INTELLIGENT AGENT-BASED TECHNOLOGIES FOR NETWORK WORMS SIMULATION

Kamaeva Kristina, student of group 345
Chumachenko Dmytro, Associate Professor of Mathematical modelling and artificial intelligence department
National Aerospace University "Kharkiv Aviation Institute"

Widespread use and easy access to the Internet makes it a prime target for malicious activities. In particular, the Internet has become a powerful mechanism for malware distribution. Network worms, stand-alone programs that spread through computer networks using automatic search, attacks and infection of remote computers, have been developed for almost 30 years since the first Morris worm. In modern conditions, computer infrastructure is more vulnerable than ever before, because The speed of technology development is much higher than the speed of developing their protective measures.

Developing an accurate Internet worm model will give an idea of its behavior. This will identify weak points in the dynamics of the network worm, as well as create a forecast of its distribution in order to assess the damage from the worm's activities. In epidemiological studies, there are several deterministic and stochastic models for the spread of viral diseases; also, some models exist for modeling the spread of Internet worms, but they do not allow for the dynamic nature of the development of the malware epidemic process.

As part of this study, a multi-agent model of network worm propagation has been developed using the example of the Code Red worm, which helps eliminate the shortcomings of deterministic analytical models.

The adequacy of the multi-agent model largely depends on the number of agents in the system. The use of large populations and the specification of the properties of agents leads to the need to use the most modern information tools and technologies, in particular, algorithms that are optimal in the number of machine operations performed. In a multi-agent approach, the modeling process is based on building and processing an event queue, which can be divided into two types:

1. Changing the state of the agent in terms of the external environment (the physical position of the agent);
2. Change the internal state of the agent. Events of this type arise as a result of the interaction of the agent with other agents, as well as with the external environment.

The task is to find and use such a set of properties and methods of agents as objects, which would allow to take the most advantage of the multi-agent approach.

In the software package "Agent-based system of computer worms distribution in fully connected heterogeneous networks" MASWorm ", a formal

description of the constructed model is proposed. An agent can be considered as a set of parameters:

$$a = \langle s, s_t, c, l \rangle, \ a \in A, s \in S, c \in C, \quad (1)$$

where s_t is the residence time of the agent in state s; A is the number of agents; S is the number of possible states; l is life expectancy; C is the set of cells in the workspace.

The set of agent states is predefined and permanent. In the developed model, we define the set of states as:

$$S=\{Susceptible, Antidotal, Infected, Detected, Recovered\}. \quad (2)$$

where *Susceptible* is an agent is healthy and susceptible to infection by a specific worm,

Antidotal agent is healthy. Agents in this state have installed anti-virus software, therefore they cannot be infected,

Infected agent is infected and can be a carrier of the virus to other hosts,

Detected agent infection is detected by antivirus software and isolated from the network,

Recovered agent is cured and is no longer susceptible to this type of worm.

An analysis of the developed multi-agent model showed that there are two factors affecting the spread of the Code Red network worm: dynamic countermeasures taken by the ISP and users, and slowing down the speed of the network worm propagation, since the rapid reproduction of the Code Red worm caused slowdowns and problems with some routers. . Considering the dynamic aspects of human countermeasures and the variable rate of infection, we have obtained a more accurate model of the propagation of a network worm, in comparison with deterministic analytical models. The simulation results, as well as the numerical solution, show that the constructed multi-agent model to a high degree coincides with the observed real data of the Code Red worm. In particular, this explains the decrease in attempts to scan hosts during the last few hours of the spread of the worm; none of the previous deterministic models can explain this phenomenon.