A Sybilproof Indirect Reciprocity Mechanism for Peer-to-Peer Networks

Raúl Landa, Richard Clegg, Eleni Mykoniati, David Griffin, Miguel Rio

Networks and Services Research Laboratory
Department of Electronic and Electrical Engineering
University College London
The Incentives Problem

• It is individually rational for each peer to contribute as little as possible, while at the same time consuming the contributions of other peers.

• One possible solution is direct reciprocity (*Tit-for-Tat*)
  – It has some problems, though:
    • High churn rates
    • Mismatch of reciprocation and content interest

• Indirect Reciprocity
  – Usually *reputation systems*
Attacks on Reputation Systems

• Sybil Attack
  – Peers create arbitrary contributions between fictitious peers

• Slander Attack
  – Peers lie regarding the contributions of other peers

• Whitewashing Attack
  – Discarding identities that have been labeled as malicious
Attacks on Reputation Systems

- **Sybil Attack**
  - Peers create arbitrary contributions between fictitious peers

- **Slander Attack**
  - Peers lie regarding the contributions of other peers

- **Whitewashing Attack**
  - Discarding identities that have been labeled as malicious
PledgeRoute

• Reduces indirect reciprocity to direct reciprocity and *contribution transfer*

• Contributions can be moved between peers
  – Completely decentralized
  – Resistant to Sybil, slander and whitewashing attacks

• Based in the Dijkstra algorithm over the \((\mathbb{R}, \text{max}, \text{min})\) semi-ring
Definitions

• Contribution network $\mathcal{G}$
  – $w_{ij}$ represent the un-reciprocated contributions from peer $i$ to peer $j$

• Social Capital
• Pledged Resources
• Peer Wealth
• Interest Network
Definitions

- Contribution network $G$

- Social Capital
  – Peer weighted out-degree in $G$

- Pledged Resources
  – Peer weighted in-degree in $G$

- Peer Wealth
  – Difference between both

- Interest Network
Definitions

- Contribution network $\mathcal{G}$
- Social Capital
- Pledged Resources
- Peer Wealth

- Interest Network
  - Links represent availability of useful services
PledgeRoute

• Peers map the contribution topology $G$

• We assume that peers know their neighbors in $H$

• The idea is to route contributions over $G$ to allow services in $H$
Direct Reciprocity

\[ G \]

\[ H \]

Raúl Landa

A Sybilproof Indirect Reciprocity Mechanism for Peer-to-Peer Networks

INFOCOM 2009
Direct Reciprocity
Direct Reciprocity

\[ G \cap H \]
A Sybilproof Indirect Reciprocity Mechanism for Peer-to-Peer Networks
A Sybilproof Indirect Reciprocity Mechanism for Peer-to-Peer Networks
PledgeRoute: Direct Reciprocity
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer
PledgeRoute: Contribution Transfer

Direct Reciprocity

Indirect Reciprocity
Protocol Specifics: Interaction Policies

• Peers use self-certifying identifiers
  – All protocol messages are digitally signed

• Peer requests can be:
  – **Altruistic**
    • Best effort service
    • Increases Social Capital
    • Bootstrapping
  – **Reciprocating**
    • Preferential Service
    • Decreases Social Capital
    • Operate as an Incentives Mechanism
The contribution network is discovered using self-avoiding random walks with a biased distribution.

This favors paths with consistently high social capital.
Contribution Topology Discovery

- The contribution network is discovered using self-avoiding random walks with a biased distribution.
- This favors paths with consistently high social capital.

![Diagram of contribution network]
Contribution Topology Discovery

The Author
March 30, 2009

⇒ (1)

1
Contribution Topology Discovery

- **Pledge Announcement Messages**

- PAM represent self-avoiding paths annotated with contributions

- Peers update their contribution network model with these paths
Contribution Topology Discovery

- **Pledge Announcement Messages**

- PAM represent self-avoiding paths annotated with contributions

- Peers update their contribution network model with these paths
Contribution Topology Discovery

- **Pledge Announcement Messages**
- PAM represent self-avoiding paths annotated with contributions
- Peers update their contribution network model with these paths
Contribution Topology Discovery

- **Pledge Announcement Messages**

- PAM represent self-avoiding paths annotated with contributions

- Peers update their contribution network model with these paths
Contribution Topology Discovery

- **Pledge Announcement Messages**

- PAM represent self-avoiding paths annotated with contributions

- Peers update their contribution network model with these paths
Contribution Topology Discovery

• **Pledge Announcement Messages**

• PAM represent self-avoiding paths annotated with contributions

• Peers update their contribution network model with these paths

![Diagram showing Pledge Announcement Messages (PAM), updates, and contributions between peers 1, 2, and 3.](image)
Contribution Topology Discovery

• **Pledge Announcement Messages**

• PAM represent self-avoiding paths annotated with contributions

• Peers update their contribution network model with these paths
Contribution Topology Discovery

- **Pledge Announcement Messages**

- PAM represent self-avoiding paths annotated with contributions

- Peers update their contribution network model with these paths
Contribution Topology Discovery

- **Pledge Announcement Messages**

- PAM represent self-avoiding paths annotated with contributions

- Peers update their contribution network model with these paths
Evaluation: Topology Discovery

- PAMs are terminated at each hop with a probability $\rho$
Contribution Transfer

• Soft-state reservation protocol
• Peers find a route in $G_i$ to the peer they want to request services from
• Source-routed Contribution Transfer Request Messages
Contribution Transfer

- Soft-state reservation protocol
- Peers find a route in $G_i$ to the peer they want to request services from
- Source-routed Contribution Transfer Request Messages
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used

\[ S_1 \rightarrow r_1 \]

CTRM

1 \rightarrow 2 \rightarrow 3 \rightarrow 4

\[ w_{12} \rightarrow w_{23} \rightarrow w_{34} \]
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used

As CTRM propagate, they set contribution reservations. As with PAMs, nested digital signatures are used.
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used
Contribution Transfer

- As CTRM propagate, they set contribution reservations
- As with PAMs, nested digital signatures are used

![Diagram showing the flow of contribution transfer with nodes 1 to 4, with contributions set at nodes 2 and 3, and CTRMs at node 4.](image-url)
Contribution Transfer

- The CTRM recipient creates a Resource Ticket for the originator
- The Resource ticket propagates back, triggering the actual contribution account subtractions

$$r_1 \leq \min(w_{12}, w_{23}, w_{34})$$
Contribution Transfer

- The Resource Ticket propagates back, triggering the actual contribution account subtractions

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

- The Resource Ticket propagates back, triggering the actual contribution account subtractions

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

- The Resource Ticket propagates back, triggering the actual contribution account subtractions

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

- The CTRM originator can then use the Resource Ticket to gain contributions in the destination

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

• The CTRM originator can then use the Resource Ticket to gain contributions in the destination

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

• The CTRM originator can then use the Resource Ticket to gain contributions in the destination

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

- The CTRM originator can then use the Resource Ticket to gain contributions in the destination

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

• This process is equivalent to *single-path maximum flow*

\[ r_1 \leq \min (w_{12}, w_{23}, w_{34}) \]
Contribution Transfer

• Problem:
  – In a contribution transfer of magnitude $r_1$ over $m$ hops, a total of $(m - 1)r_1$ contribution units are lost
  – This harms connectivity in $G$ and makes later contribution transfers harder

$r_1 \leq \min (w_{12}, w_{23}, w_{34})$
Resistance to Sybil Attacks

- The contribution transfer capacity between a sybil strategy and $G$ is bounded by the contributions on the attack links.
- These are real contributions, vouched by the nodes that received them.
Resistance to Sybil Attacks

• We formalize this by defining $\mathcal{W}(s, i)$, the contribution transfer capacity between peers $s$ and $i$.

• We describe contribution transfer using a very simple path semi-ring: $(\mathbb{K}, \oplus, \otimes) = (\mathbb{R}, \max, \min)$.

• Dijkstra’s algorithm normally operates in the usual $(\mathbb{R}, \min, +)$ semi-ring, thus giving shortest paths.

• If we use $(\mathbb{R}, \max, \min)$ instead, we get the maximum bottleneck transfer capacity tree over $\mathcal{G}$. We define this to be our $\mathcal{W}(s, i)$. 
Resistance to Sybil Attacks

• Formally, we obtain:

\[ W(s, i) = \bigoplus_{P_{si} \in \mathcal{P}_{si}} \left( \bigotimes_{l_{jk} = (n_j, n_k) \in P_{si}} w_{jk} \right) \]

Maximum over all the paths between \( s \) and \( i \)

Minimum over all the links forming each path

• This function is \textbf{sybilproof}. Using any sybil strategy cannot increase its value.
Sybilproofness \( \bigotimes \) is Non-Increasing

- Sybilproofness depends on contribution transfer potential over growing paths being non-increasing.

\[
W(P_{12}) \rightarrow W(P_{23}) \rightarrow W(P_{13})
\]

\[
P_{13} = P_{12} \cup P_{23}
\]
Sybilproofness (\(\otimes\) is Non-Increasing)

- Sybilproofness depends on contribution transfer potential over growing paths being non-increasing.

\[ P_{13} = P_{12} \cup P_{23} \]

\[ \mathcal{W}(P_{13}) = \mathcal{W}(P_{12}) \otimes \mathcal{W}(P_{23}) \]
Sybilproofness (☒ is Non-Increasing)

- Sybilproofness depends on contribution transfer potential over growing paths being non-increasing.

\[ W(P_{13}) = \min(W(P_{12}), W(P_{23})) \]

\[ P_{13} = P_{12} \cup P_{23} \]
Sybilproofness (\(\otimes\) is Non-Increasing)

- Sybilproofness depends on contribution transfer potential over growing paths being non-increasing.

\[ P_{13} = P_{12} \cup P_{23} \]

\[ \mathcal{W}(P_{13}) \leq \mathcal{W}(P_{12}) \]
Sybilproofness (⊕ is Non-Decreasing)

- Sybilproofness depends on contribution transfer potential being non-decreasing as additional paths are considered.
- Without loss of generality, assume $\mathcal{W}(P_{12}^1) \geq \mathcal{W}(P_{12}^2)$.
Sybilproofness

- Sybilproofness depends on contribution transfer potential being non-decreasing as additional paths are considered.
- Without loss of generality, assume $\mathcal{W}(P_{12}^1) \geq \mathcal{W}(P_{12}^2)$
Sybilproofness (⊕ is Non-Decreasing)

- Sybilproofness depends on contribution transfer potential being non-decreasing as additional paths are considered.
- Without loss of generality, assume $\mathcal{W}(P_{12}^1) \geq \mathcal{W}(P_{12}^2)$.

\[ \mathcal{W}(P_{12}^1 \cup P_{12}^2) = \mathcal{W}(P_{12}^1) \oplus \mathcal{W}(P_{12}^2) \]
Sybilproofness (⊕ is Non-Decreasing)

- Sybilproofness depends on contribution transfer potential being non-decreasing as additional paths are considered.
- Without loss of generality, assume \( \mathcal{W}(P^{1}_{12}) \geq \mathcal{W}(P^{2}_{12}) \)

\[
\mathcal{W}(P^{1}_{12} \cup P^{2}_{12}) = \max(\mathcal{W}(P^{1}_{12}), \mathcal{W}(P^{2}_{12}))
\]
Sybilproofness (⊕ is Non-Decreasing)

- Sybilproofness depends on contribution transfer potential being non-decreasing as additional paths are considered.
- Without loss of generality, assume \( \mathcal{W}(P_{12}^1) \geq \mathcal{W}(P_{12}^2) \)

\[
\mathcal{W}(P_{12}^1) \geq \mathcal{W}(P_{12}^2)
\]

\[
\mathcal{W}(P_{12}^1 \cup P_{12}^2) \geq \mathcal{W}(P_{12}^1)
\]
Resistance to Slander

- All claims that peers make regarding contributions are digitally signed, and audited by both peers involved
Resistance to Whitewashing

- New nodes need to go through a “social capital accumulation” bootstrapping phase
  - Predominantly altruistic requests
    - Best Effort Service
  - Small probability of being forwarded a PAM
    - Unable to perform contribution transfers

- Identities have nonzero value
Resistance to Account Manipulation

- Contribution accounts are maintained by peers, and might be modified at any time.
- Discrepancies can be modeled using the Prisoner’s Dilemma.
- Rich bibliography.

\[ w_{21} = 3 \quad w_{21} = 6 \]
Evaluation: Contribution Transfer

A Sybilproof Indirect Reciprocity Mechanism for Peer-to-Peer Networks

INFOCOM 2009

Raúl Landa
Conclusions

- **PledgeRoute** allows peers to
  - reduce indirect reciprocity to direct reciprocity
  - contribute resources to some peers
  - obtain resources from different peers, at later times

- The system is Sybilproof, and resistant to slander and whitewashing attacks

- The policies that **PledgeRoute** uses to process requests, select peers and forward messages implement an incentives mechanism
Thank You!