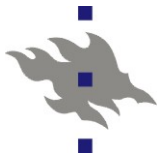
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

# Update on Freenet v0.75

**Prof. Sasu Tarkoma**

**21.1.2013**



# Freenet v0.75

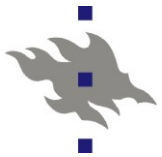
We have covered two different versions of Freenet, prior 0.7 and 0.7.

Version 0.75 builds on 0.7 and has some new elements

Details in article (The Dark Freenet, 2010)
https://freenetproject.org/papers/freenet-0.7.5-paper.pdf

Limiting connections to trusted nodes preferred (”Darknet”)
New user must know an existing user and be authenticated by the user

Alternative ”Opennet” mode possible without authentication



# v0.75 routing (similar to 0.7)

Assumes small-world property observed in how people relate in the real-life (and how airports etc. form), average path length is small

Small-world: each node in the network knows its physical neighbors as well as a small number of randomly chosen distant nodes.

Locations and keys (as numbers), Locations are identities in the network

Key-based routing with backtracking with the location optimization

Initially random keys, then location swapping to cluster nodes close in the network topology

Initiate swap with a probe message (random walk) that has a TTL (typically six)

# Location swapping details

1. A node $A$ randomly chooses a node $B$ in its proximity and initiates a swap request. Both nodes share the locations of their respective neighbors and calculate $D_1(A,B)$. $D_1(A,B)$ is the product of the existing distances between $A$ and each of $A$'s neighbors $|L(a)-L(n)|$ multiplied by the product of the existing distances between $B$ and each of $B$'s neighbors.

$$D_1(A,B) = \prod_{(A,n)\in E} |L(A)-L(n)| \cdot \prod_{(B,n)\in E} |L(B)-L(n)| \tag{1}$$

2. The nodes also compute $D_2(A,B)$, the product of the products of the differences between their locations and their neighbors' locations *after* a potential swap:

$$D_2(A,B) = \prod_{(A,n)\in E} |L(B)-L(n)| \cdot \prod_{(B,n)\in E} |L(A)-L(n)| \tag{2}$$

3. If the nodes find that $D_2(A,B) \leq D_1(A,B)$, they swap locations, otherwise they swap locations with probability $\frac{D_1(A,B)}{D_2(A,B)}$. The deterministic swap always decreases the average distances of nodes with their neighbors. The probabilistic swap is used to escape local minima.

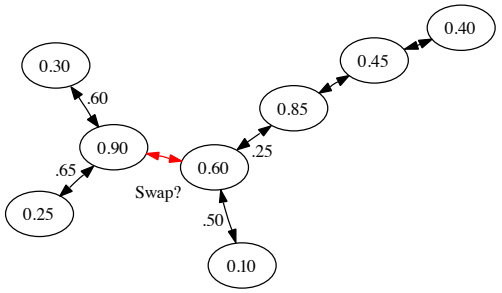
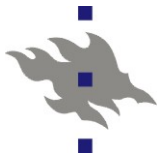



**Figure 2. This figure shows an example network with two nodes considering a swap. The result of the swap equation is $D_1$ = .60 * .65 * .25 * .50 = .04875 and $D_2$ = .30 * .35 * .05 * .80 = .0042. Since $D_1 > D_2$, they swap.**

N. Evans et al. Routing in the Dark: Pitch Black



# Details on SSK

The author generates a cryptographic keypair and a symmetric key (from the description)

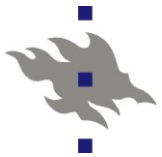
When a file is inserted into Freenet, it is encrypted with the symmetric key and signed with the private key. The signature is stored with the file.

The SSK consists of:

a hash of the public key, and the symmetric key.

Freenet nodes can verify the signature when the SSK file comes into their node, and also so that clients can verify the signature when retrieving the file. The symmetric key is used by clients to decrypt the file.

Only node with private key can write (create new versions)



# Review Questions on v0.75

**How can Freenet verify processed/routed documents?**

1. By utilizing the document key that is a hash of the document. It is easy to verify. 2. Using PKI and metadata. Check signature.

**What about latency, does the routing take delay into account?**

In 2003-2005 Freenet used latency as a metric for routing, this was replaced by the small world design that uses the overlay topology distance (location numbers). Security/performance are open issues at the moment.

**Is location swapping secure?**

No, location swapping is vulnerable to certain kinds of attacks (bogus swap requests to drag location toward specific point). It is a weak point in the system and an open issue in the community.

https://wiki.freenetproject.org/Research_challenges

# Review questions II

**When does a node store a document?**

When it is closer to the key than the neighbours.

**What about storage?**

Files are encrypted, but for some files the nodes will know the encryption key (CHK that hashes the description for the key).

**How are versions managed (website etc.)**

SSK is used for a site. You increment a version number each time you update. You use USK (Updatable Subspace Key) to point to the current version. You can thus append and modify content (but it gets a new version number).

**What caching policy is used by Freenet?**

0.75 uses a random scheme (earlier versions LRU)