# Discrete Modelling 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

# Problem Description

Our project addresses the need for simulating worm propagation in medium-scale networks so that it is easier to understand how exactly a worm infects computers and what are some of the factors affecting its spread. Our project addresses the need for simulating worm propagation in medium-scale networks so that it is easier to understand how exactly a worm infects computers and what are some of the factors affecting its spread. We have used the discrete-event simulation model to build this tool and have also compared the results of worm propagation through random scanning and local preference scanning.

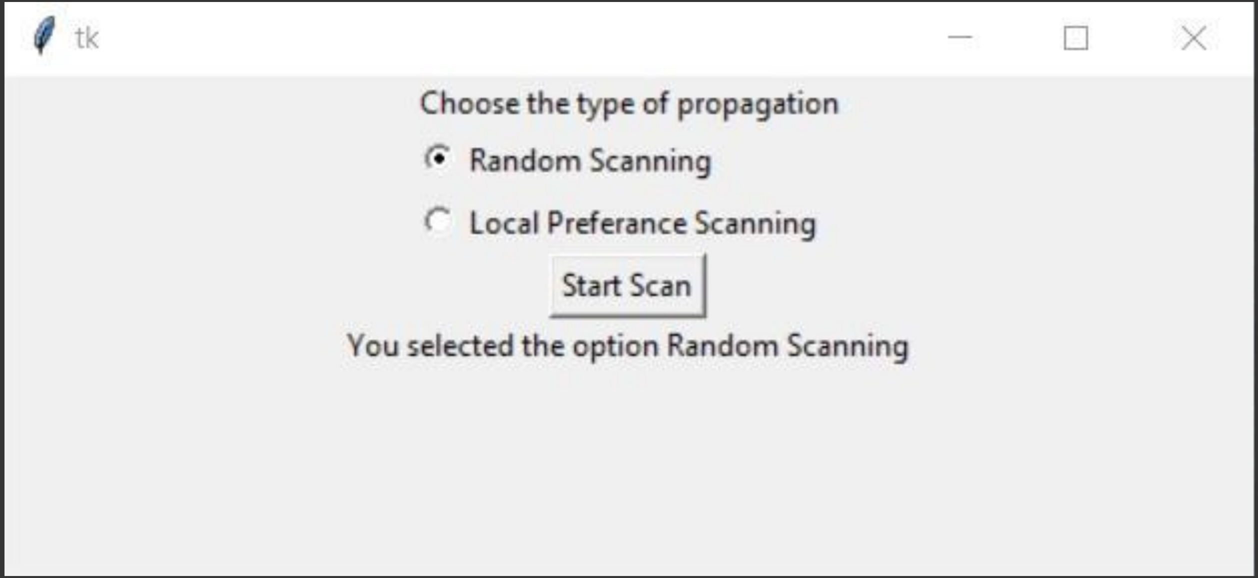
# Solution

- We have created a GUI simulation tool using Tkinter that shows how worms connected via a network propagate when a single computer of the network gets compromised. We have used the discrete time-event mathematical model for simulation.
- For the sake of simplicity, 100,000 ($\Omega$) computers have been assumed to be connected out of which 1000 (N) of them are considered to be susceptible to worm invasions.  For every 1000 computers, there exists a group of 10 computers with successive IP addresses that can be attacked by worms successfully and there are in total 100 such groups.

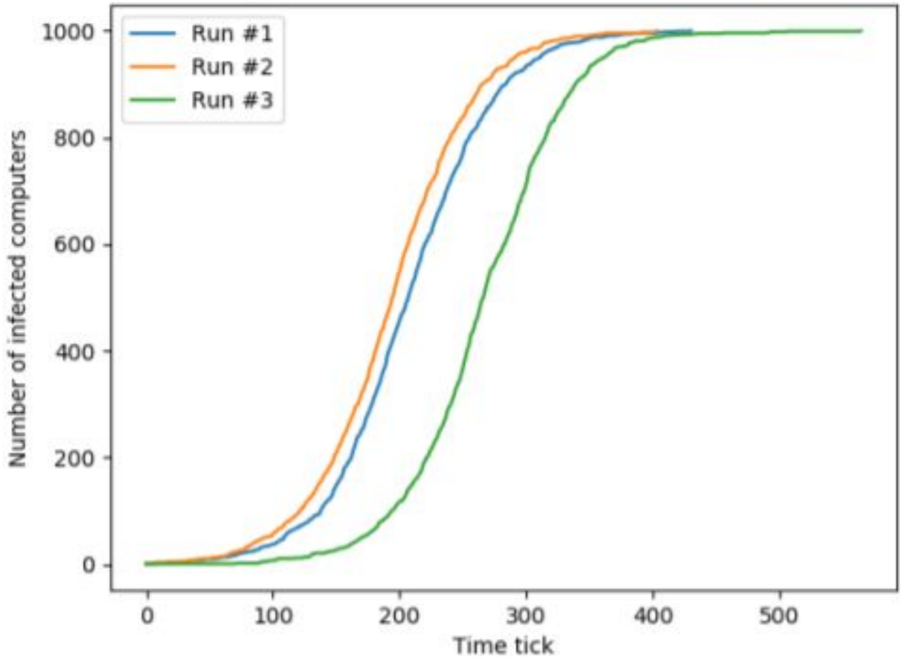
# Solution

- Initially, only one computer is assumed to be infected. After an interval of one time unit, it starts looking for other computers in the network that can be attacked. If a vulnerable system is found in the scan, then that system will become infected and can act as a new host in the next timestamp. This process keeps occurring recursively until all the 1000 vulnerable computers get infected.
- Further, we illustrate the comparison of simulation results obtained when a worm propagates through random scanning vs local preference scanning through graphs.

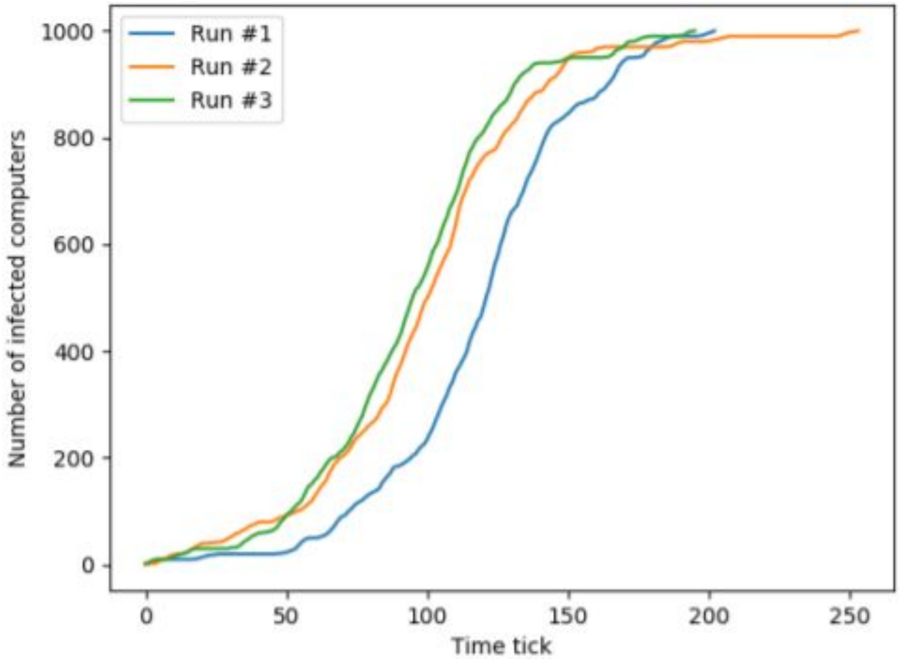
# Simulation Tool



# Results




Three simulation runs for worm propagation through random scanning method




Three simulation runs for worm propagation through local preference scanning method

# Results

- We can observe that both the methods result in an 'S-shaped curve' or a Sigmoid curve with only one inflection point. Initially, the spread is slow but the propagation increases exponentially as more and more computers get infiltrated and start acting as hosts. They keep on increasing until all the vulnerable systems in the network have been infected.
- We have also observed as expected that local preference scanning is a clear winner when it comes to spreading worms faster in a network

# Future Work

As future work, the tool can be improved to propagate through more ways such as sequential scanning, routing scanning, hit-list scanning, selective attacks, etc. The interface can be improved by providing user-defined variable values of $\Omega$, $N$, $\eta$, and controlling the speed of the time intervals. Further, for more advanced implementations, we could develop models for worm propagation in distributed networks, wireless networks [15] or introduce Machine Learning and Data Science tools to further improve our results.

# References

[1]Jyotsna Krishnaswamy, Wormulator: Simulator for Rapidly Spreading Malware, in San Jose State University SJSU ScholarWorks, 2009 https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1068&context=etd_projects

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

[3] Veracode, Computer Worm. https://www.veracode.com/security/computer-worm

[4] Josh Fruhlinger, What is a computer worm? How this self-spreading malware wreaks havoc, https://www.csoonline.com/article/3429569/what-is-a-computer-worm-how-this-self-spreading-malware-wreaks-havoc.html

[5] SoftwareLab, What is a Computer Worm? https://softwarelab.org/what-is-a-computer-worm/

[6] 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. https://www.researchgate.net/publication/44262006_Worm_Analysis_through_Computer_Simulation_WAtCoS

[7] University of Central Florida, Performance Models of Computers and Networks, 2012. http://www.cs.ucf.edu/~czou/CDA6530-12/project-3.pdf

# References


[8] Wikipedia, Discrete-event simulation model, 2020 https://en.wikipedia.org/wiki/Discrete-event_simulation

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

[10] Dmitry Kozyrev, Vladimir Rykov, Statistics and Simulation, 2018. https://www.researchgate.net/publication/325197422_On_Sensitivity_of_Steady-State_Probabilities_of_a_Cold_Redundant_System_to_the_Shapes_of_Life_and_Repair_Time_Distributions_of_Its_Elements

[11] Cliff C. Zou, Don Towsley, Weibo Gong, Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm, University of Central Florida. http://cs.ucf.edu/~czou/research/emailWorm-TDSC.pdf

[12] Zesheng Chen, Worm Propagation Models, Georgia Institute of Technology. http://www.mathaware.org/mam/06/Chen.pdf

[13] Cliff Changchun Zou, Don Towsley, Weibo Gong, On the Performance of Internet Worm Scanning Strategies, Univ. Massachusetts, Amherst. http://www.eecs.ucf.edu/~czou/research/wormStrategy-techreport.pdf

[14] 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. https://www.researchgate.net/publication/253182633_Exploring_Scalability_and_Fast_Spreading_of_Local_Preference_Worms_via_Gradient_Models

[15] 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 https://doi.org/10.3390/math8030410