MALWARE PROPOGATION – PROGRAMMING ASSIGNMENT 3

Section A: Introduction

This assignment required to simulate a simple worm propagation over a network of 100,000 IP addresses. Out of the all IP addresses considered, 1000 IP addresses are vulnerable. These vulnerable IP addresses are numbered as 1, 2, 3, …, 10, 1001, 1002, 1003, …. ,1010, 2001, 2002, 2003, …., 2010, so on and so forth until, 99001, 99002, 99003, …., 99010. Random scanning worm propagation starts with one infected IP address, 1001 and at each time tick, every infected IP address will scan three other IP addresses to check if they are vulnerable. If it is vulnerable, then it attacks the computer and if it is not vulnerable, it simply moves to scan another three computers during the next time tick. If an IP address gets infected in time tick 't', then this newly infected IP address starts infecting other vulnerable IP addresses from the next time tick.

In the local-preference scanning strategy, the code is modified to pick IP addresses based on probability. With a probability of 0.8, the infected IP address (x) picks another IP address (y) within the same cluster (y is in the range x – 10 and x + 10). And with a probability of 0.2, the infected IP address scans for another IP address in the entire network.

Both the above methods are continued until every vulnerable IP address in the network is infected and the process is repeated three times to get three simulation results. Graphs are plotted showing the infection rate and the time taken to run each simulation is recorded.

Section B: Design and Implementation

The following are steps used to simulate random scanning worm propagation:
1. Generate a network of 100,000 IP addresses
2. Generate a list of all vulnerable IP addresses
3. Set the initially infected IP address to 1001 and scan rate = 3
4. For the number of infected IP addresses in the list
        Choose three random IP addresses from the network
        If randomly chosen IP address is vulnerable
                Add the IP address to the infected IP address list
        Else
                Discard the randomly chosen IP address
5. Repeat until all the vulnerable IP addresses are infected

In the local-preference scanning worm propagation, only step 4 is changes as follows:
For the number of infected IP addresses in the list
        For the i between 0 and scan rate:
                Generate a probability value between 0 and 1
                If probability <= 0.8
                    Select a random IP address in +/- 10 range of infected IP
                Else
                Select a random IP address in the entire network

MALWARE PROPOGATION – PROGRAMMING ASSIGNMENT 3

Section C: Output and Output Analysis

Eustis does not have pip3 installed, hence use the following command lines to be able to install the prebuilt libraries:

```
wget https://bootstrap.pypa.io/get-pip.py
python3 get-pip.py –user
export PATH="/home/net/<USER-NAME>/.local/bin:$PATH"
source ~/.bashrc
```

A shell script called install_pip.sh is provided in the submission to execute the above commands. Make the shell script executable using `chmod +x install_pip.sh`

My program was written in Python and requires some prebuilt libraries which can be installed using the following commands:
```
pip3 install --user random
pip3 install --user math
pip3 install --user matplotlib
pip3 install --user progressbar2
```

Once all the required libraries are installed, the source codes can be executed using the following commands:
```
python3 Prog_assignment3.1.py
python3 Prog_assignment3.2.py
```

The output for the programs is graphs showing infection rate for three execution cycles and also the time taken to complete infection in all three execution cycles. The obtained graph looks as follows:

It was noticed that more time was taken to infect all vulnerable IP addresses in Random-Scanning worm propagation than Local-Preference Scanning worm propagation.

## MALWARE PROPOGATION – PROGRAMMING ASSIGNMENT 3

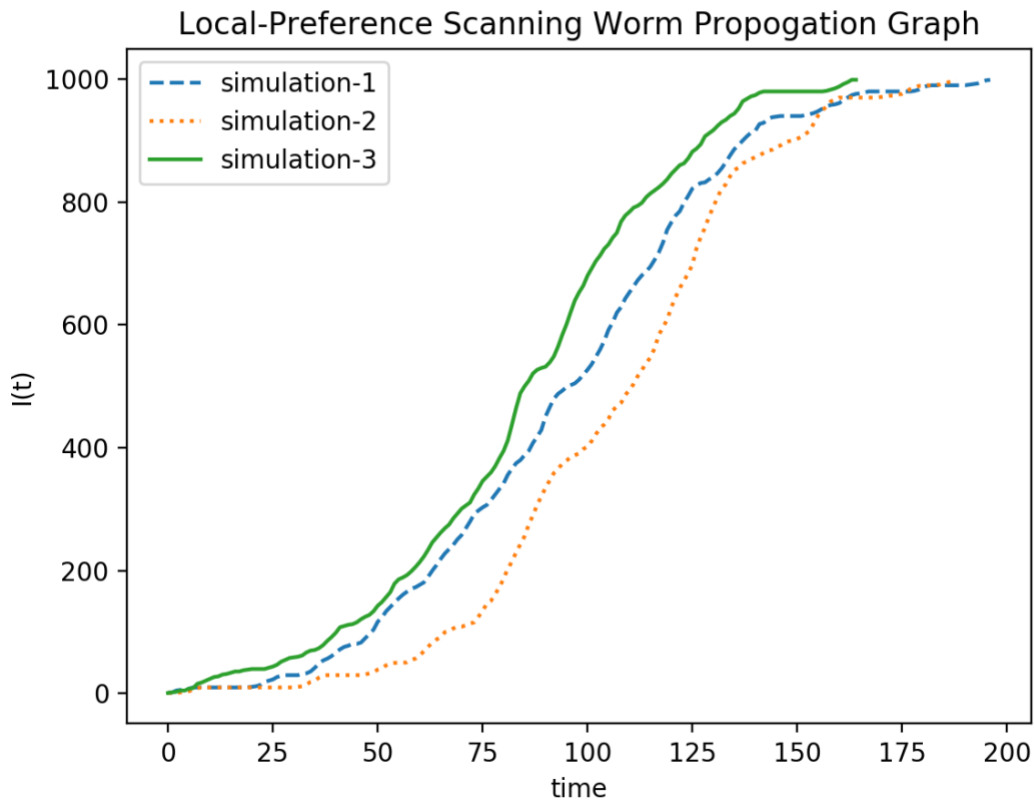**Graph of Random-Scanning Worm Propagation:**
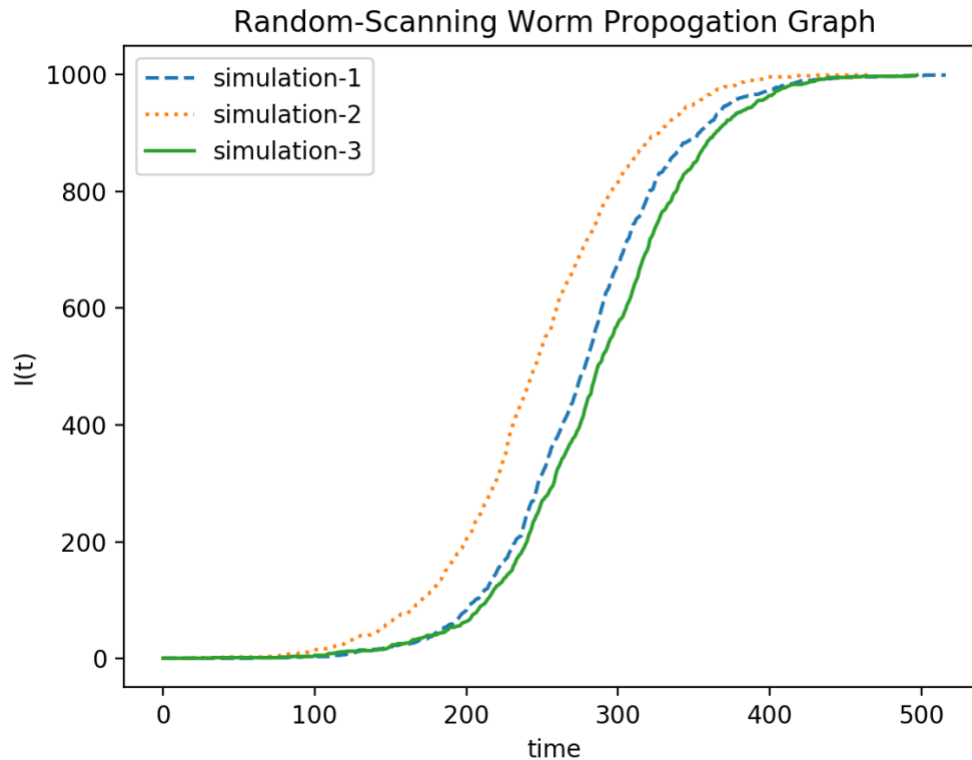


**Output showing time taken for infection in Random-Scanning Worm Propagation:**

```
[Aahanas-MBP:Desktop aahana$ python3 Prog_assignment3.1.py
Iteration 1:
100% (1000 of 1000) |########################| Elapsed Time: 0:05:32 Time:  0:05:32
Iteration 2:
100% (1000 of 1000) |########################| Elapsed Time: 0:04:54 Time:  0:04:54
Iteration 3:
100% (1000 of 1000) |########################| Elapsed Time: 0:04:20 Time:  0:04:20
Number of time steps taken to infect all 1000 vulnerable computers in simulation-1:  517
Number of time steps taken to infect all 1000 vulnerable computers in simulation-2:  467
Number of time steps taken to infect all 1000 vulnerable computers in simulation-3:  498
```

MALWARE PROPOGATION – PROGRAMMING ASSIGNMENT 3

Graph of Local-Preference Scanning Worm Propagation:

Output showing time taken for infection in Local-Preference Scanning Worm Propagation:

```
[Aahanas-MBP:Desktop aahana$ python3 Prog_assignment3.2.py
Iteration 1:
100% (1000 of 1000) |########################| Elapsed Time: 0:02:08 Time:  0:02:08
Iteration 2:
100% (1000 of 1000) |########################| Elapsed Time: 0:01:42 Time:  0:01:42
Iteration 3:
100% (1000 of 1000) |########################| Elapsed Time: 0:01:39 Time:  0:01:39
Number of time steps taken to infect all 1000 vulnerable computers in simulation-1:  197
Number of time steps taken to infect all 1000 vulnerable computers in simulation-2:  189
Number of time steps taken to infect all 1000 vulnerable computers in simulation-3:  165
```