**SPIDER ALERT**

**ABSTRACT**

Social network worms, such as email worms and face book worms, pose a critical security threat to the Internet. Modeling their propagation dynamics is essential to predict their potential damages and develop countermeasures. Although several analytical models have been proposed for modeling propagation dynamics of social network worms, there are two critical problems unsolved: temporal dynamics and spatial dependence. First, previous models have not taken into account the different time periods of Internet users checking emails or social messages, namely, temporal dynamics. Second, the problem of spatial dependence results from the improper assumption that the states of neighboring nodes are independent. These two problems seriously affect the accuracy of the previous analytical models. To address these two problems, we propose a novel analytical model. This model implements a spatial temporal synchronization process, which is able to capture the temporal dynamics. Additionally, we find the essence of spatial dependence is the spreading cycles. By eliminating the effect of these cycles, our model overcomes the computational challenge of spatial dependence and provides a stronger approximation to the propagation dynamics. To evaluate our susceptible-infectious immunized (SII) model, we conduct both theoretical analysis and extensive simulations. Compared with previous epidemic models and the spatial-temporal model, the experimental results show our SII model achieves a greater accuracy. We also compare our model with the susceptible-infectious-susceptible and susceptible-infectious-recovered models. The results show that our model is more suitable for modeling the propagation of social network worms.

**Existing system**

The existing system Social networks have become attractive targets for worm creators because of the following characteristics. First, they rely on the information like contact lists contained in a victim’s machine to locate new targets. This intelligent mechanism allows far more efficient propagation than traditional scanning worms that make a large number of wild guesses for every successful infection. Second, by using social engineering techniques exploiting trust in social networks, many users fail to recognize malicious codes that are sent by their friends and subsequently become infected. This results in a wide range that worms propagate to. Third, researchers have found that social networks exhibit both small world properties and scale-free behaviors. This means that the spreading of social network worms can be incredibly fast because the highly connected “hub” nodes of a scale-free network and the short paths in a strongly clustered small world will greatly facilitate the propagation of an infection over the whole network.

**Disadvantages**

1. The virus spread of social network worms depends on human involvement. That is Internet users periodically check their newly arrived emails or messages, and are lured to open those which are actually worm copies.
2. The period for checking these emails or messages depends on users’ own patterns.
3. Previous models cannot present accurate and realistic spreading procedure.
4. The spreading of social network worms relies on the topology of social networks. In the modeling,
5. The probability of a node being infected will increase when its neighbors have been infected.

**Proposed system**

In this proposed system extensive analyses on two important problems, temporal dynamics and spatial dependence, which crucially affect the accuracy of the existing analytical models. Our analysis shows that previous works cannot model the realistic propagation with different checking time periods of users. Moreover, the analysis shows the spreading cycles formed in the modeling lead to considerable errors in estimating the infection probabilities. We propose a novel SII model. This model implements a spatial-temporal synchronization process, which helps us to solve the problem of modeling temporal dynamics. Furthermore, by eliminating the effect of those cycles, the SII model overcomes the computational challenge and provides a stronger approximation of spatial dependence.

**Advantages**

1. SII model is able to address two critical problems unsolved in the previous analytical models: temporal dynamics and spatial dependence.
2. Stronger approximation to the spatial dependence
3. SII model is accurate for modeling the spread of social network worms
4. SII model is more suitable for modeling the propagation of social network worms

**Modules**

1. Network analyzer
2. Node creation
3. Data transfer
4. Virus Propagation
5. Find affect nodes

**Network analyzer**

The network has divided by workgroups. This module will help us to get the connected and the active systems in the network. After getting login to our process, this module will get the connected systems and shows to the users. The user can select the system to deliver their data by file transfer.

In this module, each node registers the details such as Node IP address. Nodes details are stored and maintained in sever. After that Nodes enter the ip and to activate themselves in the network.

**Node creation**

In this module we have registered the node name and IP address this detail store the Database After click Login page enter the node name and sender decides to send data to receiver, it performs Data and sends the result to receiver, node creation id identification of data path.

**Data transfer**

The user has choice for browse the file to send. And it the data send to the receiver. By the receiver can gets the data will be sent by sender .And then the choice is authentication to produce it all.

Generally in network before transmission the data’s are converted into the network adaptable format, only these converted data are transmitted on the network. In this module the transmitted data are converted to data by using the coding and modulation technique.

**Virus Propagation**

In this module spreading of social network worms can be incredibly fast because the highly connected nodes of a scale-free network and the short paths in a strongly clustered small world will greatly facilitate the propagation of an infection over the whole network nodes.

In this module we drop the corrupted node by using the Cyclic Redundancy Check. Data packet is correct, the packet acknowledgment will be sent back to transmitter. Otherwise, the receiver drops the corrupted data packet and waits for the packet retransmission.

**Find affect nodes**

In this module SII model is find the spread of social network worm scan finds the virus and blocks the transaction from that abnormal file. SII is used for find Propagation. in this modules find the affected node from sender data. if virus data is detected node find the not send to receiver.

**SOFTWARE CONFIGURATION:**

* Front End : VISUAL STUDIO.NET 2008
* Code Behind : C#.NET
* Back End : SQL SERVER 2005
* Operating System : Windows 10

**HARDWARE CONFIGURATION:**

* Hard disk : 500 GB
* RAM : 2GB
* Processor : I3
* Monitor : 17” Color monitor
* Key board, Mouse : Multi media