

# Peer-to-Peer: Trust and Security

Tien Tuan Anh Dinh  
School of Computer Science  
The University of Birmingham  
UK

November 2009

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

# Introduction

## Definition

1. *Autonomous*
2. *Allow heterogeneity*
3. *Most traffic is among peers*

## Why P2P?

P2P **vs.** Client-Server:

- Scalability
- No single point of failure

# Introduction

## Types of P2P

### Unstructured:

- Broadcast, undeterministic search
- Example: Limewire, KaZaa, Bittorrent, etc ...

### Structured:

- Deterministic, efficient search
- Example: Chord, DHT-based Bittorrent, StormNet, etc ...



# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

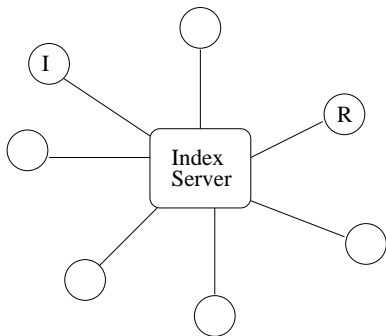
Trust in P2P

Summary

## Conclusion

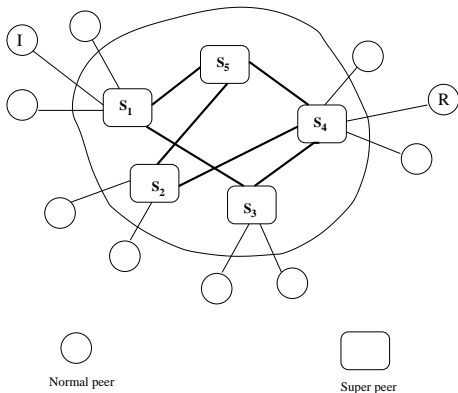
## 1st Generation - Napster

- Search done by the index server
- Easy to take down



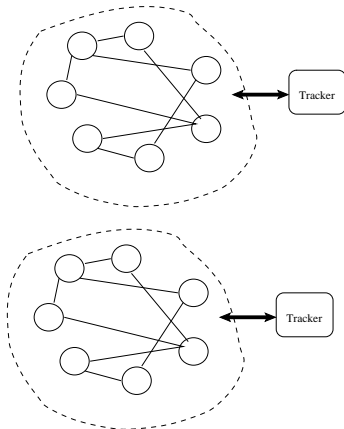
## 2nd Generation - Gnutella

- Example: Limewire, KaZaa, eDonkey
- Search by flooding, *undeterministic*
- More scalable, no single point of failure



## 3rd Generation - Bittorrent

- Peers organized into *independent swarms*
- Tracker server acts as index server for the swarm
- Search (for tracker server) assumed to be off-line
- *Tit-for-tat* improves cooperation (download speed, for instance)



# Summary

## Characteristics of Unstructured P2P

- Nodes could connect to any peer
  - Network topology: random
  - Frequent joining and leaving would not affect the network
- Search (if applicable) is done via flooding:
  - Undeterministic
  - Not scalable.



# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

# Overview

## Motivation

To address the search problem in unstructured P2P:

- Deterministic
- Scalable

## The trade-off

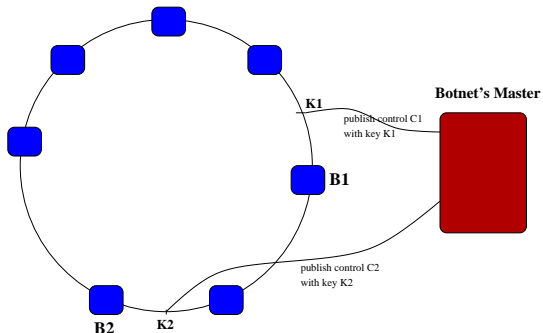
- Exact-match search
- Rigid network topology is maintained, hence the name *structured*
- Frequent joining and leaving incur great overhead





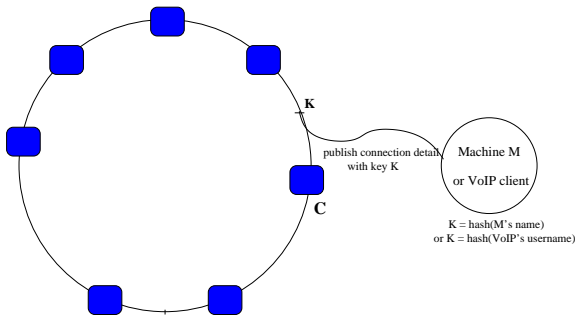


## Real Implementations - Botnet (StormNet)



- At time interval  $t$ , bot master upload control  $C_t$  with a key  $K_t$
- Bots know how to generate  $K_t$ , contact another bot  $P$  using  $\text{lookup}(K_t)$
- Download and run  $C_t$

## Real Implementation - VoIP and Windows 7



- Machines (with Windows 7) or VoIP clients given unique names
- Users publish their connection details to the structured P2P network (cloud), using the given names
- Names are used as DNS addresses



## Summary

1. Structured P2P supports deterministic, efficient exact-match search
2. Scalable, with several practical implementations
3. Not robust under high churn

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

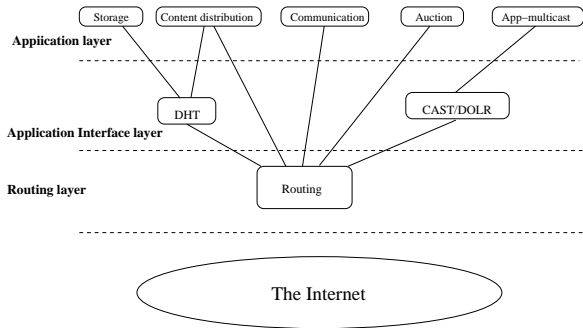
Trust in Society

Trust in P2P

Summary

## Conclusion

## P2P Abstraction



- Routing: deliver messages to destination
- Application interface: `publish(k,data)`
- Application: specific requirements, depending on the application

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

**Attacks**

Other Challenges

Summary

## Trust As a Solution

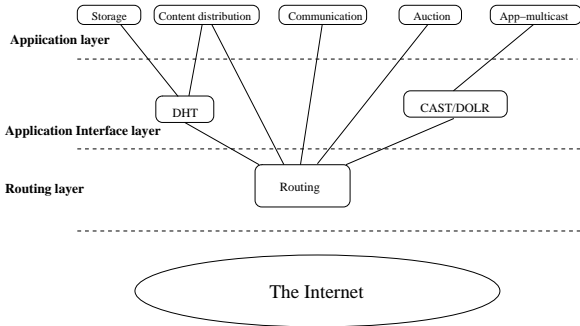
Trust in Society

Trust in P2P

Summary

## Conclusion

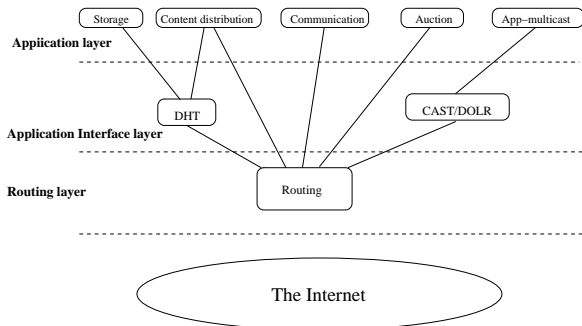
## Attacks at Different Layers



### At the Internet Layer

- Common attacks on Confidentiality, Integrity and Availability

## Attacks at Different Layers

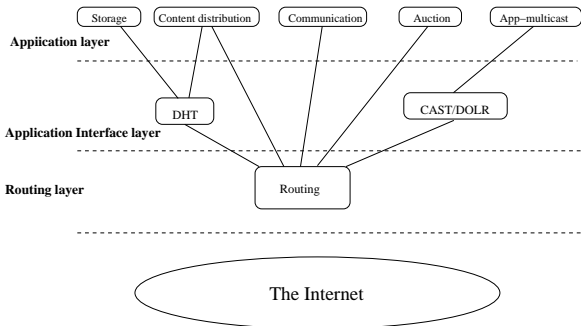


### At the Routing Layer

- No routing, redirection
- Impersonate as destination, tamper with search queries



## Attacks at Different Layers



### At the Application Layer

Application specific:

- Censorship, data corruption
- DoS
- etc ...

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

**Other Challenges**

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

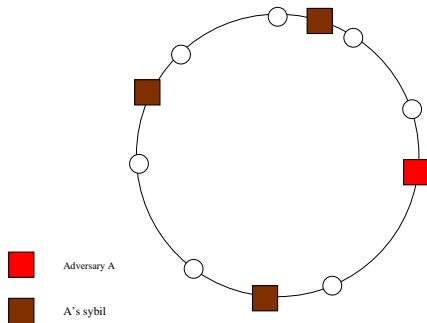
Summary

## Conclusion

# Sybil Attacks

## The Attack

- Adversary obtains multiple identities, i.e. control multiple peers
- Amplify impact of other attacks
- *Why?*: no identity management, arbitrary number of Sybils could be introduced



# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

**Summary**

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

## Summary

- P2P systems inherit security issues from the Internet layer
- P2P systems have specific security threats at all level of abstractions
- Challenging, because:
  - Nodes do not have global views of the network
  - No identity management, therefore subject to Sybil attacks

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

# Trust

## Overview

- Trust is one of the things that make our society works
- Studied extensively in social sciences: sociology, psychology, economics, politics, etc...

## Definition

*A trusts B regarding a task T means A believes that:*

1. B has the *right intention* towards A
2. B is *competent* to perform T

Note: *trust* is subjective

# Trust, Distrust, Trustworthiness and Reputation

## Trust and Distrust

- Not two ends of the same spectrum
- (*low trust, low distrust*) - casual relationship; (*low trust, high distrust*) ; (*high trust, low distrust*) ; (*high trust, high distrust*) - trust but verify
- Different emotions:
  - *trust* - docile zoo elephant munching on hay
  - *distrust* - raging wild bull elephant protecting the herd (McKnight et al.)

# Trust, Distrust, Trustworthiness and Reputation

## Trust, Trustworthiness, Reputation

- *Trust* - verb
- *Trustworthiness* - noun, constitutes trust
- In general:

*Trustworthiness* → *Trust*

- *Reputation*, cultural, physical, institutional factors constitute *trustworthiness*. With high probability:

Reputation → *Trustworthiness*

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

**Trust in P2P**

Summary

## Conclusion

# Soft Security

## Had we had trust in P2P systems

- Peer only interacts with ones it trusts
- Badly behaved ones or adversaries are detected and eliminated from the network
- Encourage cooperation among peers

# How to Compute Trustworthiness

## Reputation

- *Why?*: other factors constituting trustworthiness are not available in P2P settings
- *How*:
  - *Feedback* for peer  $i$ ,  $F_i$  is gathered
  - *Reputation Metric*: function applied over feedback, returns reputation scores:

$$R_i = m_i(\bigcup_j F_j)$$

- Simple metric: summing up all feedback for  $i$ :

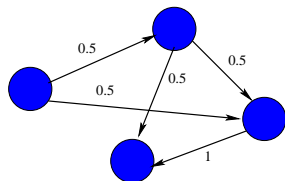
$$R_i = \sum_{f \in F_i} f$$

but vulnerable to manipulation

# How to Compute Trustworthiness

## PageRank as a Reputation Metric

- Trust graph  $G$ :  $P_i$  has link to  $P_j$  if  $P_i$  trusts  $P_j$
- PageRank values computed on  $G$  returns *importance* scores for all nodes
- A peer with high PageRank score has high reputation, as being trusted by other nodes with high reputation
- Effective, robust against manipulation



# Reputation Using Trusted Services

## Problems with Feedback

- How to incentivize peers to give feedback ?
- How can a peer distinguish good and bad behavior in order to give feedback?
  - For example: in structured P2P, how to tell if a peer  $P$  really is the destination for search key  $k$  ?

# Reputation Using Trusted Services

## Trusted Services

- Addresses the second question
- *Trusted service*: whose failure can break security properties **vs.** *trustworthy service*: will not break
- *Centralized service*: stores configuration of the network and answers queries about neighbor information
- *TPMs and other hardware-based security modules*:
  - Using features: *monotonic counters, signing, transport session, attestation*
  - Generate neighbor certificates everytime nodes join or leave
  - If  $P$  claims to be destination for key  $k$ , check  $P$ 's certificates.

# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

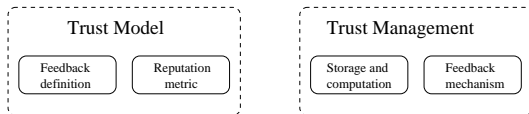
# Summary

## Trust As a Solution

- Peers can interact with ones they trust, therefore eliminate bad/adversarial ones
- Notion of trust has been studied extensively in social sciences, and recently in computer science (reputation)
- Trust can be established using reputation: computed using reputation metrics over feedback

## Implementing Trust Systems

### Trust System



# Outline

## P2P Systems

Unstructured P2P

Structured P2P

## Security in P2P

P2P Abstraction

Attacks

Other Challenges

Summary

## Trust As a Solution

Trust in Society

Trust in P2P

Summary

## Conclusion

## Conclusion

- P2P is not only about file-sharing
- Structured P2P is more scalable and could be used for very large scale applications
- P2P systems, especially based on structured P2P overlays are subject to wide range of security attacks
- Made worse by Sybil attacks
- Notion of trust offers a solution to eliminate such attacks
- Computable reputation can be used as a good indicator of trust
- Still many questions to be addressed before implementing a full trust-based infrastructure for P2P