Virus vs Alert

Who wins in a battle for control of a large network?

Jared Saia

Viruses

- quick
- crafty
- unpredictable

Desired Defense

- fast and automatic
- provable protection
- efficient

(Self-Certifying) Alert

- short proof that security flaw exists
- checkable (no false alerts)
- handles polymorphic viruses

Rules

- When a detector node receives an virus, it becomes alerted
- When an uninfected, unalerted, non-detector node receives an virus, it becomes infected.
- When an unalerted, uninfected node receives an alert, it becomes alerted

Rules

- When a node is alerted, it sends out α alerts each round
- When a node is infected, it sends out β viruses each round

Alert Network

- alerts can only be sent through a bounded degree alert network
- viruses can be sent anywhere, without regard to the alert network
- alert network is fixed before game starts

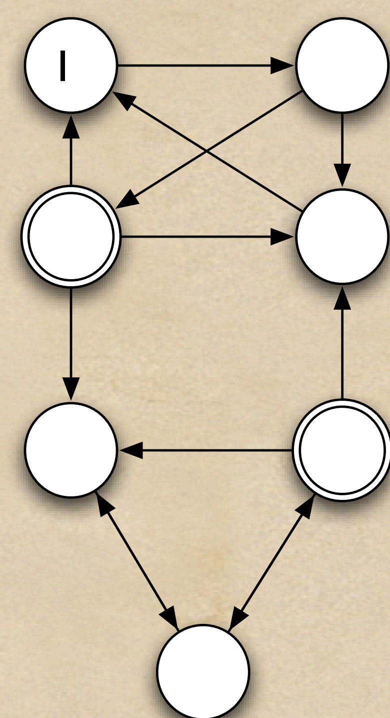
Adversarial Model

- we assume infected nodes are controlled by an adversary
- adversary knows alert network, which nodes are alerted, alert strategy, but does not know location of detectors
- adversary can coordinate infected nodes

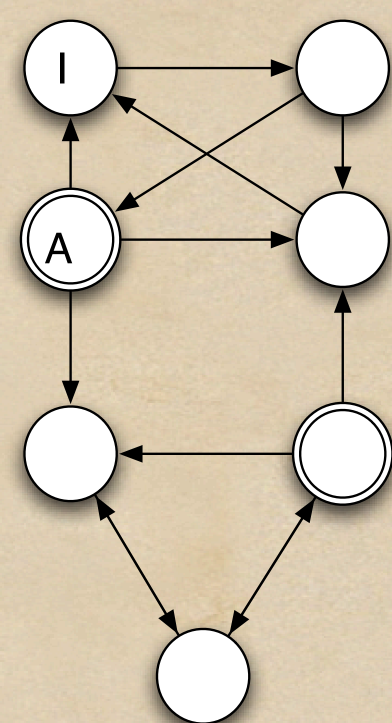
The Start

- one node infected and no nodes alerted
- alert network is fixed and known by the adversary
- (small) constant fraction of detector nodes hidden

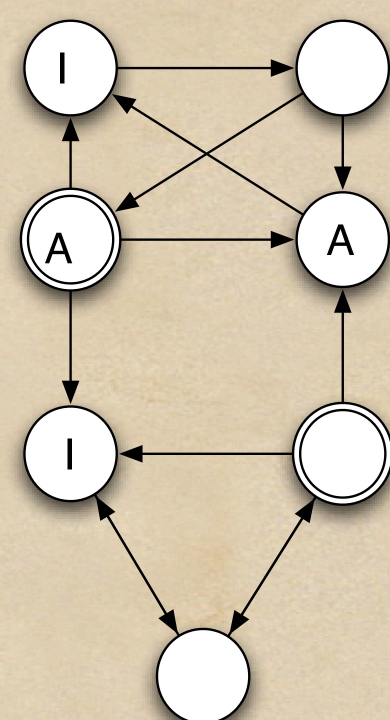
Example



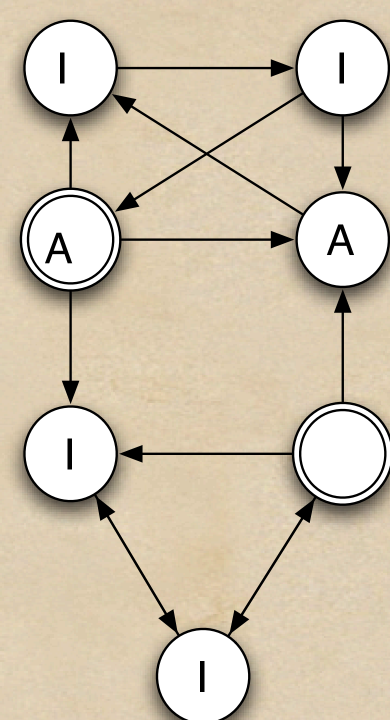
Example



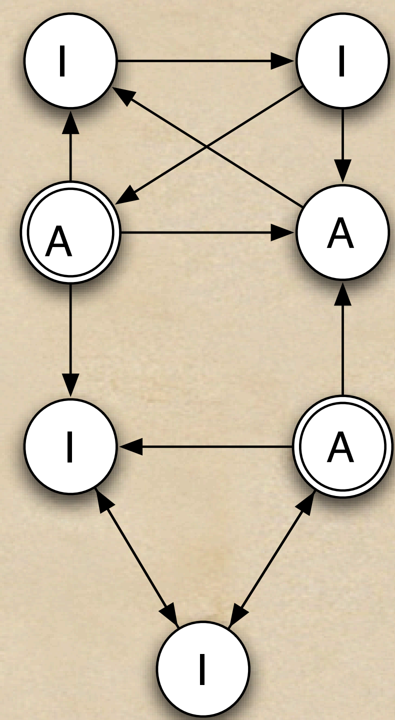
Example



Example



Example



Comparison

- advantage virus
  - head start
  - omniscience, except detector location
  - unconstrained by alert network
- advantage alert
  - hidden detector nodes

Question

- Can we choose an alert network and a strategy for the alerted nodes to ensure that only a vanishingly small fraction of nodes become infected, no matter what strategy the virus uses?

Answer

- Yes! provided that alert network has <u>expansion</u> properties
- strategy for alert is simple: each alerted node sends out α alerts to randomly selected neighbors each round

Expansion

- A graph has expansion factor λ if for every vertex set S which is "not too large":

$$|N(S)| \geq \lambda |S|$$

- Where N(S) is the set of neighbors of S

Theorem 1

- If $\alpha = \beta$ and $\gamma > 1 - \lambda/(2d)$
- Then only o(1) fraction of nodes infected with probability 1 - o(1)
- Where γ is the fraction of detector nodes and d is the degree of the alert network

Theorem 2

- Let $r = \alpha/\beta$ and $\gamma > 0$
- If $\dfrac{r}{1-\gamma} > \dfrac{2d}{\lambda}$
- Then only o(1) fraction of nodes infected with probability 1 - o(1)

Question

- Is good expansion for the alert network <u>necessary</u> in order to save almost all of the nodes?

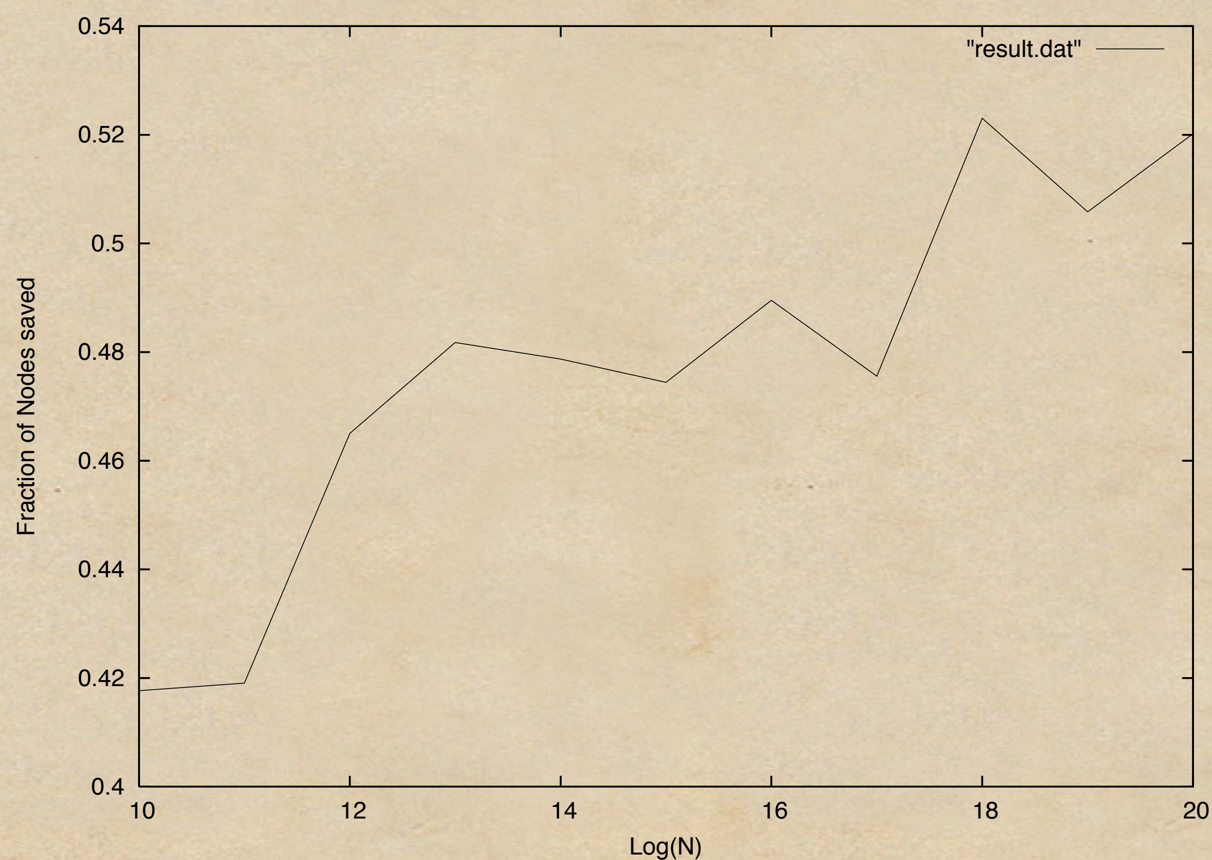
Answer

- Sort of.
- We can show that if the alert network has "bounded growth", there is a strategy for the virus that wins against <u>every</u> alert strategy

Experiments

- Alert network is random regular graph
- Virus strategy is to spread uniformly at random, ignoring which nodes are alerted and the network topology

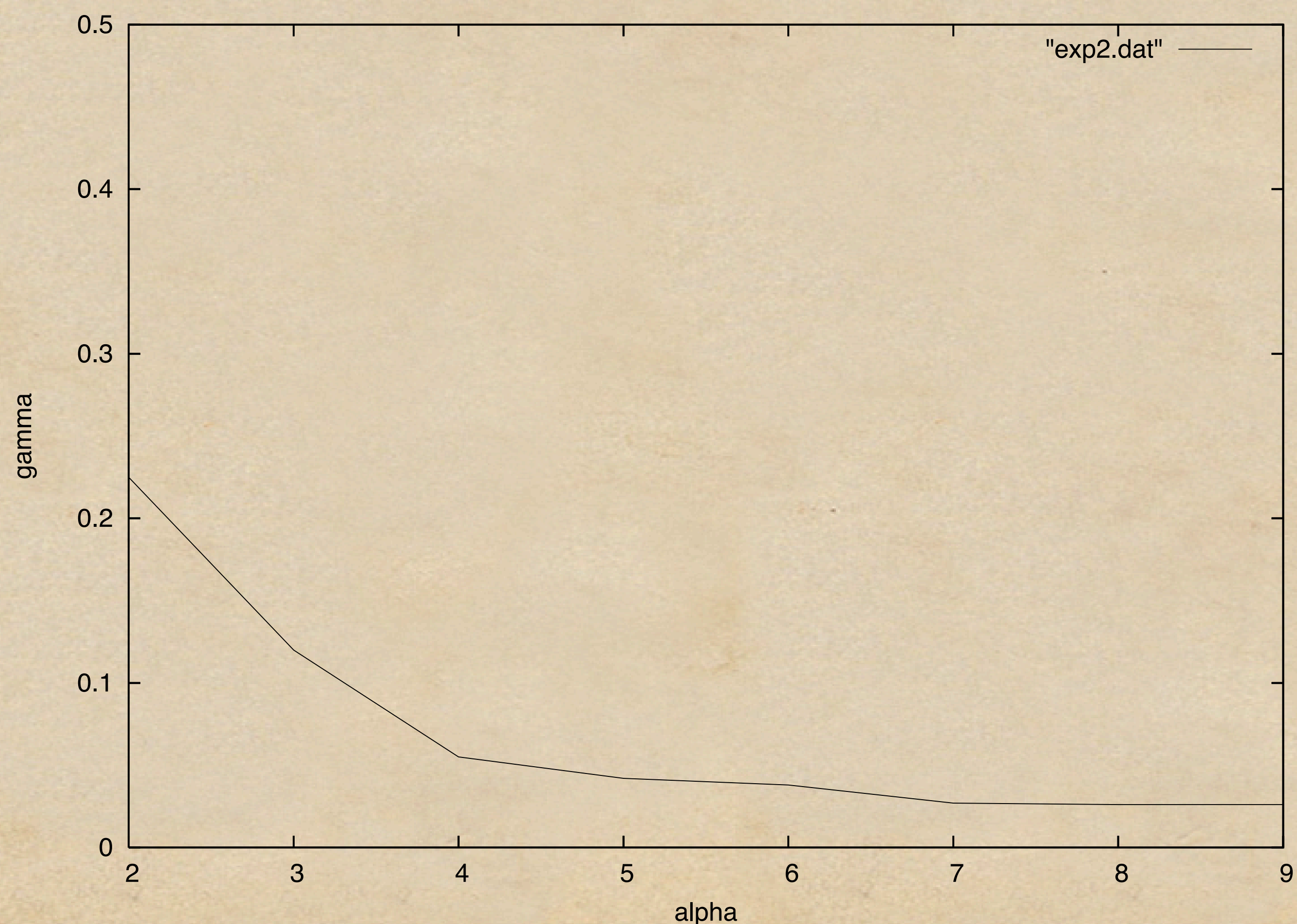
Fraction Saved



$$\alpha = \beta = 1$$

$$\gamma = .1$$

Contour Plot 95% saved



$n = 100,000$

$\beta = 1$

Open Problems

- other models for the spread of a dynamic process and its inhibitor over a population
- need large n for asymptotics to "kick in" - is there a way to reduce required n?
- is there any hope when number of detector nodes is not linear?