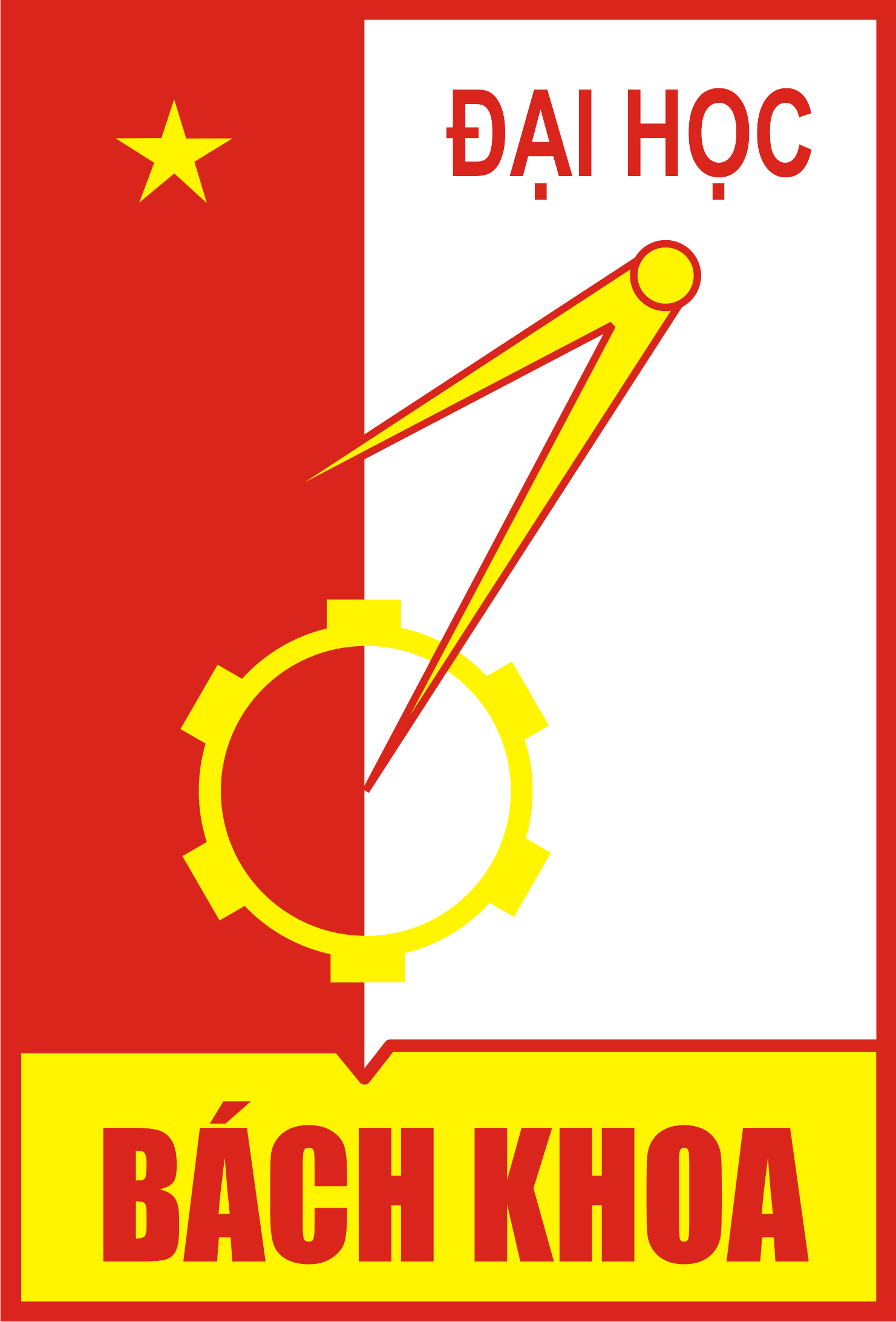
**HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF INTERNATIONAL EDUCATION**

****

**Agent Software Engineering**

**Virus on a Network**

**Lecturer: PGS.TS. Cao Tuan Dung**

**Student: Nguyen Van Cao**

**MSSV: 20138707**

**HA NOI 2018**

Table of Contents

[I. Bài toán thực tế 1](#_Toc514855405)

[1. What is a Computer Virus? 1](#_Toc514855406)

[2. How does a computer virus attack? 2](#_Toc514855407)

[3. How do computer viruses spread? 2](#_Toc514855408)

[4. Type of Virus 2](#_Toc514855409)

[5. How to protect against computer viruses? 4](#_Toc514855410)

[II. Simulated in NetLogo 6](#_Toc514855411)

[1. Theoretical basis 6](#_Toc514855412)

[1.1. What is it? 6](#_Toc514855413)

[1.2. How it work 6](#_Toc514855414)

[1.3. How to use it 6](#_Toc514855415)

[1.4. Things to notice 7](#_Toc514855416)

[1.5. Things to try 7](#_Toc514855417)

[2. Source code 7](#_Toc514855418)

[2.1. Components used? 7](#_Toc514855419)

[2.2. Analys source code 9](#_Toc514855420)

[2.3. Một số chỉnh sửa 9](#_Toc514855421)

1. **Bài toán thực tế**
2. **What is a Computer Virus?**

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator. In contrast, a computer worm is stand-alone programming that does not need to copy itself to a host program or require human interaction to spread. Viruses and worms may also be referred to as malware.

The term "virus" is also commonly, but erroneously, used to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer "worms", ransomware, spyware, adware, trojan horses, keyloggers, rootkits, bootkits, malicious Browser Helper Object (BHOs) and other malicious software. The majority of active malware threats are actually trojan horse programs or computer worms rather than computer viruses. The term computer virus, coined by Fred Cohen in 1985, is a misnomer. Viruses often perform some type of harmful activity on infected host computers, such as acquisition of hard disk space or central processing unit (CPU) time, accessing private information (e.g., credit card numbers), corrupting data, displaying political or humorous messages on the user's screen, spamming their e-mail contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive "payload" and attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which modify other software without user consent.

1. **How does a computer virus attack?**

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed. This means that a virus can remain dormant on your computer, without showing major sings or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.

While some viruses can be playful in intent and effect, others can have profound and damaging effects, such as erasing data or causing permanent damage to your hard disk, and worst yet, some are even design with financial gains in mind.

1. **How do computer viruses spread?**

A virus can be spread by opening an email attachment, clicking on an executable file, visiting an infected website or viewing an infected website advertisement. It can also be spread through infected removable storage devices, such USB drives. Once a virus has infected the host, it can infect other system software or resources, modify or disable core functions or applications, as well as copy, delete or encrypt data. Some viruses begin replicating as soon as they infect the host, while other viruses will lie dormant until a specific trigger causes malicious code to be executed by the device or system. Many viruses also include evasion or obfuscation capabilities that are designed to bypass modern antivirus and antimalware software and other security defenses. The rise of polymorphic malware development, which can dynamically change its code as it spreads, has also made viruses more difficult to detect and identify.

1. **Type of Virus**

* **File infectors**: Some file infector viruses attach themselves to program files, usually selected .com or .exe files. Some can infect any program for which execution is requested, including .sys, .ovl, .prg, and .mnu files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly contained programs or scripts sent as an attachment to an email note.
* **Macro viruses**: These viruses specifically target macro language commands in applications like Microsoft Word and other programs. In Word, macros are saved sequences for commands or keystrokes that are embedded in the documents. Macro viruses can add their malicious code to the legitimate macro sequences in a Word file. Microsoft disabled macros by default in more recent versions of Word; as a result, hackers have used social engineering schemes to convince targeted users to enable macros and launch the virus. As macro viruses have seen a resurgence in recent years, Microsoft added a new feature in Office 2016 that allows security managers to selectively enable macro use for trusted workflows only, as well as block macros across an organization.
* **Overwrite viruses**: Some viruses are designed specifically to destroy a file or application's data. After infecting a system, an overwrite virus begins overwriting files with its own code. These viruses can target specific files or applications or systematically overwrite all files on an infected device. An overwrite virus can install new code in files and applications that programs them to spread the virus to additional files, applications and systems.
* **Polymorphic viruses**: A polymorphic virus is a type of malware that has the ability to change or mutate its underlying code without changing its basic functions or features. This process helps a virus evade detection from many antimalware and threat detection products that rely on identifying signatures of malware; once a polymorphic virus' signature is identified by a security product, the virus can then alter itself so that it will no longer be detected using that signature.
* **Resident viruses**: This type of virus embeds itself in the memory of a system. The original virus program isn't needed to infect new files or applications; even if the original virus is deleted, the version stored in memory can be activated when the operating system loads a specific application or function. Resident viruses are problematic because they can evade antivirus and antimalware software by hiding in the system's RAM.
* **Rootkit viruses**: A rootkit virus is a type of malware that installs an unauthorized rootkit on an infected system, giving attackers full control of the system with the ability to fundamentally modify or disable functions and programs. Rootkit viruses were designed to bypass antivirus software, which typically scanned only applications and files. More recent versions of major antivirus and antimalware programs include rootkit scanning to identify and mitigate these types of viruses.
* **System or boot-record infectors**: These viruses infect executable code found in certain system areas on a disk. They attach to the DOS bootsector on diskettes and USB thumb drives or the Master Boot Record on hard disks. In a typical attack scenario, the victim receives storage device that contains a boot disk virus. When the victim's operating system is running, files on the external storage device can infect the system; rebooting the system will trigger the boot disk virus. An infected storage device connected to a computer can modify or even replace the existing boot code on the infected system so that when the system is booted next, the virus will be loaded and run immediately as part of the master boot record. Boot viruses are less common now as today's devices rely less on physical storage media.

1. **How to protect against computer viruses?**

To avoid contact with a virus it’s important to exercise caution when surfing the web, downloading files, and opening links or attachments. As a best practice, never download text or email attachments that you’re not expecting, or files from websites you don’t trust.

Some anti-virus methods:

* Buy legitimate software, and register it.
* Make sure your software is up to date.
* Don’t click on links or open attachments from email addresses you don’t know.
* Instantly leave websites you’ve been routed to without your consent.
* Have a pop-up blocker running on your web browser.
* Use a reputable antivirus program, and always keep it updated.
* Regularly back up your important files to an external drive or a remote storage service.

1. **Simulated in NetLogo**
2. **Theoretical basis**
   1. **What is it?**

This model demonstrates the spread of a virus through a network. Although the model is somewhat abstract, one interpretation is that each node represents a computer, and we are modeling the progress of a computer virus (or worm) through this network. Each node may be in one of three states: susceptible, infected, or resistant. In the academic literature such a model is sometimes referred to as an SIR model for epidemics.

* 1. **How it work**
* Each time step (tick), each infected node (colored red) attempts to infect all of its neighbors. Susceptible neighbors (colored green) will be infected with a probability given by the **VIRUS-SPREAD-CHANCE** slider. This might correspond to the probability that someone on the susceptible system actually executes the infected email attachment. Resistant nodes (colored gray) cannot be infected. This might correspond to up-to-date antivirus software and security patches that make a computer immune to this particular virus.
* Infected nodes are not immediately aware that they are infected. Only every so often (determined by the **VIRUS-CHECK-FREQUENCY** slider) do the nodes check whether they are infected by a virus. This might correspond to a regularly scheduled virus-scan procedure, or simply a human noticing something fishy about how the computer is behaving. When the virus has been detected, there is a probability that the virus will be removed (determined by the **RECOVERY-CHANCE** slider).
* If a node does recover, there is some probability that it will become resistant to this virus in the future (given by the **GAIN-RESISTANCE-CHANCE** slider).
* When a node becomes resistant, the links between it and its neighbors are darkened, since they are no longer possible vectors for spreading the virus.
  1. **How to use it**
* Using the sliders, choose the **NUMBER-OF-NODES** and the **AVERAGE-NODE-DEGREE** (average number of links coming out of each node).
* The network that is created is based on proximity (Euclidean distance) between nodes. A node is randomly chosen and connected to the nearest node that it is not already connected to. This process is repeated until the network has the correct number of links to give the specified average node degree.
* The **INITIAL-OUTBREAK-SIZE** slider determines how many of the nodes will start the simulation infected with the virus.
* Then press **SETUP** to create the network. Press **GO** to run the model. The model will stop running once the virus has completely died out.
* The **VIRUS-SPREAD-CHANCE**, **VIRUS-CHECK-FREQUENCY**, **RECOVERY-CHANCE**, and **GAIN-RESISTANCE-CHANCE** sliders (discussed in "How it Works" above) can be adjusted before pressing GO, or while the model is running.
* The **NETWORK STATUS** plot shows the number of nodes in each state (S, I, R) over time.
  1. **Things to notice**

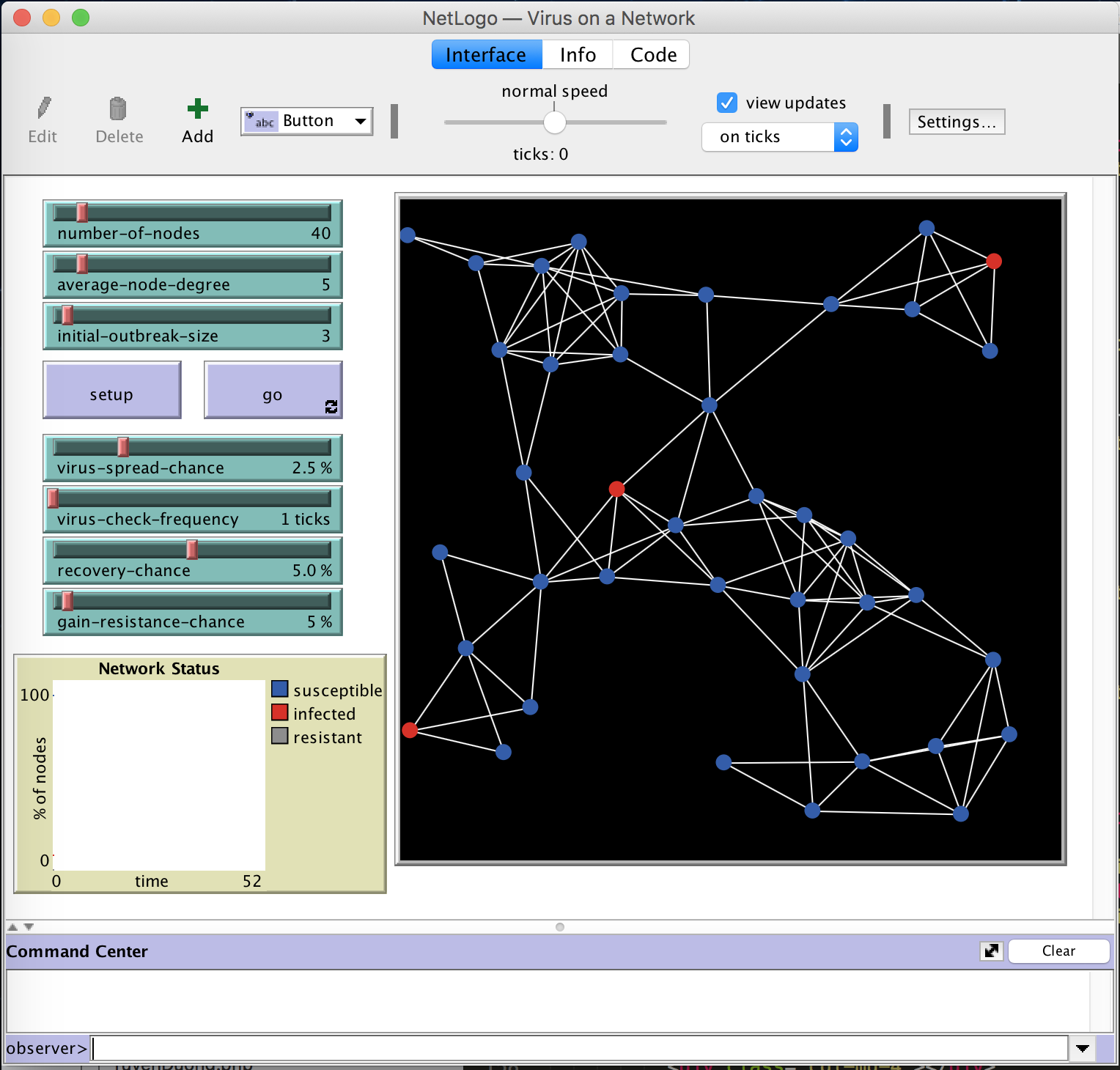
At the end of the run, after the virus has died out, some nodes are still susceptible, while others have become immune. What is the ratio of the number of immune nodes to the number of susceptible nodes? How is this affected by changing the **AVERAGE-NODE-DEGREE** of the network?

* 1. **Things to try**

Set **GAIN-RESISTANCE-CHANCE** to 0%. Under what conditions will the virus still die out? How long does it take? What conditions are required for the virus to live? If the **RECOVERY-CHANCE** is bigger than 0, even if the **VIRUS-SPREAD-CHANCE** is high, do you think that if you could run the model forever, the virus could stay alive?

1. **Source code**
   1. **Components used?**

* **Kinds of Agents**
  + **Turles:** is the node on the screen. Each node represents a PC.
  + **Link:** Presentationthe association of nodes is related.
* **Control:**
  + **Slider:**
    - **NUMBER-OF-NODES:** defines the number of nodes in the network
    - **AVERAGE-NODE-DEGREE:** average number of links coming out of each node
    - **INITIAL-OUTBREAK-SIZE:** determines how many of the nodes will start the simulation infected with the virus.
    - **VIRUS-SPREAD-CHANCE:** Green node probability is infected by red neighbor node
    - **VIRUS-CHECK-FREQUENCY:** frequency time check virus of system (n ticks / 1 check)
    - **RECOVERY-CHANCE:** there is a probability that the virus will be removed when the virus has been detected
    - **GAIN-RESISTANCE-CHANCE:** Resolve the virus after recovery.
  + **Button:**
    - **SETUP:** setup environment after defined
    - **GO:** Run algorithms in code
  + **Plot: NETWORK STATUS:** The graph shows the increase and decrease of the three types of nodes over time



* 1. **Analys source code**
  2. **Một số chỉnh sửa**