We want to avoid marking or encrypting normal traffic. We want to avoid marking or encrypting normal traffic.

Secure Sampling

Packets require keys and crypto, therefore secure sampling does not work. Good for short connections because no key lookups / key exchange required.

Statistical Fault Localization

Secure fault localization (FL): slow, but does not need key infrastructure.

Adversarial powers covers active attack by hacked routers, greedy ISPs, and botnets. Protocols are incentive compatible because only the end points are involved.

Protocols are efficient enough to run in high adversarially.

Conclusions

Composing PQM for client and server setting is the same as generic secure sampling except that:

- If the packet loss rate on the path is less than 5%, then we do not run secure fault localization.
- Otherwise, we run secure fault localization.

Sent statistics: probes until the end of the salt interval.