Dynamics of Malware Spread in Decentralized Peer-to-Peer Networks

ABSTRACT:
In this paper, we formulate an analytical model to characterize the spread of malware in decentralized, Gnutella type peer-to-peer (P2P) networks and study the dynamics associated with the spread of malware. Using a compartmental model, we derive the system parameters or network conditions under which the P2P network may reach a malware free equilibrium. The model also evaluates the effect of control strategies like node quarantine on stifling the spread of malware. The model is then extended to consider the impact of P2P networks on the malware spread in networks of smart cell phones.

Existing System:

- In previous simulation model uses a combination of the deterministic epidemic model and a general stochastic epidemic model to model the effect of large-scale worm attacks.

- In an Existing system the complexity of the general stochastic epidemic model makes it difficult to derive insightful results that could be used to contain the worm.

- In a previous study it is used to detect the presence of a worm by detecting the trend, not the rate, of the observed illegitimate scan traffic.

- The filter is used to separate worm traffic from background non worm scan traffic.
Proposed System:

- This model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage.

- We obtain the probability that the total number of hosts that the worm infects is below a certain level.

- Our strategy can effectively contain both fast scan worms and slow scan worms without knowing the worm signature in advance or needing to explicitly detect the worm.

- Our automatic worm containment schemes effectively contain the worms and stop its spreading.

HARDWARE REQUIREMENTS

- SYSTEM : Pentium IV 2.4 GHz
- HARD DISK : 40 GB
- MONITOR : 15 VGA colour
- MOUSE : Logitech.
- RAM : 256 MB
- KEYBOARD : 110 keys enhanced.
SOFTWARE REQUIREMENTS

- Operating system : Windows XP Professional
- Front End : JAVA
- Tool : NETBEANS IDE

Modules of the Project

- User Interface Design
- Worm Propagation Model
- Scanning for worms
- Detecting and categorizing worms
- Containment of worms

Module Description

User Interface Design

In this module we have designed the user interface for all the hosts. We design the user interface to show our propagation of worms in a graphical manner or GUI. By showing the output in GUI gives more attractive and understandable to everyone. Then we design the containment window to show the scanning, detection of worms. Thus we design the whole user interface in this module.

Worm Propagation Model

In this module, we create a worm spreading model. This model is designed for the propagation of worms inside a network. Inside the network we spread the worms in a controlled environment. To create worm propagation model we need to form a network
by using the server socket class and socket class available in Java. These two classes are used to create a connection to transfer data from a host to other host inside a network.

**Scanning for worms**

Our strategy is based on limiting the number of scans to dark-address space. The limiting value is determined by our analysis. Our automatic worm containment schemes effectively contain both uniform scanning worms and local preference scanning worms, and it is validated through simulations and real trace data to be non-intrusive.

**Detecting and categorizing worms**

The model is developed for uniform scanning worms and then extended to preference scanning worms. We detect these two worms and categorize it in this module.

**Containment of worms**

This model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, we are able to 1) provide a precise condition that determines whether the worm spread will eventually stop and 2) obtain the distribution of the total number of hosts that the worm infects.

**REFERENCE:**

Krishna, Ramachandran and Biplab Sikdar, “Dynamics of Malware Spread in Decentralized Peer-to-Peer Networks”, *IEEE Transactions on Dependable and Secure Computing, Vol. 8, No.4, July/August 2011.*