University of Central Florida

Department of Computer Science

CAP 6135 : Malware and Software Vulnerability Analysis

Spring 2023

Programming Assignment 3: Worm Propagation Simulation

by

Aakash Shah

---

1. Worm Propagation Description:

- Assume that in an isolated network (mini Internet) with **A=50,000** IP address space. The IP addresses can be treated as having value from 1 to 50,000. There are **N = 500** computers vulnerable to the worm under consideration in this network. These vulnerable computers have the following specific IP addresses:
- 1, 2, 3,…, 10
- 1001, 1002, …., 1010,
- 2001, 2002, …, 2010,
- …..
- 49001, 49002, …, 49010
- That is, every cluster of 50 computers with contiguous IP addresses is vulnerable to the worm, and there is one cluster of 50 vulnerable computers for every 1000 contiguous IP addresses (for a total of 10 clusters of vulnerable computers). The remaining 49,500 IP addresses are not vulnerable to this worm.

- Now suppose the worm starts infecting this network on the first infected machine with the IP address of 2010. At every discrete time tick t, the worm-infected computer sends B scans and contacts to B IP address within this network (remember, there are only 50,000 IP addresses in the network). If at time t the scan hits a vulnerable computer, the vulnerable computer is considered "infected" at time t+1. However, this newly infected computer is silent and starts scanning others only at discrete time tick t+20. We use I(t) to represent the number of computers infected at time t (t=1, 2, 3, ...). So initially I(0) = 1. This initially infected computer scans the IP space immediately, starting at time t=1.

2. Instruction to run the code

- Unzip the submitted zip file
- One need to install the libraries as below if not installed:
  pip3 install random
  pip3 install matplotlib
  pip3 install numpy
- Run the code:
  python random_scan.py
  python simulation_scan.py

3. Implementation

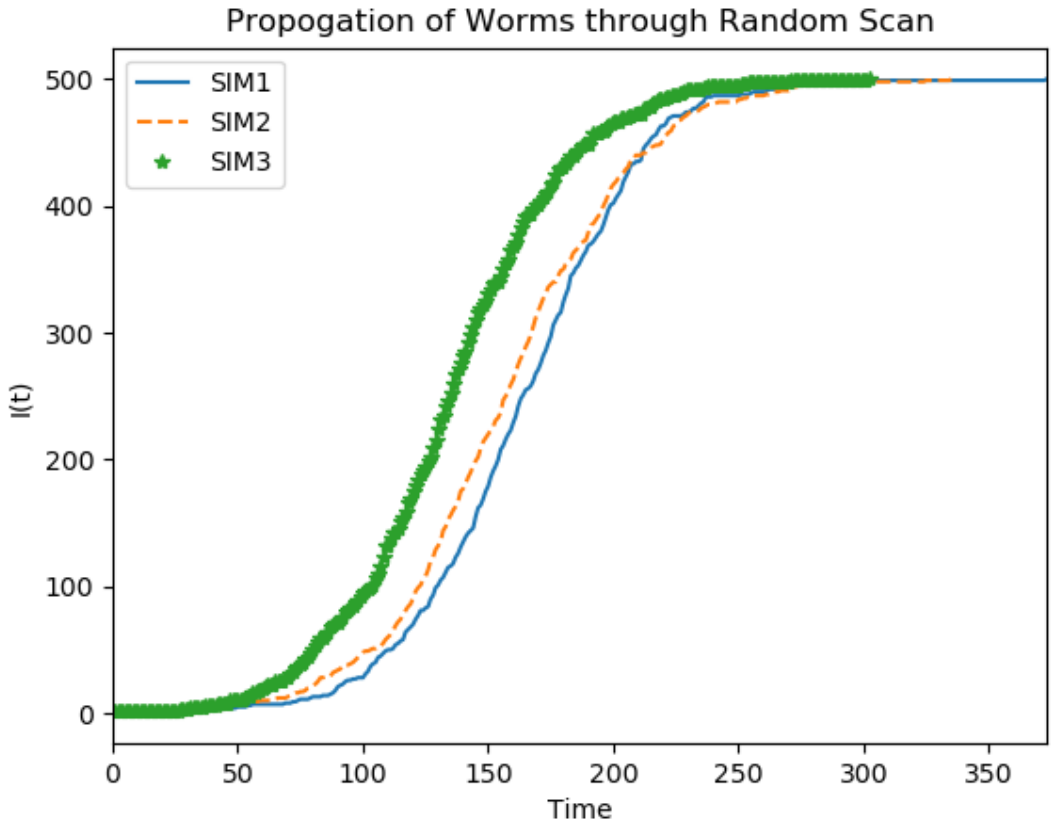
- **Random scan worm propagation simulation**
  We simulate a worm propagation with the scan rate of **4** (i.e., an infected computer scans 4 IPs in a time unit). Then to simulate the worm propagation for 3 independent simulation runs we get the vector of the number of infected, ***I(t)***, 3 times. Each of the simulation run ends when all vulnerable machines have been infected.
- **Sequential scan worm propagation simulation**

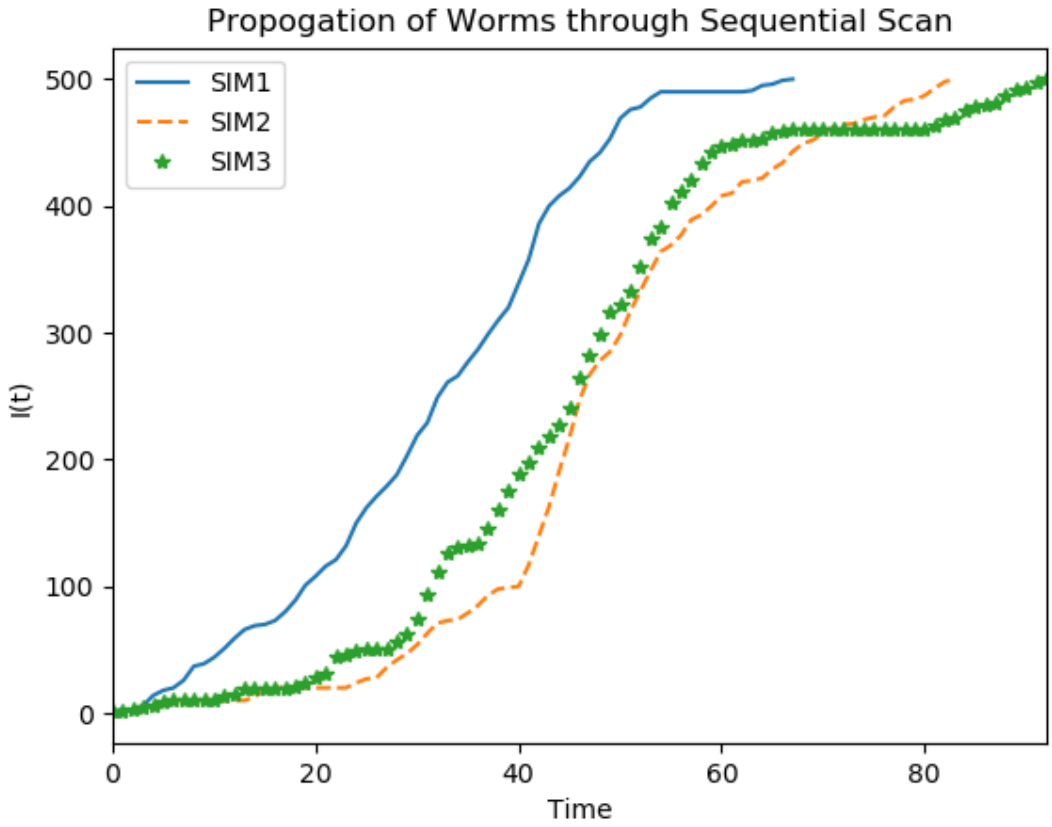
We simulate sequential scanning strategy. When a vulnerable computer with an IP address value of x is infected, it modifies its scan behavior to either a sequential scan host with a 70% chance or a random scan host with a 30% chance.

- For a sequential-scanning node, it picks the scanning target IP addresses ***y*** sequentially after its own IP value, i.e., x+1, x+2, x+3,.... When the scanned IP address reaches 50,000, the next IP to scan would be with value of 1.
- For a random-scanning node, it picks a random target IP value **y** between 1 to 50,000.

Again we assume that the worm starts its infection within this network from 1 initially infected machine, which has the IP address of **2010**. Then we simulate the worm propagation with scan rate of 4 for 3 simulation runs.

4. Figures


Propogation of Worms through Random Scan
SIM1
SIM2
SIM3
I(t)
Time
0
100
200
300
400
500
0
50
100
150
200
250
300
350


Propogation of Worms through Sequential Scan
SIM1
SIM2
SIM3
I(t)
Time
0
100
200
300
400
500
0
20
40
60
80

OUTPUT:

```
aa073875@net1547:~/Assign_3$ python random_scan.py
Time ticks for simulation 1:  334
Time ticks for simulation 2:  353
Time ticks for simulation 3:  277
aa073875@net1547:~/Assign_3$ python random_scan.py
Time ticks for simulation 1:  307
Time ticks for simulation 2:  428
Time ticks for simulation 3:  455
aa073875@net1547:~/Assign_3$ python random_scan.py
Time ticks for simulation 1:  330
Time ticks for simulation 2:  273
Time ticks for simulation 3:  263
aa073875@net1547:~/Assign_3$ python random_scan.py
Time ticks for simulation 1:  306
Time ticks for simulation 2:  335
Time ticks for simulation 3:  487
aa073875@net1547:~/Assign_3$ python random_scan.py
Time ticks for simulation 1:  374
Time ticks for simulation 2:  336
Time ticks for simulation 3:  303
```

```
aa073875@net1547:~/Assign_3$ python sequential_scan.py
Time ticks for simulation 1:  117
Time ticks for simulation 2:  68
Time ticks for simulation 3:  85
aa073875@net1547:~/Assign_3$ python sequential_scan.py
Time ticks for simulation 1:  75
Time ticks for simulation 2:  71
Time ticks for simulation 3:  109
aa073875@net1547:~/Assign_3$ python sequential_scan.py
Time ticks for simulation 1:  87
Time ticks for simulation 2:  75
Time ticks for simulation 3:  98
aa073875@net1547:~/Assign_3$ python sequential_scan.py
Time ticks for simulation 1:  58
Time ticks for simulation 2:  78
Time ticks for simulation 3:  77
aa073875@net1547:~/Assign_3$ python sequential_scan.py
Time ticks for simulation 1:  85
Time ticks for simulation 2:  93
Time ticks for simulation 3:  59
```