The Economics of Censorship Resistance

George Danezis & Ross Anderson

University of Cambridge, Computer Laboratory,
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom.

June 10, 2004

Outline

A brief history of on-line censorship resistance

Time line:

- `anon.penet.fi` vs the Church of Scientology (1996).
- Napster vs the music industry (2001).
- Notice & Take Down web material on ISPs.

Emergence of the peer-to-peer paradigm:

- Eternity (1996), Freenet (2000), Free Haven (2000)
- Deployed: Kazaa, Gnutella, MojoNation (RIP)
- Peer-to-peer systems and lawsuits.

A brief history of on-line censorship resistance

Time line:

- `anon.penet.fi` vs the Church of Scientology (1996).
- Napster vs the music industry (2001).
- Notice & Take Down web material on ISPs.

Emergence of the peer-to-peer paradigm:

- Eternity (1996), Freenet (2000), Free Haven (2000)
- Deployed: Kazaa, Gnutella, MojoNation (RIP)
- Peer-to-peer systems and lawsuits.

A brief history of on-line censorship resistance

Time line:

- `anon.penet.fi` vs the Church of Scientology (1996).
- Napster vs the music industry (2001).
- Notice & Take Down web material on ISPs.

Emergence of the peer-to-peer paradigm:

- Eternity (1996), Freenet (2000), Free Haven (2000)
- Deployed: Kazaa, Gnutella, MojoNation (RIP)
- Peer-to-peer systems and lawsuits.

A brief history of on-line censorship resistance

Time line:

- `anon.penet.fi` vs the Church of Scientology (1996).
- Napster vs the music industry (2001).
- Notice & Take Down web material on ISPs.

Emergence of the peer-to-peer paradigm:

- Eternity (1996), Freenet (2000), Free Haven (2000)
- Deployed: Kazaa, Gnutella, MojoNation (RIP)
- Peer-to-peer systems and lawsuits.

A brief history of on-line censorship resistance

Time line:

- `anon.penet.fi` vs the Church of Scientology (1996).
- Napster vs the music industry (2001).
- Notice & Take Down web material on ISPs.

Emergence of the peer-to-peer paradigm:

- Eternity (1996), Freenet (2000), Free Haven (2000)
- Deployed: Kazaa, Gnutella, MojoNation (RIP)
- Peer-to-peer systems and lawsuits.

A brief history of on-line censorship resistance

Time line:

- `anon.penet.fi` vs the Church of Scientology (1996).
- Napster vs the music industry (2001).
- Notice & Take Down web material on ISPs.

Emergence of the peer-to-peer paradigm:

- Eternity (1996), Freenet (2000), Free Haven (2000)
- Deployed: Kazaa, Gnutella, MojoNation (RIP)
- Peer-to-peer systems and lawsuits.

An economic model of censorship and resistance

We will create a model that describes:

- Nodes with heterogeneous preferences.
- A particular model of censorship.
- The conflict between the censor and the censored node.

Using this model:

- Compare two ways of achieving censorship resistance.
- Judge the stability of these mechanisms.
- Calculate the resistance nodes will put up and the cost to the adversary.

An economic model of censorship and resistance

We will create a model that describes:

- Nodes with heterogeneous preferences.
- A particular model of censorship.
- The conflict between the censor and the censored node.

Using this model:

- Compare two ways of achieving censorship resistance.
- Judge the stability of these mechanisms.
- Calculate the resistance nodes will put up and the cost to the adversary.

An economic model of censorship and resistance

We will create a model that describes:

- Nodes with heterogeneous preferences.
- A particular model of censorship.
- The conflict between the censor and the censored node.

Using this model:

- Compare two ways of achieving censorship resistance.
- Judge the stability of these mechanisms.
- Calculate the resistance nodes will put up and the cost to the adversary.

An economic model of censorship and resistance

We will create a model that describes:

- Nodes with heterogeneous preferences.
- A particular model of censorship.
- The conflict between the censor and the censored node.

Using this model:

- Compare two ways of achieving censorship resistance.
- Judge the stability of these mechanisms.
- Calculate the resistance nodes will put up and the cost to the adversary.

An economic model of censorship and resistance

We will create a model that describes:

- Nodes with heterogeneous preferences.
- A particular model of censorship.
- The conflict between the censor and the censored node.

Using this model:

- Compare two ways of achieving censorship resistance.
- Judge the stability of these mechanisms.
- Calculate the resistance nodes will put up and the cost to the adversary.

An economic model of censorship and resistance

We will create a model that describes:

- Nodes with heterogeneous preferences.
- A particular model of censorship.
- The conflict between the censor and the censored node.

Using this model:

- Compare two ways of achieving censorship resistance.
- Judge the stability of these mechanisms.
- Calculate the resistance nodes will put up and the cost to the adversary.

Basics

Modelling heterogeneous preferences of nodes:

- There are N nodes in the system.
- Each node can store and help distribute T resources.
- There are two kinds of resources in the system: red and blue .
- Each node prefers to distribute a balanced amount of red and blue resources according to its preferences r_i and b_i ($r_i + b_i = 1$).

Example

A left-leaning node might prefer to help distribute mostly Guardian articles instead of Telegraph articles ($r_i = 0.9$ and $b_i = 0.1$). A node will less partisan views might prefer to maintain a more even balance ($r_i = 0.5$ and $b_i = 0.5$).

Basics

Modelling heterogeneous preferences of nodes:

- There are N nodes in the system.
- Each node can store and help distribute T resources.
- There are two kinds of resources in the system: red and blue .
- Each node prefers to distribute a balanced amount of red and blue resources according to its preferences r_i and b_i ($r_i + b_i = 1$).

Example

A left-leaning node might prefer to help distribute mostly Guardian articles instead of Telegraph articles ($r_i = 0.9$ and $b_i = 0.1$). A node will less partisan views might prefer to maintain a more even balance ($r_i = 0.5$ and $b_i = 0.5$).

Basics

Modelling heterogeneous preferences of nodes:

- There are N nodes in the system.
- Each node can store and help distribute T resources.
- There are two kinds of resources in the system: red and blue .
- Each node prefers to distribute a balanced amount of red and blue resources according to its preferences r_i and b_i ($r_i + b_i = 1$).

Example

A left-leaning node might prefer to help distribute mostly Guardian articles instead of Telegraph articles ($r_i = 0.9$ and $b_i = 0.1$). A node will less partisan views might prefer to maintain a more even balance ($r_i = 0.5$ and $b_i = 0.5$).

Basics

Modelling heterogeneous preferences of nodes:

- There are N nodes in the system.
- Each node can store and help distribute T resources.
- There are two kinds of resources in the system: red and blue .
- Each node prefers to distribute a balanced amount of red and blue resources according to its preferences r_i and b_i ($r_i + b_i = 1$).

Example

A left-leaning node might prefer to help distribute mostly Guardian articles instead of Telegraph articles ($r_i = 0.9$ and $b_i = 0.1$). A node will less partisan views might prefer to maintain a more even balance ($r_i = 0.5$ and $b_i = 0.5$).

Basics

Modelling heterogeneous preferences of nodes:

- There are N nodes in the system.
- Each node can store and help distribute T resources.
- There are two kinds of resources in the system: red and blue .
- Each node prefers to distribute a balanced amount of red and blue resources according to its preferences r_i and b_i ($r_i + b_i = 1$).

Example

A left-leaning node might prefer to help distribute mostly Guardian articles instead of Telegraph articles ($r_i = 0.9$ and $b_i = 0.1$). A node will less partisan views might prefer to maintain a more even balance ($r_i = 0.5$ and $b_i = 0.5$).

A unimodal utility model

We reflect the balance of red and blue resources a node holds and helps distribute through using a unimodal utility model.
A node that holds R red resources and B blue resources (with $R + B = T$) has a utility of:

$$U_i(R, B) = -T(R/T - r_i - 1)(R/T - r_i + 1) \quad (1)$$

- Maximal utility when $R = r_i T$ and $B = b_i T$.
- Utility decreases as the balance R, B shifts away.

A unimodal utility model

We reflect the balance of red and blue resources a node holds and helps distribute through using a unimodal utility model.
A node that holds R red resources and B blue resources (with $R + B = T$) has a utility of:

$$U_i(R, B) = -T(R/T - r_i - 1)(R/T - r_i + 1) \tag{1}$$

- Maximal utility when $R = r_i T$ and $B = b_i T$.
- Utility decreases as the balance R, B shifts away.

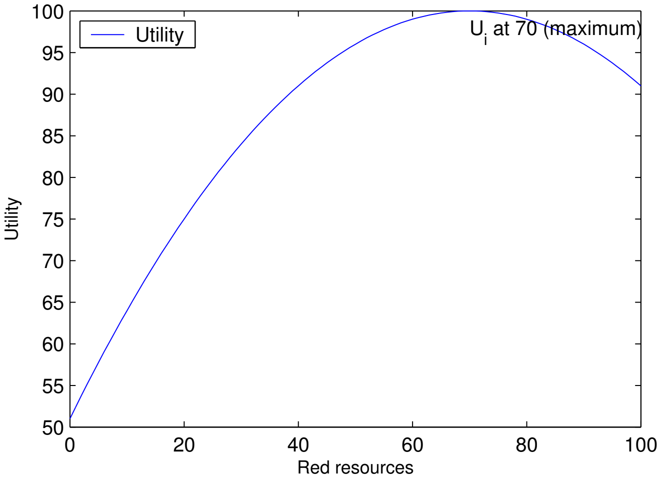
A unimodal utility model

We reflect the balance of red and blue resources a node holds and helps distribute through using a unimodal utility model.
A node that holds R red resources and B blue resources (with $R + B = T$) has a utility of:

$$U_i(R, B) = -T(R/T - r_i - 1)(R/T - r_i + 1) \quad (1)$$

- Maximal utility when $R = r_i T$ and $B = b_i T$.
- Utility decreases as the balance R, B shifts away.

Graphically



Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share.*
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), . . .

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share.*
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), ...

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share*.
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), . . .

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share.*
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), . . .

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share.*
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), . . .

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share*.
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), ...

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share*.
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), . . .

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share*.
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), ...

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share*.
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), ...

Which is better?

Two paradigms for censorship resistance

The random model:

- Resources are *scattered randomly* across some nodes.
- Censorship would inconvenience everyone.
- Difficult to select target nodes.
- Eternity, Freenet, FreeHaven, Distributed Hash Tables.

The Discretionary model:

- Nodes download whatever they like and *chose what to share*.
- Sharing happens as a by-product of other activities.
- Kazaa, Gnutella, eDonkey (eMule), . . .

Which is better?

In terms of our model...

- In the *discretionary model* nodes can chose the balance of resources they hold. They will try to maximise their utility by having $R = r_i T$ red resources and $B = b_i T$ blue resources.
- In the *random model* each node receives a sample of all resources stored in the system. If the system stores R red resources and B blue resources, each node will hold $R = r_s T$ red resources and $B = b_s T$ blue resources where r_s and b_s are:

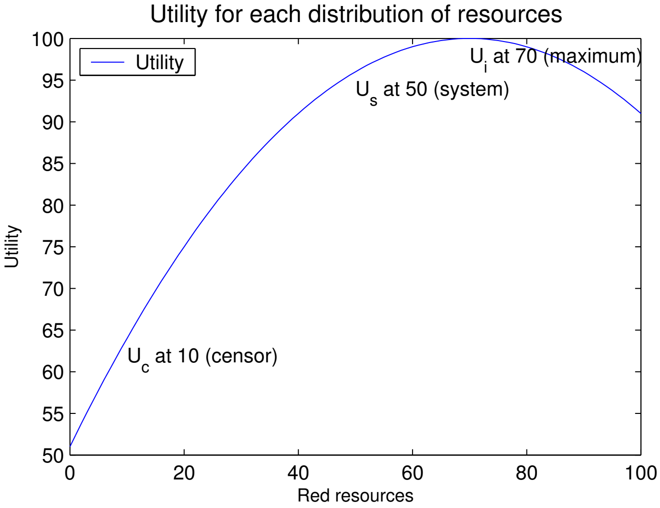
$$r_s = \frac{\mathcal{R}}{\mathcal{R} + \mathcal{B}} \qquad b_s = \frac{\mathcal{B}}{\mathcal{R} + \mathcal{B}} \tag{2}$$

In terms of our model...

- In the *discretionary model* nodes can chose the balance of resources they hold. They will try to maximise their utility by having $R = r_i T$ red resources and $B = b_i T$ blue resources.
- In the *random model* each node receives a sample of all resources stored in the system. If the system stores R red resources and B blue resources, each node will hold $R = r_s T$ red resources and $B = b_s T$ blue resources where r_s and b_s are:

$$r_s = \frac{\mathcal{R}}{\mathcal{R} + \mathcal{B}} \qquad b_s = \frac{\mathcal{B}}{\mathcal{R} + \mathcal{B}} \tag{2}$$

Graphically



Preliminary comparison

- The utility of a node in the *random model* is lower or equal to its utility in the *discretionary model*.

$$U_i(r_i T, b_i T) \geq U_i(r_s T, b_s T) \quad (3)$$

Unless $r_i = r_s$ and $b_i = b_s$.

- Unless all nodes in the system have equal r_i and b_i there is no set system-wide values r_s and b_s that can maximise the utility of all nodes.

Preliminary comparison

- The utility of a node in the *random model* is lower or equal to its utility in the *discretionary model*.

$$U_i(r_i T, b_i T) \geq U_i(r_s T, b_s T) \tag{3}$$

  Unless $r_i = r_s$ and $b_i = b_s$.
- Unless all nodes in the system have equal r_i and b_i there is no set system-wide values r_s and b_s that can maximise the utility of all nodes.

Preliminary comparison (2)

- In the random model each node has incentives to cheat to shift the system-wide parameters r_s and b_s towards its own preferences.
  Flooding, reputation attacks, denial of service, dropping resources, ... and we have not even talked about censorship yet!
- The system-wide parameters need to be set in a *fair* way: elections, e-cash, reputation, ..., need to resist attacks.
- Even then nodes have incentives to leave the network to join another one with parameters that matches their preferences closer.

Preliminary comparison (2)

- In the random model each node has incentives to cheat to shift the system-wide parameters r_s and b_s towards its own preferences.
  Flooding, reputation attacks, denial of service, dropping resources, ... and we have not even talked about censorship yet!
- The system-wide parameters need to be set in a *fair* way: elections, e-cash, reputation, ..., need to resist attacks.
- Even then nodes have incentives to leave the network to join another one with parameters that matches their preferences closer.

Preliminary comparison (2)

- In the random model each node has incentives to cheat to shift the system-wide parameters r_s and b_s towards its own preferences.
  Flooding, reputation attacks, denial of service, dropping resources, . . . and we have not even talked about censorship yet!
- The system-wide parameters need to be set in a *fair* way: elections, e-cash, reputation, . . . , need to resist attacks.
- Even then nodes have incentives to leave the network to join another one with parameters that matches their preferences closer.

Preliminary comparison (2)

- In the random model each node has incentives to cheat to shift the system-wide parameters r_s and b_s towards its own preferences.
  Flooding, reputation attacks, denial of service, dropping resources, ... and we have not even talked about censorship yet!
- The system-wide parameters need to be set in a *fair* way: elections, e-cash, reputation, ..., need to resist attacks.
- Even then nodes have incentives to leave the network to join another one with parameters that matches their preferences closer.

Preliminary comparison (2)

- In the random model each node has incentives to cheat to shift the system-wide parameters r_s and b_s towards its own preferences.
  Flooding, reputation attacks, denial of service, dropping resources, . . . and we have not even talked about censorship yet!
- The system-wide parameters need to be set in a *fair* way: elections, e-cash, reputation, . . . , need to resist attacks.
- Even then nodes have incentives to leave the network to join another one with parameters that matches their preferences closer.

Introducing censorship

Censorship:

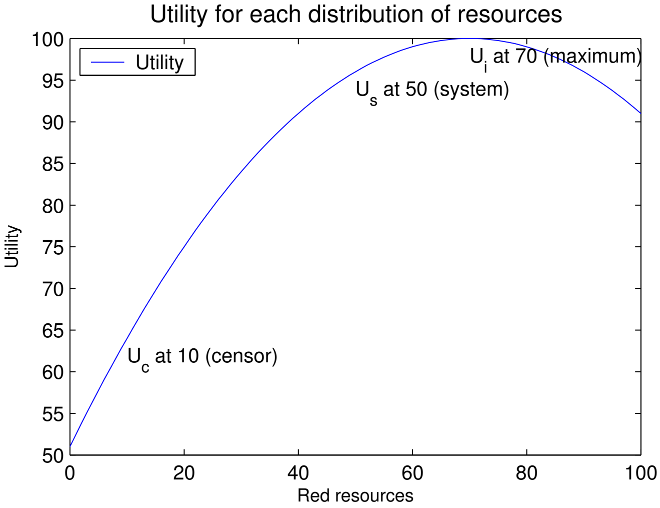
- A censor targets a set of individual nodes.
- He imposes on them a particular distribution $r_c T$ of red resources and $b_c T$ of blue resources.

Introducing censorship

Censorship:

- A censor targets a set of individual nodes.
- He imposes on them a particular distribution $r_c T$ of red resources and $b_c T$ of blue resources.

Graphically



Introducing resistance

A node under censorship can chose to resist:

- It sets aside a *defence budget* t.
- The defence budget is subtracted from its ability to distribute resources $(T - t)$.
- A node has a probability $P(t)$ of foiling censorship depending of its defence budget t.

$$P(t) = \frac{1}{T}t \tag{4}$$

$(P(T) = 1$ and $P(0) = 0)$

- If it foils censorship a node has its previous distribution of resources, otherwise it has the distribution imposed by the censor.

Introducing resistance

A node under censorship can chose to resist:

- It sets aside a *defence budget* t.
- The defence budget is subtracted from its ability to distribute resources $(T - t)$.
- A node has a probability $P(t)$ of foiling censorship depending of its defence budget t.

$$P(t) = \frac{1}{T}t \tag{4}$$

  $(P(T) = 1$ and $P(0) = 0)$

- If it foils censorship a node has its previous distribution of resources, otherwise it has the distribution imposed by the censor.

Introducing resistance

A node under censorship can chose to resist:

- It sets aside a *defence budget* t.
- The defence budget is subtracted from its ability to distribute resources $(T - t)$.
- A node has a probability $P(t)$ of foiling censorship depending of its defence budget t.

$$P(t) = \frac{1}{T} t \tag{4}$$

$(P(T) = 1 \text{ and } P(0) = 0)$

- If it foils censorship a node has its previous distribution of resources, otherwise it has the distribution imposed by the censor.

Introducing resistance

A node under censorship can chose to resist:

- It sets aside a *defence budget* t.
- The defence budget is subtracted from its ability to distribute resources $(T - t)$.
- A node has a probability $P(t)$ of foiling censorship depending of its defence budget t.

$$P(t) = \frac{1}{T} t \tag{4}$$

$(P(T) = 1$ and $P(0) = 0)$

- If it foils censorship a node has its previous distribution of resources, otherwise it has the distribution imposed by the censor.

Utility and defence budget: *discretionary model*

A node in the *discretionary model* has an expected utility of:

$$U = P(t)U_i(r_i(T-t), b_i(T-t)) + (1-P(t))U_i(r_c(T-t), b_c(T-t)) \quad (5)$$

Expected utility is maximised when the defence budget is:

$$t_d = \frac{T}{2}\frac{2U_i(r_c, b_c) - U_i(r_i, b_i)}{U_i(r_c, b_c) - U_i(r_i, b_i)} \quad (6)$$

For the defence budget t_d to be positive it must be that:

$$U_i(r_c T, b_c T) < U_i(r_i T, b_i T) \quad (7)$$

$$2U_i(r_c, b_c) < U_i(r_i, b_i) \quad (8)$$

Utility and defence budget: *discretionary model*

A node in the *discretionary model* has an expected utility of:

$$U = P(t)U_i(r_i(T-t), b_i(T-t)) + (1-P(t))U_i(r_c(T-t), b_c(T-t)) \quad (5)$$

Expected utility is maximised when the defence budget is:

$$t_d = \frac{T}{2}\frac{2U_i(r_c, b_c) - U_i(r_i, b_i)}{U_i(r_c, b_c) - U_i(r_i, b_i)} \quad (6)$$

For the defence budget t_d to be positive it must be that:

$$U_i(r_c T, b_c T) < U_i(r_i T, b_i T) \quad (7)$$

$$2U_i(r_c, b_c) < U_i(r_i, b_i) \quad (8)$$

Utility and defence budget: *discretionary model*

A node in the *discretionary model* has an expected utility of:

$$U = P(t)U_i(r_i(T-t), b_i(T-t)) + (1-P(t))U_i(r_c(T-t), b_c(T-t)) \quad (5)$$

Expected utility is maximised when the defence budget is:

$$t_d = \frac{T}{2}\frac{2U_i(r_c, b_c) - U_i(r_i, b_i)}{U_i(r_c, b_c) - U_i(r_i, b_i)} \quad (6)$$

For the defence budget t_d to be positive it must be that:

$$U_i(r_c T, b_c T) < U_i(r_i T, b_i T) \quad (7)$$

$$2U_i(r_c, b_c) < U_i(r_i, b_i) \quad (8)$$

Utility and defence budget: *random model*

Similarly for the *random model* the defence budget will be:

$$t_s = \frac{T}{2} \frac{2U_i(r_c, b_c) - U_i(r_s, b_s)}{U_i(r_c, b_c) - U_i(r_s, b_s)} \tag{9}$$

Note that:

$$\forall i \in \mathcal{S}, t_d \geq t_s \Rightarrow \sum_{i \in \mathcal{S}} t_d \geq \sum_{i \in \mathcal{S}} t_s \tag{10}$$

Therefore the defence budget of a node in the random model will be lower than in the discretionary model.

The overall effort in defence of any set of nodes will also be lower.

Utility and defence budget: *random model*

Similarly for the *random model* the defence budget will be:

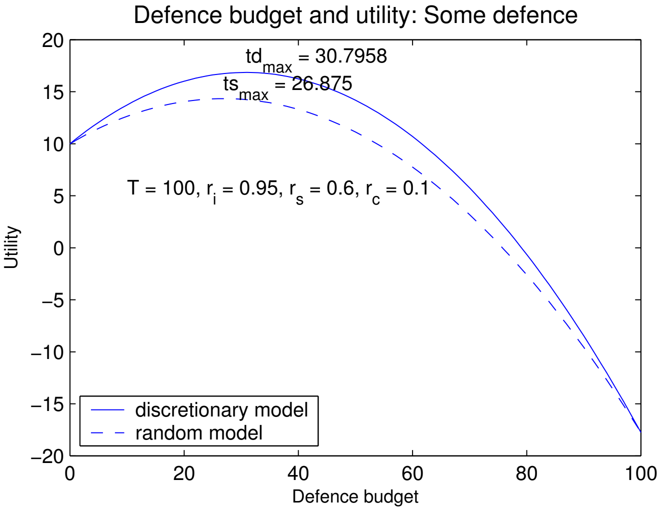
$$t_s = \frac{T}{2} \frac{2U_i(r_c, b_c) - U_i(r_s, b_s)}{U_i(r_c, b_c) - U_i(r_s, b_s)} \tag{9}$$

Note that:

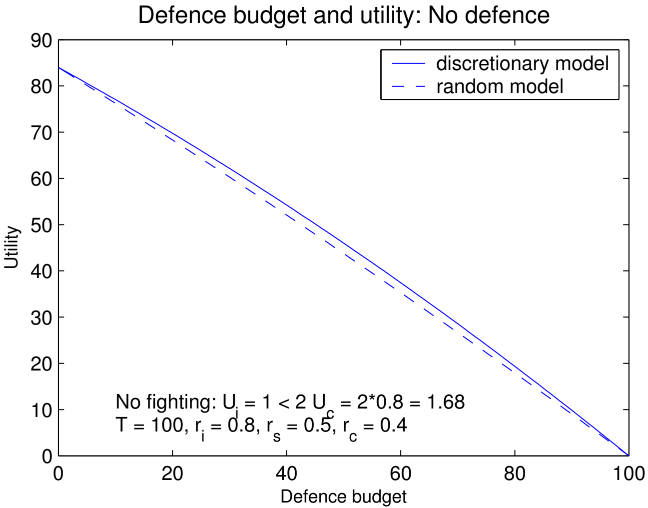
$$\forall i \in \mathcal{S}, t_d \geq t_s \Rightarrow \sum_{i \in \mathcal{S}} t_d \geq \sum_{i \in \mathcal{S}} t_s \tag{10}$$

Therefore the defence budget of a node in the random model will be lower than in the discretionary model.
The overall effort in defence of any set of nodes will also be lower.

Some defence



No defence


Defence budget and utility: No defence
discretionary model
random model
No fighting: U_i = 1 < 2 U_c = 2*0.8 = 1.68
T = 100, r_i = 0.8, r_s = 0.5, r_c = 0.4
Utility
Defence budget
0
10
20
30
40
50
60
70
80
90
0
20
40
60
80
100

A first framework to evaluate censorship resistance

- Utility is about local distribution.
  (What if the red files are globally available?)
- Censorship and defence are local.
  (Censorship resistance is not transformed into a public good)
- Abstract away from real implementation costs.
  (Some random models might be technically more efficient)
- What about the strategy of the censor?

A first framework to evaluate censorship resistance

- Utility is about local distribution.
  (What if the red files are globally available?)
- Censorship and defence are local.
  (Censorship resistance is not transformed into a public good)
- Abstract away from real implementation costs.
  (Some random models might be technically more efficient)
- What about the strategy of the censor?

A first framework to evaluate censorship resistance

- Utility is about local distribution.
  (What if the red files are globally available?)
- Censorship and defence are local.
  (Censorship resistance is not transformed into a public good)
- Abstract away from real implementation costs.
  (Some random models might be technically more efficient)
- What about the strategy of the censor?

A first framework to evaluate censorship resistance

- Utility is about local distribution.
  (What if the red files are globally available?)
- Censorship and defence are local.
  (Censorship resistance is not transformed into a public good)
- Abstract away from real implementation costs.
  (Some random models might be technically more efficient)
- What about the strategy of the censor?

Random or discretionary model?

- Discretionary model provides higher utility and a higher local and global defence budget.
- Random model makes the network more fragile: nodes have incentives to cheat or leave.
- Random model introduces the need for complex mechanisms such as elections, reputation, public verifiability...

Random or discretionary model?

- Discretionary model provides higher utility and a higher local and global defence budget.
- Random model makes the network more fragile: nodes have incentives to cheat or leave.
- Random model introduces the need for complex mechanisms such as elections, reputation, public verifiability...

Random or discretionary model?

- Discretionary model provides higher utility and a higher local and global defence budget.
- Random model makes the network more fragile: nodes have incentives to cheat or leave.
- Random model introduces the need for complex mechanisms such as elections, reputation, public verifiability. . .