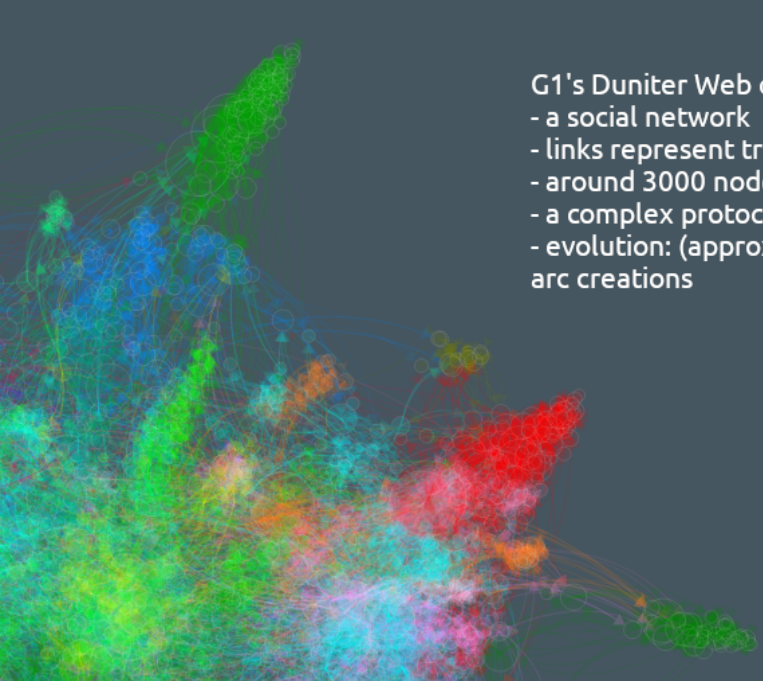
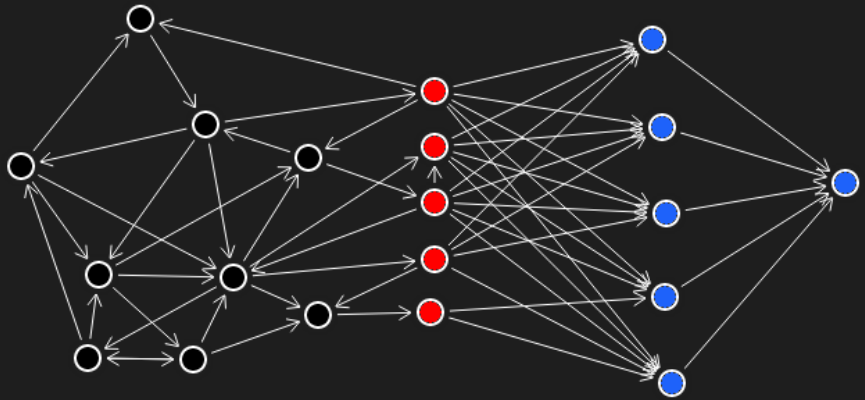
Analysis of the Sybil defense of Duniter-based cryptocurrencies

Lucas Isenmann

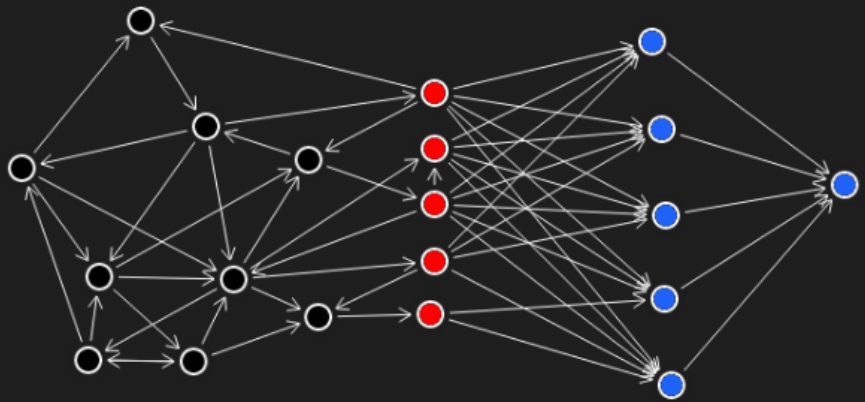
Université de Montpellier, LIRMM



G1's Duniter Web of Trust in 2021:
- a social network
- links represent trust
- around 3000 nodes
- a complex protocol
- evolution: (approximately) 2 rules about node and arc creations

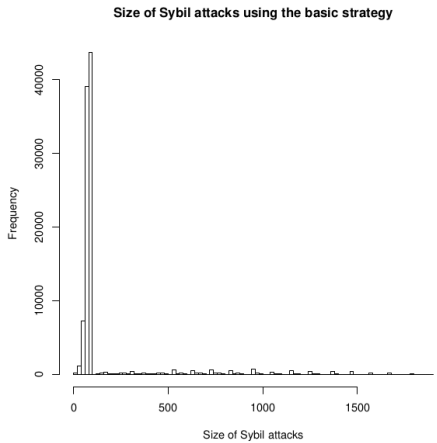

honests
attackers
fake

$$attack(A) \leq c(A)\frac{(\Delta-\delta+1)^k-1}{\Delta-\delta}$$



Conclusions

- in theory Sybil attacks are limited but can be huge
- in practice, Sybil attacks are not so huge



Openings

- time and social constraints also limit Sybil attacks
- consider more clever Sybil attack strategies
- precision of the simplification?