As presented at NIKSUN WWSMC
July 25-27, 2011 | www.niksun.com

NJIT New Jersey's Science & Technology University

Dynamic Trust Management for Mitigation of Malware Dissemination in P2P Networks

Roberto Rojas-Cessa

Assoc. Professor

In collaboration with Lin Cai

Networking Research Laboratory

Department of Electrical and Computer Engineering

New Jersey Institute of Technology

Newark, NJ 07102

Email: rojas@njit.edu

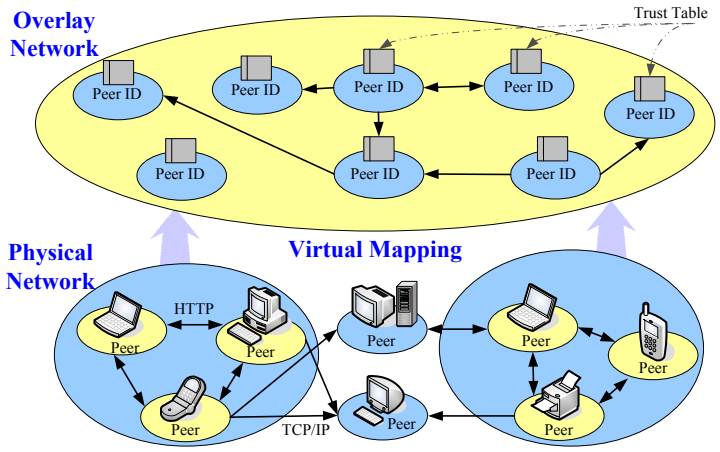
This presentation is based on:

NJIT New Jersey's Science & Technology University

- Lin Cai and Roberto Rojas-Cessa, "Three-Dimensional Based Trust Management Scheme for Virus Control in P2P Networks," Proc. IEEE ICC 2010, 5 pp., Cape Town, South Africa, May 23-27, 2010.

  Lin Cai and Roberto Rojas-Cessa, "Bounding Virus Proliferation in P2P Networks with a Diverse-Parameter Trust Management Scheme," IEEE Commun. LettersVol. 3(10), pp. 812-814, December 2009.

Peer-to-peer network overview



Peer-to-peer network security threats

- New avenues for distributing viruses and Trojans
  - Denial-Of-Service attacks (DoS) Decentralized P2P networks (Gnutella)
  - Virus distribution
  - Unauthorized access to information

- Solution: Local Antivirus software
  - Based on knowledge of existing hazardous files or software.
  - New virus can be uknown until the local database is updated.
  - ***The detection information may be kept from other peers.***

Introduction to dynamic trust management

Problem:

Worms, viruses, and intruding files find an open door to the downloading host in peer-to-peer (P2P) networks: proliferation.

How to decide whether to download a file or not from a peer?

Trust management.

Question (goal):

Can we bound virus proliferation in P2P networks with a trust management scheme?

Related Works

- **Eigentrust [1]**
  - A trusts B, B trusts C => A trusts C
  - Matrix of normalized local trust from global trust values
- **Voting Reputation System [2]**
  - Voting based schemes require to wait for all replies and confirmations.
  - The combined rating of its own reputation and a quorum of its peers.
  - Quorum selection: neighbor-voting, friend-voting
- **Push based Reputation System (DTM scheme) [3]**
  - The combined rating of its own reputation and message from its trustees.
  - Based on localized trust evaluation and in alert dissemination to prevent others from downloading a file from a suspicious peer.
  - Aggregate, process and disseminate transaction-based warning.

Trust Management Objective

- Based primarily on Peer reputation (trust value) and file reputation
- Use Infectious Value, *Iv(i,j)* under infectious environments
- Warning of infected files

Properties:

- No central coordination
- Global behavior emerges from local interactions
- Peers are autonomous
- Peers and connections can be unreliable

Double Layer Dynamic Trust (DDT) Management Scheme [5]

- Trust Value: $Tv(i,j)=\frac{\text{Legitimate-file Downloads}}{\text{Total Downloads}}$

A trust value at peer A about peer B : A's expectation on probability of a legitimate file if downloaded from B.

- Infectious Value: $I_V(i,j)$

possibility of internal infection at A from a downloaded file from peer B.

- Threshold of Trust Value: Th_T

Any peer in the system that is trusted by any other peer is called trustee and any peer that trusts a trustee is called truster.

- Threshold of file reputation: Th_F

Determines whether a file is innocuous or dangerous.

- Local Virus Detection Probability: $P_d(i)$
- Infection probability: $P_I(f)$
- Trustee set of peer i: $\Theta(i)$

DDT: Trust Value Update after an Event

- Local trust value calculation

  $Tv(i,j) = \frac{Clean\ Downloads}{Total\ Downloads}$

- Local trust value update

  - Clean (virus free) downloads

    $Tv(i,j)=a*Tv(i,j),\ a>1.$

  - Malicious downloads

    $Tv(i,j)=b*Tv(i,j),\ 0<b<1.$

    $Iv(i,j)=Iv(i,j)+1;$

    $F(i,fl)=F(i,fl)+1;$

    If $Tv(i,j) > Thw$ → issue warning to trusters, with format $\{ID, vj, f_m, Q, d\}$.

    ID: warning message identification number.

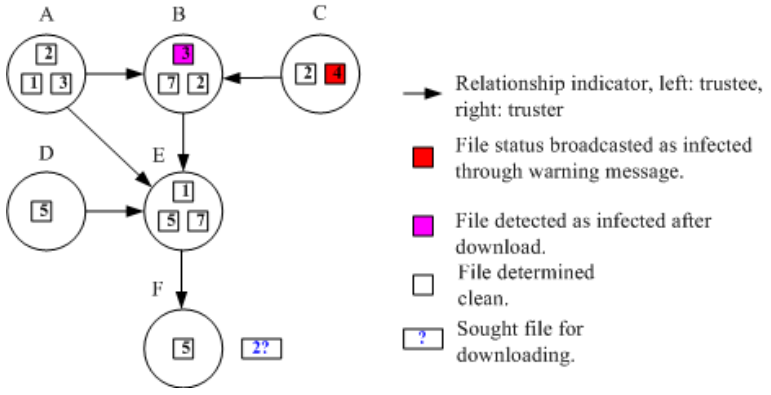
    vj: identification of the peer.

    f_m: file's name.

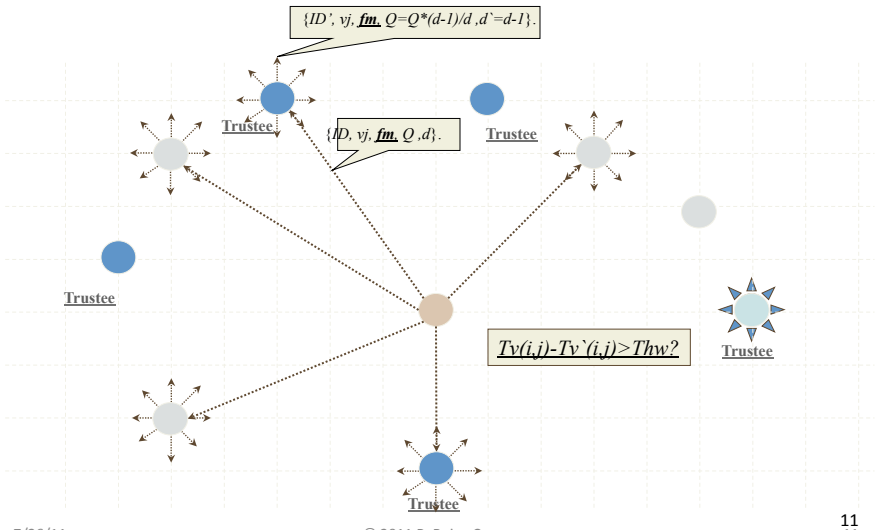
    Q: degradation of the trust value.

    d: number of truster hops the warning message is allowed to propagate.

DDT: Simple Example of Events

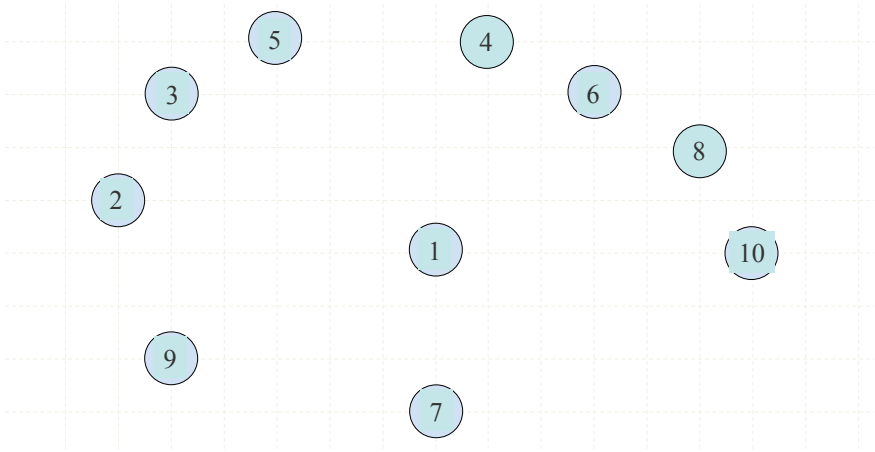


DDT: Trust Management Scheme



Simulation Model

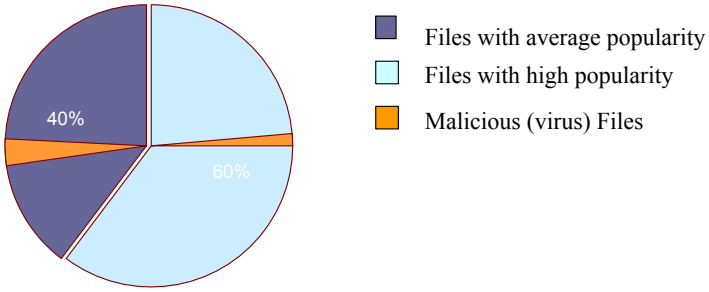
Simulated P2P mesh network with 100 nodes. Each peer is marked with an unique ID.



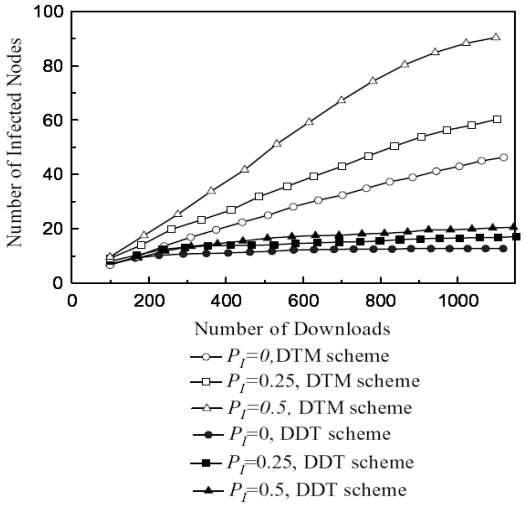
Simulation Model: File Distribution

Total number of files = 150, with an average of three copies each, uniformly distributed randomly among the 100 peers. Among them 60% are popular files, and 10 files are infected.

We evaluate the total number of infected peers after each time slot.



DDT: Performance Evaluation



Unfairness in Ratio-based Trust values

Ratio Based trust value calculation

–The calculation and aggregation of the local trust values : challenging.

–Normalization of trust value seems to be norm.

Dynamic trust, Trust value=good downloads/total downloads.

Eigen trust,

$$c_{ij} = \frac{s_{ij}}{\sum_j s_{ij}}, \qquad s_{ij} = sat(i,j) - unsat(i,j)$$

$$c_{ij} = \frac{1}{1} = 1, c_{ik} = \frac{10000}{10000} = 1$$

sat(i,j): no. of satisfactory transactions

unsat(i,j): no. of unsatisfactory transactions

Problem: 1) A peer can achieve trust value 1 by doing 1 successful download.

Another peer can achieve trust value 1 after 10000 downloads.

It is unfair and may lead to sybil attacks

Although *Cij=Cik*, peer *k* has more trustable performance than peer *j*.

2) Only peer reputations are considered. Infectious environments can flex the trend of trust values

3D: Trust Management Scheme Objective [6]

- Based primarily on Peer reputation (trust value) and file reputation
- Three-dimension trust value calculation (to distinguish number of historical transactions)
- Use Infectious Value, *Iv(i,j)* under infectious environments
- Warning of infected files

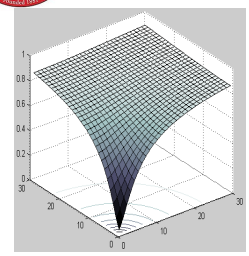
Properties:

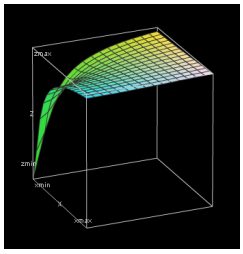
- No central coordination
- Global behavior emerges from local interactions
- Peers are autonomous
- Peers and connections can be unreliable
- History of transactions is considered with high importance

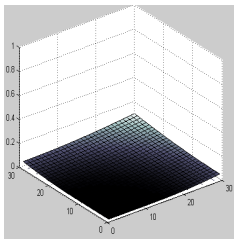
3D Trust Value Estimation Scheme

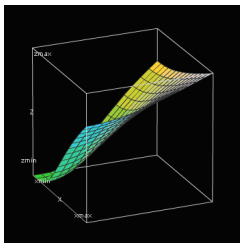
- Combination of trust values of peers and infection values of both peers and content.
- File reputation value to evaluate distributed content.
- Warnings issued to other peers about infected files.
- Uses a three-dimensional (3D) historical normalization

3D: Trust Value Calculation









The surface of the two functions $z = e^{-\frac{50}{\sqrt{x^2+y^2}}}$ $z = e^{-\frac{5}{\sqrt{x^2+y^2}}}$

3D trust value calculation

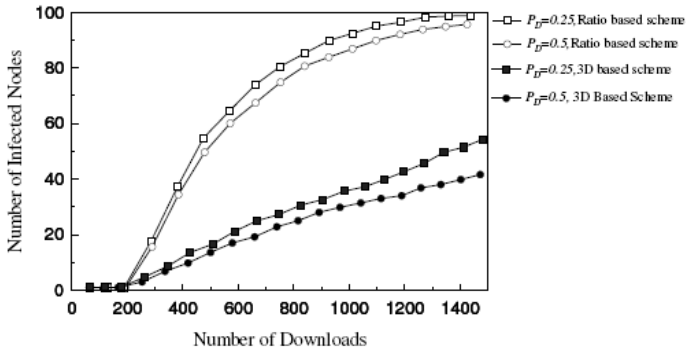
$$c_{ij} = \alpha^{-\frac{\beta}{\sqrt{sat(i,j)^2+tol(i,j)^2}}}$$

where α, β are two parameters controlling the approaching speed to 1.

Scenario

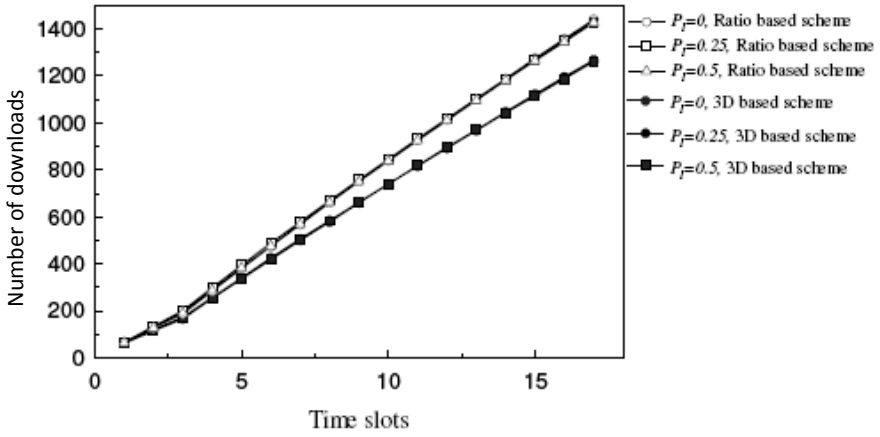
1. Ratio based (RA) and 3D models are compared.
2. At the beginning, the peers do not know each other.
3. A peer downloads a file from an unknown peer if and only if he can not find the downloading source anywhere else.
4. The attacker joins the system from the third time slot.
5. The attacker contains: clean and infected files.
6. The trust relationship: built through interactions.
7. The performance: number of nodes infected.

Performance by Number of Downloads



Comparison of Ratio Based Scheme and 3D based scheme, under *PD* = 0.25, 0.5

Performance: Download Activity



Download activity of the network using the 3D based scheme.

Conclusions

- Local trust value is effective for systems where files don't get infected.
- Warning distribution system: globalization of data on network and risks.
- Combined File based reputation with peer reputation (trust and infectious) showed their efficiency in bounding virus proliferation in an infectious environment.
- Using a 3D model, the trust value is more effective than ratio-based for evaluation of trust values. Nodes with more established reputation can be identified.
- The use peer and file reputation have little impact on downloading activity.

References

References:

[1] Kamvar S.D., Schlosser M.T., and Garcia-Molina H. The Eigentrust algorithm for reputation management in p2p networks. *Proc. 12th International World Wide Web Conference*, pp. 785-791, 2003.

[2] S. Marti and H. Garcia-Molina, "Limited Reputation Sharing in P2P Systems," Proc. of the 5th *ACM Conference on Electronic commerce (EC)*, pp. 91-101, New York, NY, May 2004.

[3] X. Dong, W. Yu, and Y. Pan, "A Dynamic Trust Management Scheme to Mitigate Malware Proliferation in P2P network," Proc. *IEEE International Conference on Communications 2008*, 5 pages, Beijing, China, May 2008.

[4] E.K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim., "A Survey and Comparison of Peer-to-Peer Overlay Network Schemes," IEEE Comm. Survey and Tutorial, Vol. 7, Issue 2, 2nd Quarter 2005, pp. 72-93, 2005.

[5] Lin Cai and Roberto Rojas-Cessa, "Bounding Virus Proliferation in P2P Networks with a Diverse-Parameter Trust Management Scheme," IEEE Commun. Letters, Vol. 3(10), pp. 812-814, December 2009.

[6] L. Cai and R. Rojas-Cessa, "Three-Dimensional Based Trust Management Scheme for Virus Control in P2P Networks," IEEE International Conference on Communications, pp. 5, May 2010.