Social Network Based Worm Containment in Cellular Networks

Zhichao Zhu, Guohong Cao, and Sencun Zhu

Introduction & Motivation

New trends of Cellular Networks

- Openness would allow richer applications to run over mobile phones
- Witness a similar evolution of worms as have been seen in wired world

Mobile Worms

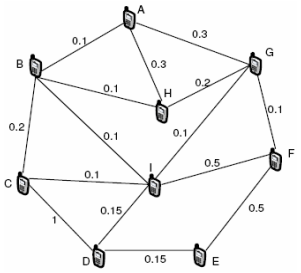
- Mobile worm vs. Internet worm
- Slow start and exponential propagation
- Rely on social engineering (user interaction) for worm activation

Self-Propagated MMS Worms

- Exploring contact list (phonebook)
- Exploring contact history (traffic records)
- Trust within close friends wins higher chance of infection success

Cellular Social Relationship Graph

- Social networking between mobiles
- Predict the worm propagation pattern
- Traffic traces to a topology graph



This topology graph gives an overview of how mobiles are related with each other and how worms might use these social relationships to propagate themselves

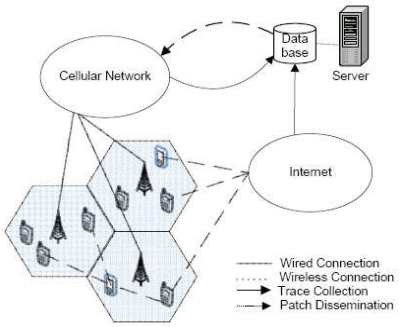
Methods

Social Network based Patching Scheme

- Contest between worm propagation and patch dissemination
- Uniform patching vs. Targeted patching
  - •Time limits
  - •Bandwidth bottlenecks

Targeted Patching

- Only mobile devices which act as a *bridge* between social clusters within the network should be patched first
- **Balanced Patching** vs. **Clustered Patching**



The architecture graph of our systematic worm containment strategy

Controbutions

- Constructed a topology graph of social relations between mobiles by extracting patterns from network traffic traces
- Propose a new containment strategy by partitioning mobiles appropriately based on their social relationship graph
- Experimentally compare our targeted patching algorithms against a benchmark uniformly random patching strategy

Patching by Graph Partitioning

Balanced Patching

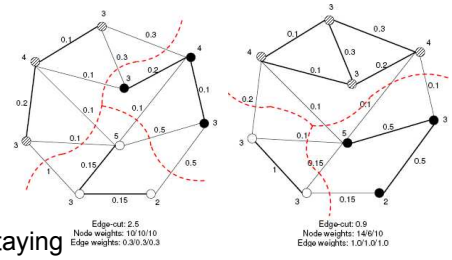
- Keep the damage to each partition balanced
- i.e. multilevel KL algorithm

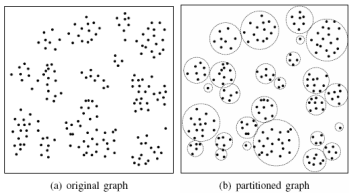
Clustered Patching

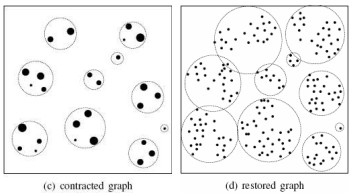
- keep mobiles close to each other staying in the same partition, and divide nodes that are not close into different partitions
- NP-hard Problem

Heuristic Recursive Algorithm

- Expanding Stage
  - Grow each partition P by adding new nodes to it until C(P) does not increase any longer
- Contracting Stage
  - Each partition P_i contracts to a node i, all the interconnection edges between two partitions P_i and P_j become an edge e(i,j), w(i, j) = C(P_i, P_j)
- Restoring Stage
  - replacing each condensed node in each partition with its original nodes



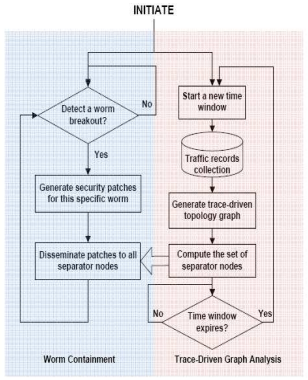


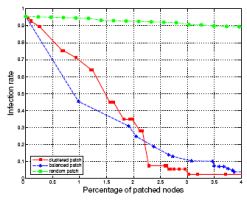


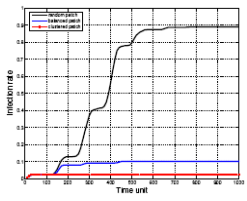
Trace-driven Approach

Using a real network from one of the largest cellular service providers in the US for our worm propagation modeling and simulations

- Preserve the uniqueness of the identifiers of ip addresses and phone numbers involved
- Provide a sessions-level information for traffic exchanged between two endpoints per application over two weeks period in April 2008
- Contain information about 2 million users across 65000 base station cells all over the US with applications of MMS, HTTP, SIP and so on







This work was supported by Narus Inc.