# Worm Simulation with a Realistic Internet Model

Georgia Institute of Technology

ECE 6110 CAD for Computer Networks

Fall 2017

Georgia Tech School of Electrical and Computer Engineering
College of Engineering

Xueyang Xu (GT ID: 903234112)

Xingyu Liu (GT ID: 903233948)

Yunwei Qiang (GT ID: 903231467)

Wenxin Fang (GT ID: 903231847)

Nan Li (GT ID: 903230813)

## Background

Internet worm spread is a phenomenon involving millions of hosts, who interact in complex and diverse environment. Aggressive worms further interact with the underlying Internet topology - the dynamics of the spread is constrained by the limited bandwidth of network links, and high-volume scan traffic leads to BGP router failure thus affecting global routing. Worm traffic also interacts with legitimate background traffic competing for (and often winning) the limited bandwidth resources.

To faithfully simulate worm spread and other Internet-wide events such as DDoS, flash crowds and spam we need a detailed Internet model, a packet-level simulation of relevant event features, and a realistic model of background traffic on the whole Internet.

With proposed model and implementation of a distributed worm simulator, called PAWS, we validate PAWS in a variety of scenarios, and evaluate costs and benefits of distributed worm simulation.

## What you're going to do?

In this project, we will provide a worm simulation with a more realistic internet model than previous projects. We will mainly focus on two types of worm, Code Red 2 and Slammer.

Both worms are well-known for their widely spreading in early 2000s. Furthermore, we will inspect the pattern of their behavior under different circumstances. For instance, the spreading pattern of worms may vary under different level of background traffic and limited bandwidth.

Also, whether applying defense measures can result to different outcomes. Patching and quarantine defense can be chosen as a defensive method and start taking effect at a specific time during the propagation stage of worm. By running simulation under such different situation, we can acquire a comprehensive understanding of worm spreading in realistic internet.

## What type of experiments you're going to run?

We simulate two well-known worm spread events: Code Red 2 and SQL Slammer. In addition to worms, we also simulate realistic internet traffic and consider different conditions:   presence of worm defenses, limited bandwidth of network links and high-volume scan traffic. In conclusion, we are going to run four experiments as below.

a. Simulate three CRv2 worm spread events (propagation without patching, propagation with universal patching, propagation with subnet patching).

b. Simulate Slammer congestion-constrained worm spread and occurrence of router failures due to large volume of scan traffic.
c. Simulate number of scans in the Internet for worm propagation with and without the router failure.

d. Simulate with different bandwidth values.

## What you expect to find out by running these experiments

We are going to explore through a variety of parameters (BW, worm type etc.) to find out the worm behavior with respect to different network conditions, and further come out effective solution to worm attacks.

a. By simulating three CRv2 worm spread events, we expect to find out the number of infected hosts with patching should be less than the number of infected hosts without patching; universal patching should be better in defending worm propagation. (See Figure 2)

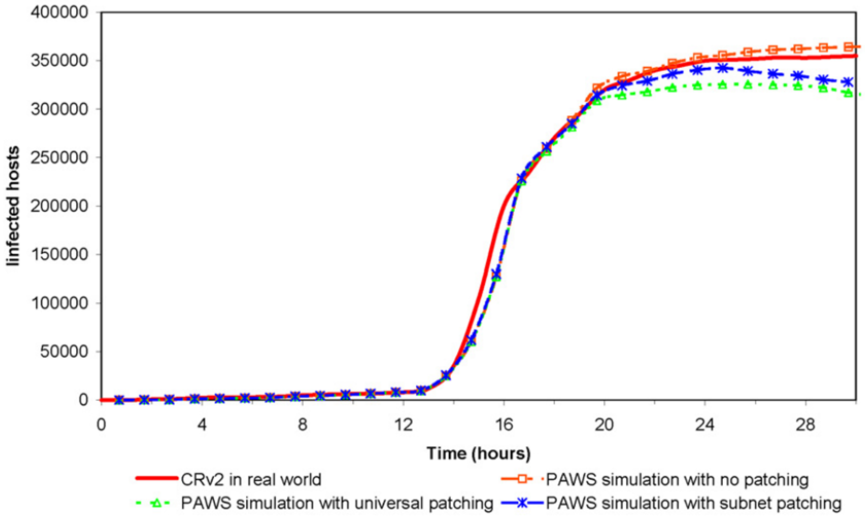

**Figure 2: Simulation of CRv2**

b. By simulating Slammer congestion-constrained worm spread and occurrence of router failures due to large volume of scan traffic, we expect to find out that the infected rate with router failure should be smaller than the infected rate without router failure within the same time range. (See Figure 3)

c. By simulating number of scans in the Internet for worm propagation with and without the router failure, we expect to find out that parts of scans will be drop due to router failure. (See Figure 3)

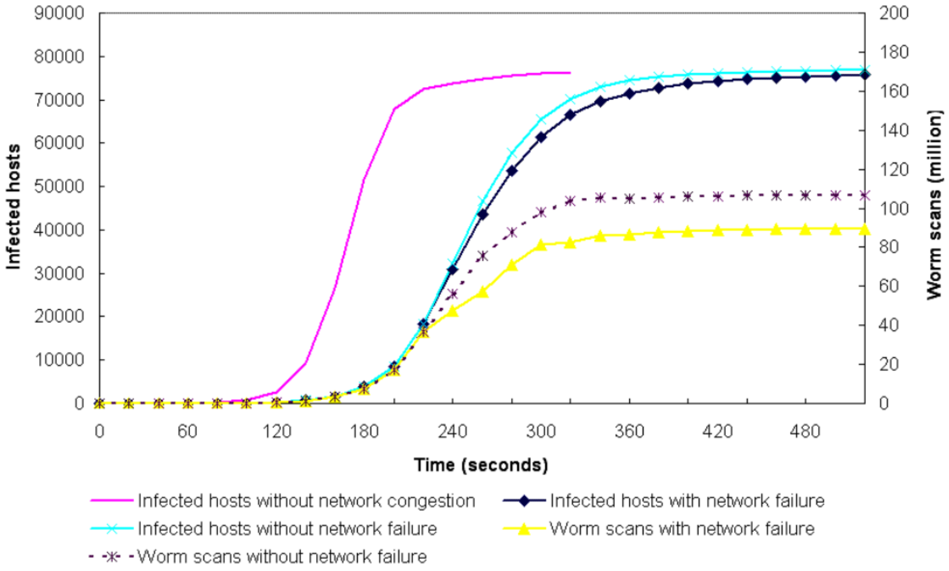

**Figure 3: Simulation of Slammer**

d. By simulate network conditions (infected hosts, worm scans etc.) with three different bandwidth assignments, we expect to compare the worm propagation with respect to bandwidth and validate the assertion that the propagation rate can be slowed by choosing smaller bandwidth. (See Figure 4)

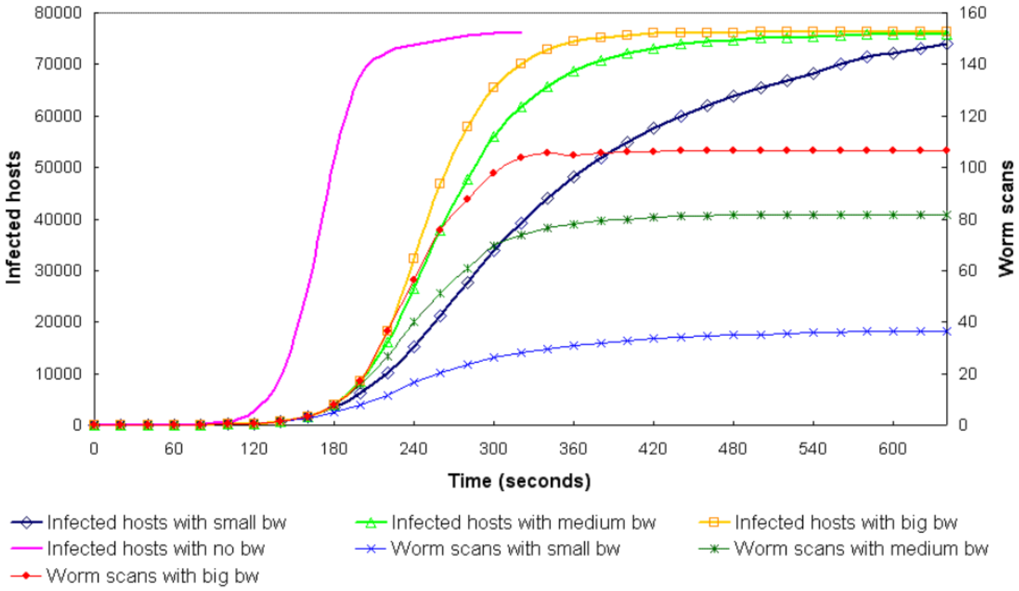

**Figure 4: Simulation with different bandwidth values assignments in Table 1**

## An analysis of what models in ns-3 vs what you have to create

Similar as what we have done in previous projects, we will use existing IPv4/UDP/TCP model to build the network. NS-3 build in topology helpers will work as the building blocks of our complete topology. NS-3's MPI interface may be utilized to accelerate the simulation. But it depends on the exact simulation.

According to the goals we have set, we will create variations of worm based on our previous work in p3, which is a basic framework of worm applications with simple life-cycle control. We will develop some defense strategies to see whether it could effectively stop the propagation of worms. Moreover, router failure may be occurred due to very high traffic caused by the worm, which we are going to implement.