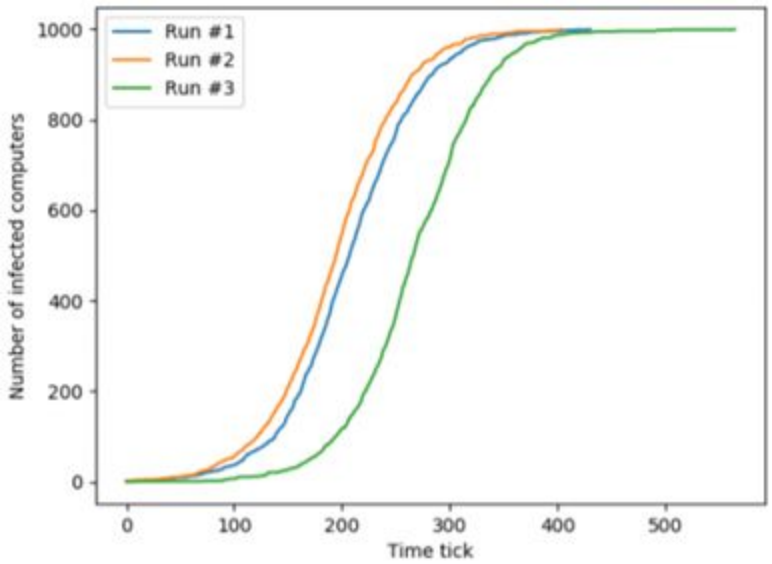
The newly infected computers also act as host and infect more computers recursively

STEP 04

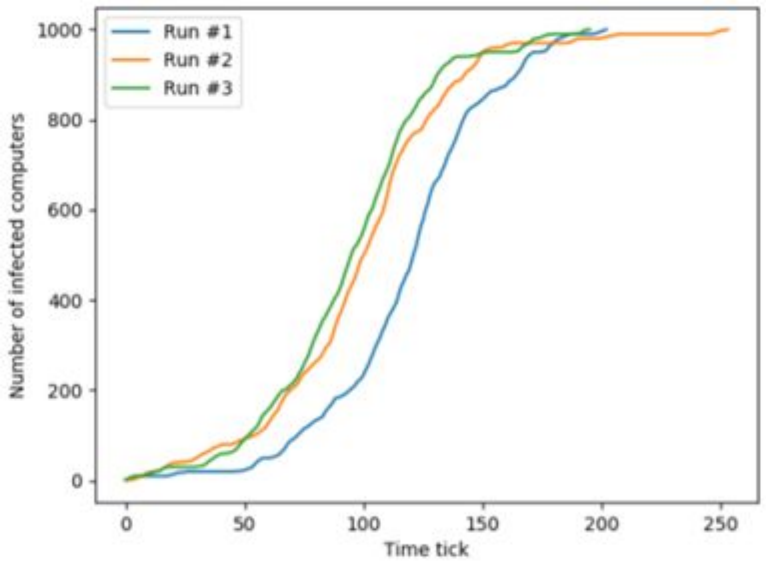
The simulation ends when all the 1000 vulnerable computers have been infected

RESULTS

GRAPHS



Three simulation runs for worm propagation through Random Scanning method



Three simulation runs for worm propagation through Local Preference Scanning method

INFERENCES

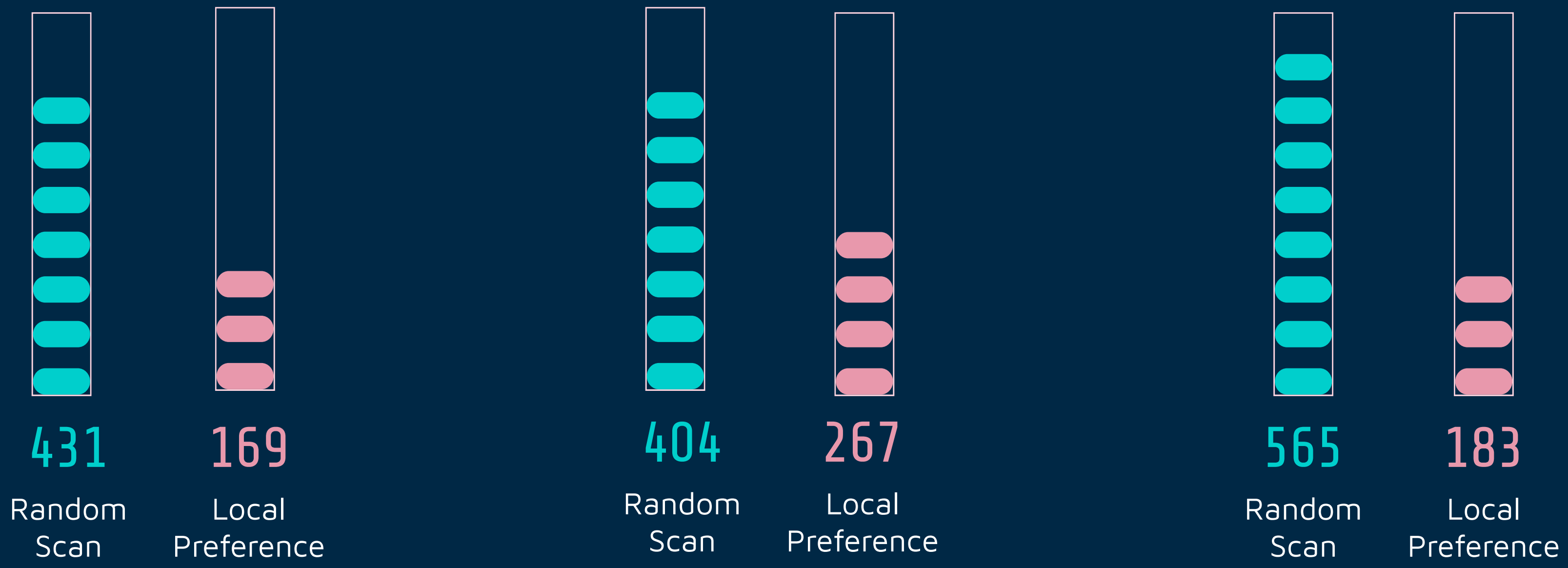
Both the methods result in an 'S-shaped curve' or Sigmoid curve with only one inflection point

Initially, the spread is slow but the propagation increases exponentially as the infection spreads

The graph keeps increasing until all the 1000 vulnerable systems in the network are infected

ANALYSIS

Time intervals taken for the worm to spread to all vulnerable computers



Hence, **Local Preference Scanning is faster** at worm propagation as compared to Random Scanning

CONCLUSION

FUTURE WORK

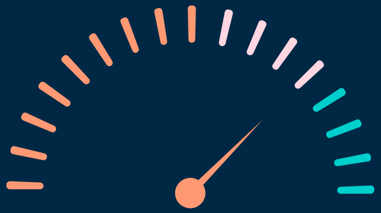
NETWORK TYPES

We could develop models for worm propagation in distributed networks, wireless networks, etc as discussed in [12]

SCANNING METHODS

More ways of worm propagation such as sequential scanning, routing scanning, hit-list scanning, selective attacks, etc

USER CONTROL



More user control options can be added in the tool like changing variable values of Ω, N, η according to user's choices

[12] Farrah Kristel Batista, Angel Martín del Rey and Araceli Queiruga-Dios, A New Individual-Based Model to Simulate Malware Propagation in Wireless Sensor Networks, MDPI, 2020

REFERENCES

[1] Wormulator: Simulator for Rapidly Spreading Malware, in San Jose State University SJSU ScholarWorks, 2009

—Jyotsna Krishnaswamy

[2] Worm Analysis through Computer Simulation (WAtCoS), The International Journal of Learning Annual Review, 2008.

— Madihah Mohd Saudi
— Kamaruzzaman Seman
— Emran Mohd Tamil
— Mohd Yamani Idna Idris

[3] 44 Must-Know Malware Statistics to Take Seriously in 2020, 2020

—Legal Job Site

[4] Computer Worm, 2020. https://en.wikipedia.org/wiki/Computer_worm

—Wikipedia

[5] A Survey Paper on Malicious Computer Worms, International Journal of Advanced Research in Computer Science & Technology, 2015

— B. Rajesh
— Y.R. Janardhan Reddy
— 1B. Dillip Kumar Reddy

[6] Discrete system simulation. https://www.tutorialspoint.com/modelling_and_simulation/modelling_and_simulation_discrete_system_simulation.htm

—Tutorials Point

REFERENCES

[7] Statistics and Simulation, 2018.

—Dmitry Kozyrev
—Vladimir Rykov

[8] Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm, University of Central Florida

— Cliff C Zou
— Don Towsley
— Weibo Gong

[9] Worm Propagation Models, Georgia Institute of Technology

—Zesheng Chen

[10] On the Performance of Internet Worm Scanning Strategies, Univ. Massachusetts, Amherst

— Cliff Changchun. Zou
— Don Towsley
— Weibo Gong

[11] Exploring Scalability and Fast Spreading of Local Preference Worms via Gradient Models, 17th EICAR Annual Conference, 2008

— Markos Avlonitis
— Emmanouil Magkos
— Michalis Stefanidakis
— Vassileios Chrissikopoulos

[12] A New Individual-Based Model to Simulate Malware Propagation in Wireless Sensor Networks, MDPI, 2020 Amherst

— Farrah Kristel Batista
— Angel Martin del Ray
— Araceli Queiruga-Dios

THANK YOU

Avinash Khetri 2K18/IT/035
Shreoshi Roy 2K18/SE/120