

Anonymity Networks

Laslo Hunhold

Mathematisches Institut
Universität zu Köln

27th July 2017

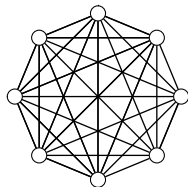


In the lecture '*Information Theory and Statistical Physics*' by Prof. Dr. Johannes BERG

motivation

- ▶ hide initiator of a message in a computer network
- ▶ safe whistleblowing under corporate and state surveillance
- ▶ 'deniable communication'
- ▶ decentralized

idea



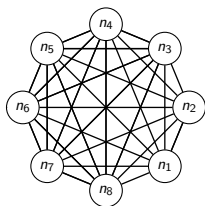
node network participant

link possible message path

- ▶ all nodes have equal weight
- ▶ message unmodifiable, only receiver is known
- ▶ each node on path: biased coin flip: forward or deliver
- ▶ each node on path: initiator or just forwarder?

→ message initiator gets lost in the crowd

model



- ▶ N nodes n_1, \dots, n_N with $\mathbb{P}(n_i \text{ is initiator}) =: \mathbb{P}(X = n_i) =: p_i$
- ▶ n_i probably innocent $\leftrightarrow p_i \leq \frac{1}{2}$
- ▶ forwarding probability λ

if message received **then**

flip biased coin $\mathbb{P}(\text{heads}) = \lambda$

if heads **then**

forward to a uniformly chosen node

else

deliver to receiver

end if

end if

degree of anonymity

best case $\bar{X} := X : \forall i \in \{1, \dots, N\} : p_i = \frac{1}{N}$

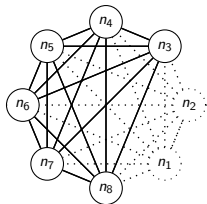
$$\bar{H} := H(\bar{X}) = - \sum_{i=1}^N p_i \cdot \ln(p_i) = \ln(N - C)$$

worst case $\underline{X} := X : \forall i \in \{1, \dots, N\} \setminus \{j\} : p_i = 0 \wedge p_j = 1$

$$\underline{H} := H(\underline{X}) = - \sum_{i=1}^N p_i \cdot \ln(p_i) = 1 \cdot \ln(1) = 0$$

$$d(X) := 1 - \frac{\bar{H} - H(X)}{\bar{H}} = \frac{H(X)}{\bar{H}} \in [0, 1]$$

corruption

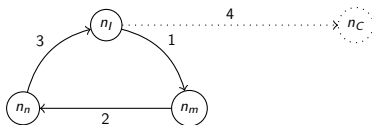


- ▶ $0 \leq C < N$ corrupt nodes (incoming message passer known)
- ▶ behave normally
- ▶ wait for message to be passed to us
- ▶ analyze probability of passer being initiator

$\mathbb{P}(\text{passer is initiator}) > \frac{1}{2} \rightarrow \text{unmasked}$

analysis

events



let $k > 0$

$H_k :=$ first corrupt node is at the k th path-position

$$H_{k+} := \bigvee_{i=k}^{\infty} H_i$$

$I :=$ first corrupt node immediately postcedes the message initiator

$$\mathbb{P}(\text{passer is initiator}) = \mathbb{P}(I | H_{1+})$$

note: $H_1 \rightarrow I$, but $I \not\rightarrow H_1$

analysis

general probability I

$$\mathbb{P}(I|H_{1+}) = \frac{N - \lambda(N - C - 1)}{N}$$

proof:

$$\mathbb{P}(H_k) = \left(\lambda \cdot \frac{N - C}{N}\right)^{k-1} \cdot \left(\lambda \cdot \frac{C}{N}\right)$$

$$\Rightarrow \mathbb{P}(H_{k+}) = \sum_{i=k}^{\infty} \mathbb{P}(H_i) = \dots = \frac{C \cdot \left(\lambda \cdot \frac{N-C}{N}\right)^k}{(N - C) \cdot \left(1 - \lambda \cdot \frac{N-C}{N}\right)}$$

$$H_1 \rightarrow I \Rightarrow \mathbb{P}(I|H_1) = 1$$

$$\mathbb{P}(I|H_{2+}) = \frac{1}{N - C}$$

analysis

general probability II

$$\begin{aligned}\mathbb{P}(I) &\stackrel{TP}{=} \mathbb{P}(H_1) \mathbb{P}(I|H_1) + \mathbb{P}(H_{2+}) \mathbb{P}(I|H_{2+}) = \dots \\ &= \frac{\lambda \cdot C}{N} \cdot \left(1 + \frac{\lambda}{N - \lambda \cdot (N - C)} \right)\end{aligned}$$

$$\begin{aligned}\mathbb{P}(I|H_{1+}) &\stackrel{CP}{=} \frac{\mathbb{P}(I \wedge H_{1+})}{\mathbb{P}(H_{1+})} \quad | \quad I \rightarrow H_{1+} \\ &= \frac{\mathbb{P}(I)}{\mathbb{P}(H_{1+})} = \dots \\ &= \frac{N - \lambda(N - C - 1)}{N}\end{aligned}$$

□

good node $\mathbb{P}(\text{good node } i \text{ is initiator}) = \frac{1 - \mathbb{P}(I|H_{1+})}{N - C - 1} = \frac{\lambda}{N} < \frac{1}{N} \leq \frac{1}{2}$
 \Rightarrow all good nodes besides passer are innocent

corrupt node $\mathbb{P}(\text{corrupt node } i \text{ is initiator}) = 0$

analysis

passer innocence

$$\text{passer innocent} \Leftrightarrow \lambda > \frac{1}{2} \wedge N \geq \frac{1}{1 - \frac{1}{2 \cdot \lambda}} \cdot (C + 1)$$

proof:

$$\frac{1}{2} \geq \mathbb{P}(I|H_{1+}) = \frac{N - \lambda(N - C - 1)}{N} \quad \Bigg| \quad \left(\lambda - \frac{1}{2}\right) > 0$$

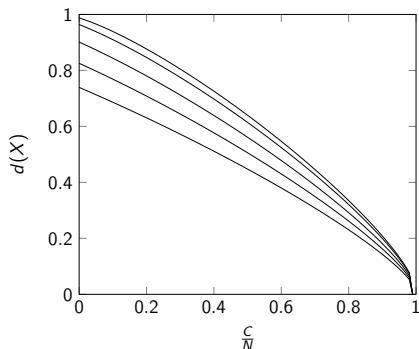
$$\Leftrightarrow N \geq \frac{1}{1 - \frac{1}{2 \cdot \lambda}} \cdot (C + 1)$$



analysis

degree of anonymity

$$\begin{aligned}d(X) &= \frac{C \cdot 0 + \mathbb{P}(I|H_{1+}) \cdot \ln(\mathbb{P}(I|H_{1+})) + (N - C - 1) \cdot \frac{\lambda}{N} \cdot \ln\left(\frac{\lambda}{N}\right)}{\ln(N - C)} \\ &= \dots = \frac{(N - \lambda \cdot (N - C - 1)) \cdot \ln\left(\frac{N}{N - \lambda \cdot (N - C - 1)}\right) + \lambda \cdot (N - C - 1) \cdot \ln\left(\frac{N}{\lambda}\right)}{N \cdot \ln(N - C)}\end{aligned}$$



conclusion

- ▶ blending in with the crowd works as long as it is large enough
- ▶ nothing to hide, but others to protect
- ▶ full paper on <http://frign.de/>