

PEER-TO-PEER NETWORKS FOR DEFENSE AGAINST INTERNET WORMS

Srinivas Shakkottai

University of Illinois at Urbana-Champaign

Joint work with

Prof. R. Srikant

INTERPERF-2006

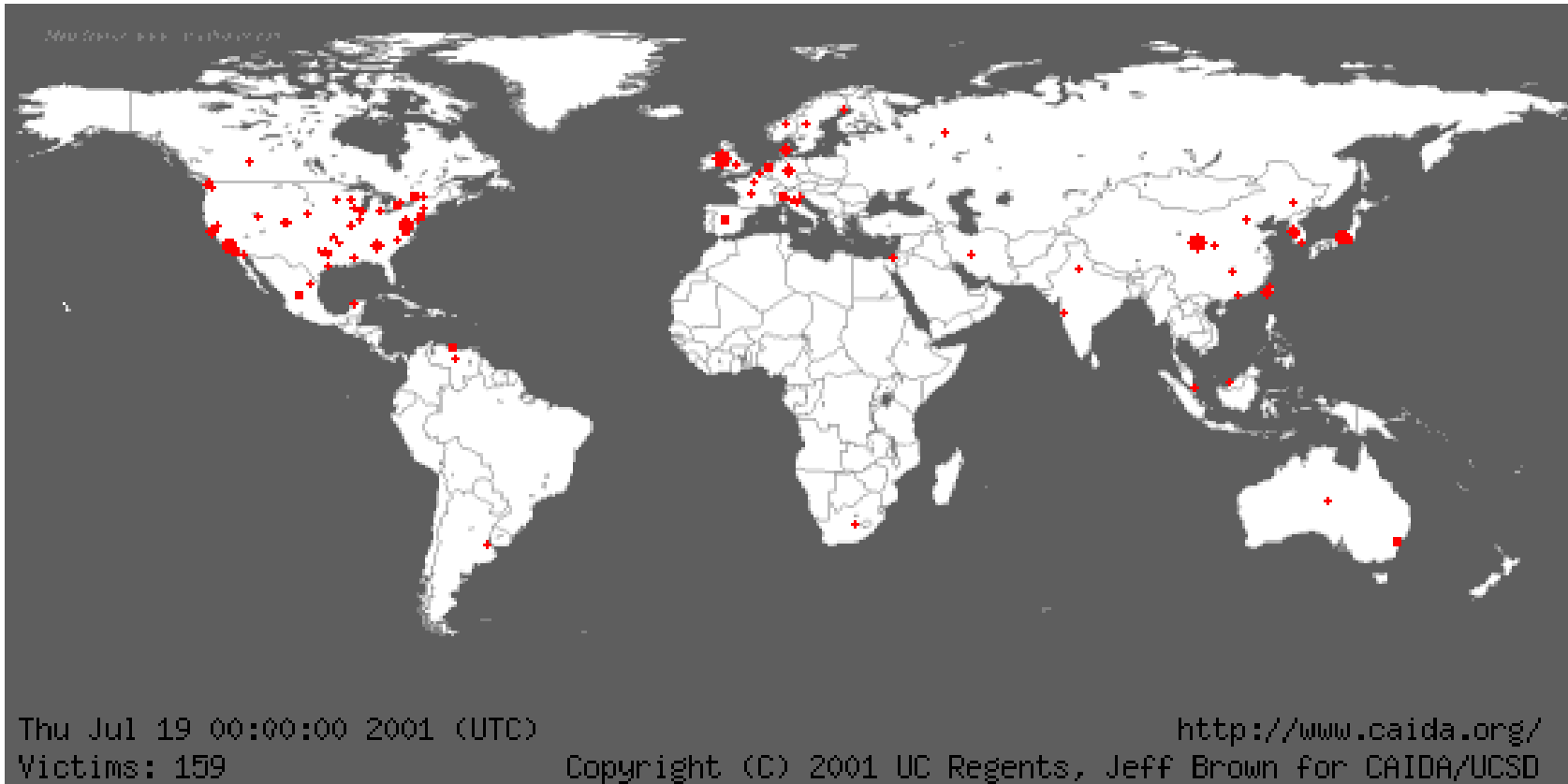


Viruses and Worms

- A *computer virus* attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels.
 - attached to an executable file
 - cannot be spread without a human action.
- A *worm* is similar to a virus by its design, and is considered to be a sub-class of a virus.
 - ability to travel without any help
 - takes advantage of file or information transport features on your system.



Geographic Propagation



Some Related Work

- C. C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," (CCS'02)
- M. Liljenstam and D. Nicol, "Comparing passive and active worm defenses," (QEST '04).
- M. Vojnovic and A. J. Ganesh, "On the effectiveness of automatic patching," WORM '05.
- D. Moore, C. Shannon, G. Voelker, and S. Savage, "Network telescopes," (CAIDA Tech Report).
- M. Williamson, "Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code," ASAC Security Conference '02.



System Model

- Fixed number of hosts N .
- Study the system using fluid differential equations.
- Valid because the number of hosts in the system is usually large.
- Assume that the number of infected hosts in the system when the patch is released is small as compared to N .
 - True of all attacks seen thus far.



Classical Epidemic Model

- N : Total hosts, $I(t)$: Infected, $S(t)=N-I(t)$: Susceptible.
- Infected hosts select a victim at random, avg time taken to infect a susceptible host is 1.

$$\frac{dI(t)}{dt} = I(t) \left(\frac{N - I(t)}{N} \right)$$

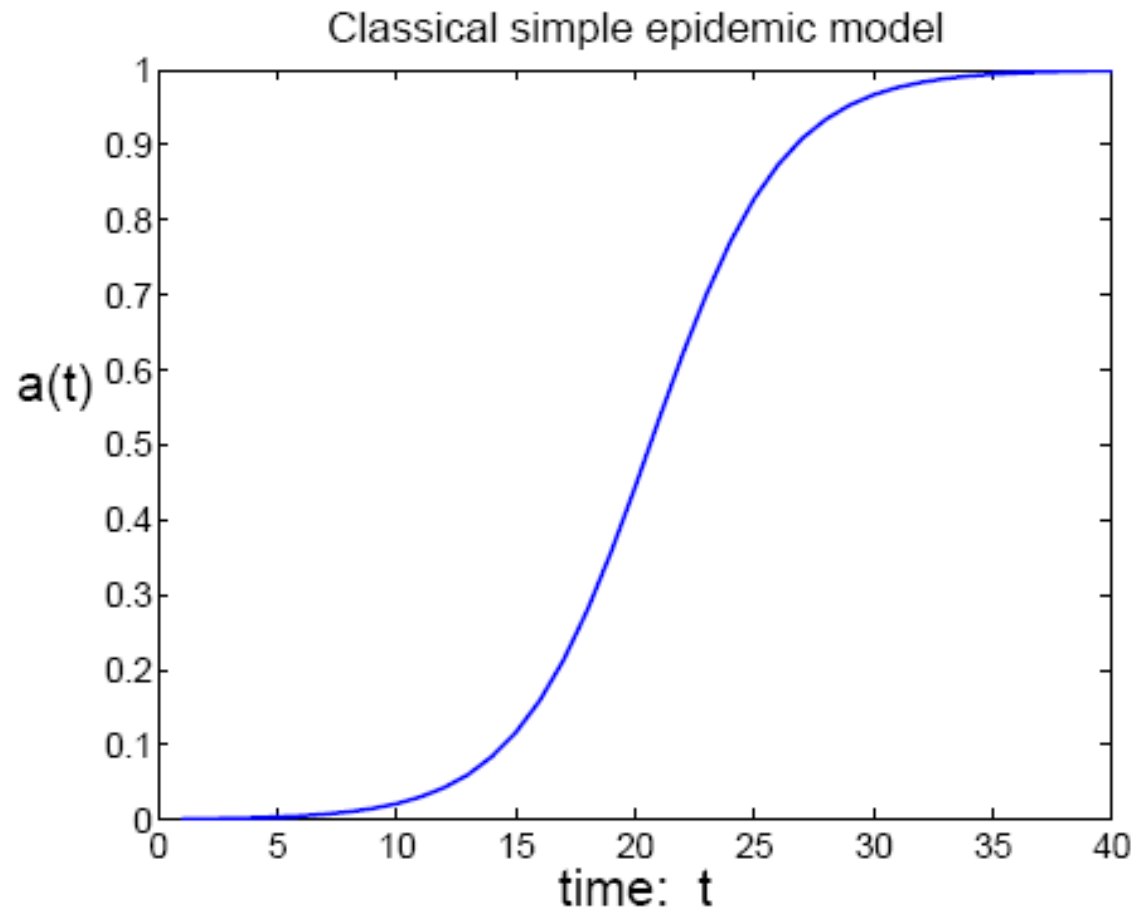
Number of infected
hosts

$$I(t) = \frac{I(0)e^t}{1 - \frac{I(0)}{N} (1 - e^t)}$$

Probability of finding
a susceptible host



Total Infected Hosts



Fixed Number of Patch Servers

- \bar{P} : patch servers, γ patches per sec, $P(t)$: patched

$$\begin{aligned} \frac{d P(t)}{d t} &= \gamma \bar{P} \quad \begin{array}{l} \text{Rate of infection} \\ \swarrow \checkmark \end{array} \quad \begin{array}{l} \text{Rate of patching} \\ \swarrow \checkmark \end{array} \\ \frac{d I(t)}{d t} &= \frac{S(t) I(t)}{N} - \frac{\gamma \bar{P} I(t)}{S(t) + I(t)} \\ N &= S(t) + I(t) + P(t) \end{aligned}$$

- Each patch server has fixed capacity
- Patching rate remains constant



Solving the Equations

- Patching is independent of infection.

$$\frac{d I(t)}{dt} - \left(1 - \frac{P(t)}{N} - \frac{\gamma \bar{P}}{N - P(t)} \right) I(t) = -\frac{I^2(t)}{N}$$

- Second Order Bernoulli Differential equation, whose solution is of form:

$$V(t) = \frac{\frac{1}{N} \int J(t) dt + C}{J(t)}$$

where $V(t) = \frac{1}{I(t)}$.



Closed Form Solution

- Solving the differential equation yields

$$I(t) = \frac{(N - \bar{P} - \gamma \bar{P} t) \left(\exp \left(t - \frac{\bar{P} t}{N} - \frac{\gamma \bar{P} t^2}{2N} \right) \right)}{\exp \left(t - \frac{\bar{P} t}{N} - \frac{\gamma \bar{P} t^2}{2N} \right) + C},$$

where $C = (N - \bar{P})/I(0) \in \Theta(N)$.

- Similar to Logistic equation: $I(t) = \frac{N e^t}{e^t + N/I(0) - 1}$

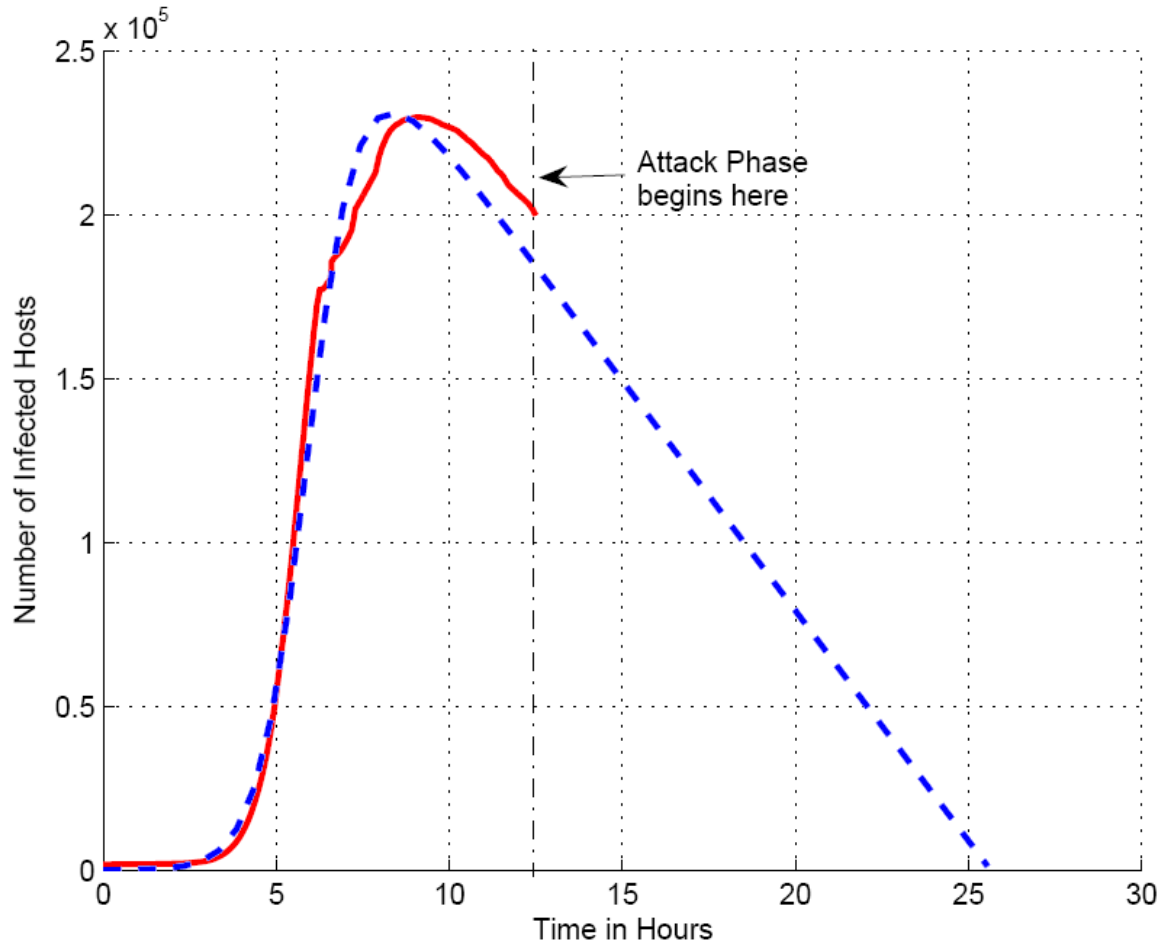


Results for Fixed Number of Patch Servers

- When does the infection hit its peak value?
 - time of order $\Theta(\ln N)$.
 - Same as no patching
- What is the number of infected hosts at this time?
 - of order $\Theta(N)$.
 - Same as no patching
- How long does it take to eliminate the worm?
 - time of order $\Theta(N)$.
 - Takes a long time to eliminate the worm



Experiment



Peer-to-Peer Patching

- Security ensured by checking a hash.

$$\begin{aligned}\frac{d P(t)}{d t} &= \frac{\gamma}{N} (S(t) + I(t)) P(t) \\ \frac{d I(t)}{d t} &= \frac{1}{N} S(t) I(t) - \frac{\gamma}{N} I(t) P(t) \\ N &= S(t) + I(t) + P(t)\end{aligned}$$

Every patched host helps



Solving the Equations

- Patching is independent of infection.

$$\frac{d I(t)}{dt} - \left(1 - \frac{1 + \gamma}{N} P(t) \right) I(t) = -\frac{I^2(t)}{N}.$$

- Second Order Bernoulli Differential equation, whose solution is of form:

$$V(t) = \frac{\frac{1}{N} \int J(t) dt + C}{J(t)}$$

where $V(t) = \frac{1}{I(t)}$.



Closed Form Solution

$$I(t) = \left(\frac{1}{N^2} \frac{\bar{P} e^{\gamma t}}{1 - \frac{\bar{P}}{N}} + \frac{1}{N} + C e^{\gamma t} \left(\frac{\bar{P}}{N} + \left(1 - \frac{\bar{P}}{N} \right) e^{-\gamma t} \right)^{\frac{1}{\gamma} + 1} \right)^{-1}$$

- Effect of exponential patching shows up.

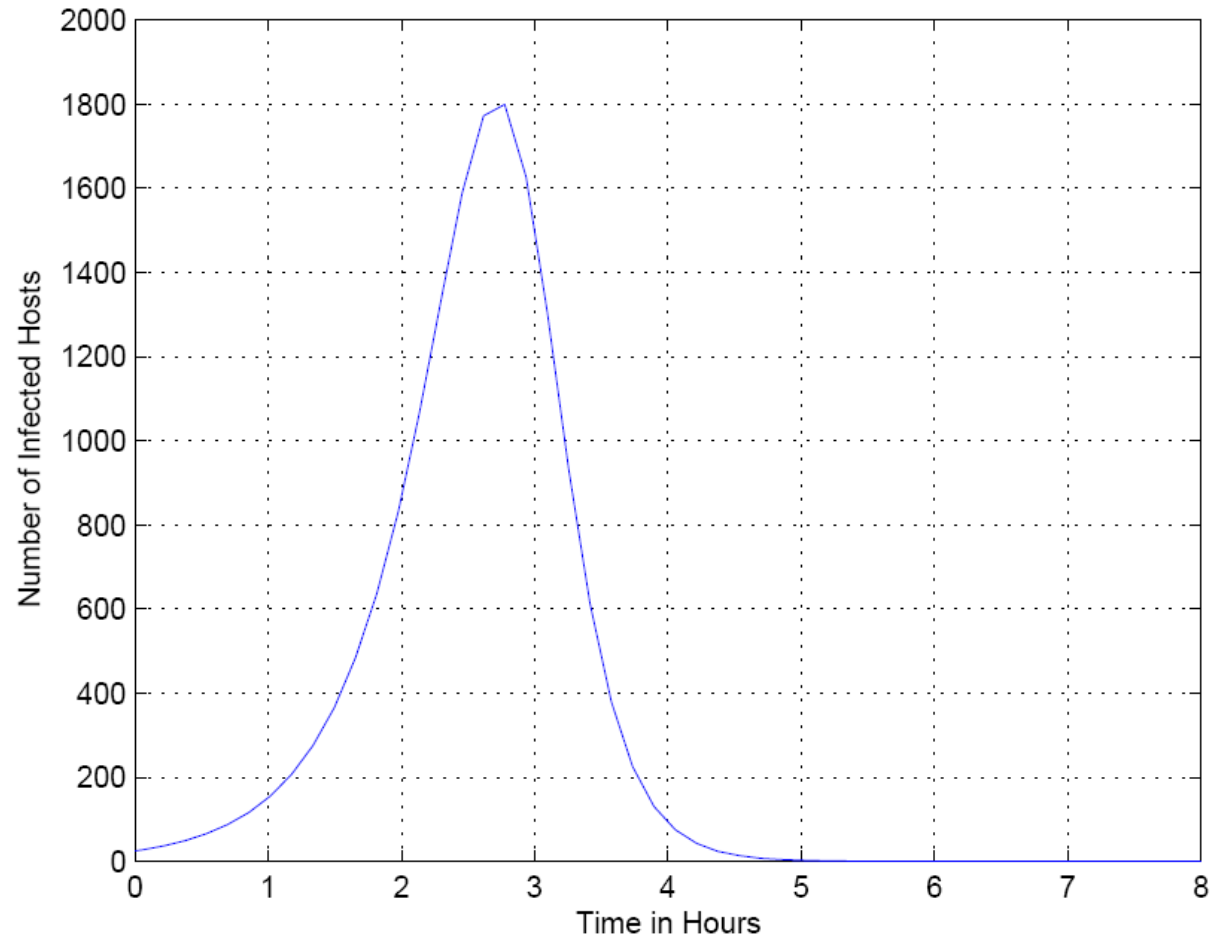


Results

- When does the infection hit its peak value?
 - time of order $\Theta(\ln N)$.
- What is the number of infected hosts at this time?
 - of order $\Theta(N^{\frac{1}{\gamma}})$ if $\gamma > 1$, $\Theta(N)$ else
 - γ increased by throttling.
- How long does it take to eliminate the worm?
 - time of order $\Theta(\ln N)$.



Simulation



Conclusion

- Epidemic model paradigm for the spread of computer worms.
- Fluid model gives a tractable way of handling the analysis.
- Quantitative results on performance of different schemes.
- Peer-to-peer patch dissemination is vastly superior to fixed number of patch servers.



Thank you!

