

Hybrid Mobile Anonymity Networks (Cellular and Peer-to-Peer)

Francesco Pittaluga

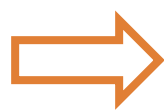
Background

Problem

Cellular network operators are a potentially dangerous adversary. By default, they have the capability to observe all paths and locate every node in the network.

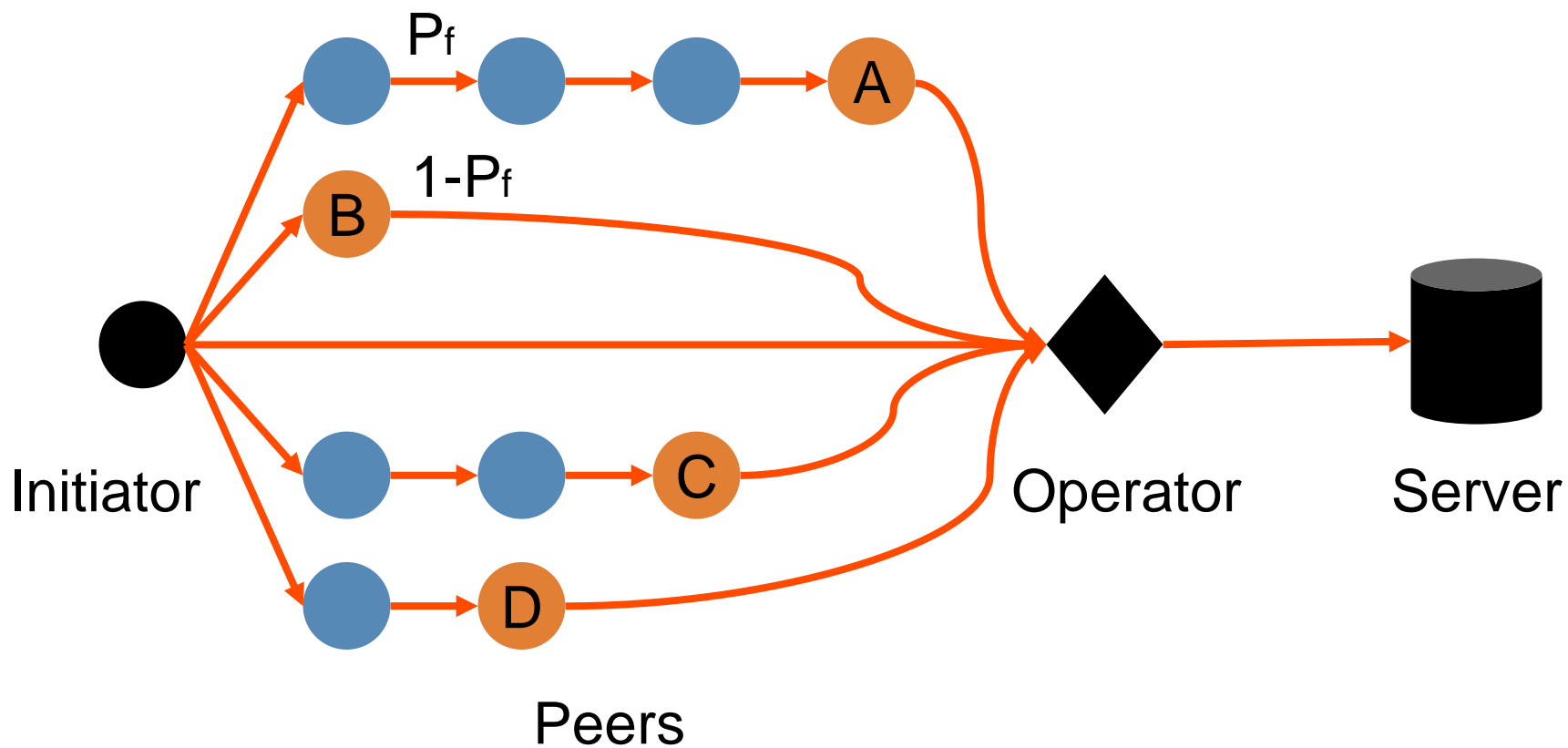
Solution (Adagna et al. 2010)

Leverage mobile phones Wi-Fi and Bluetooth capabilities to create a hybrid cellular and peer-to-peer (P2P) network.

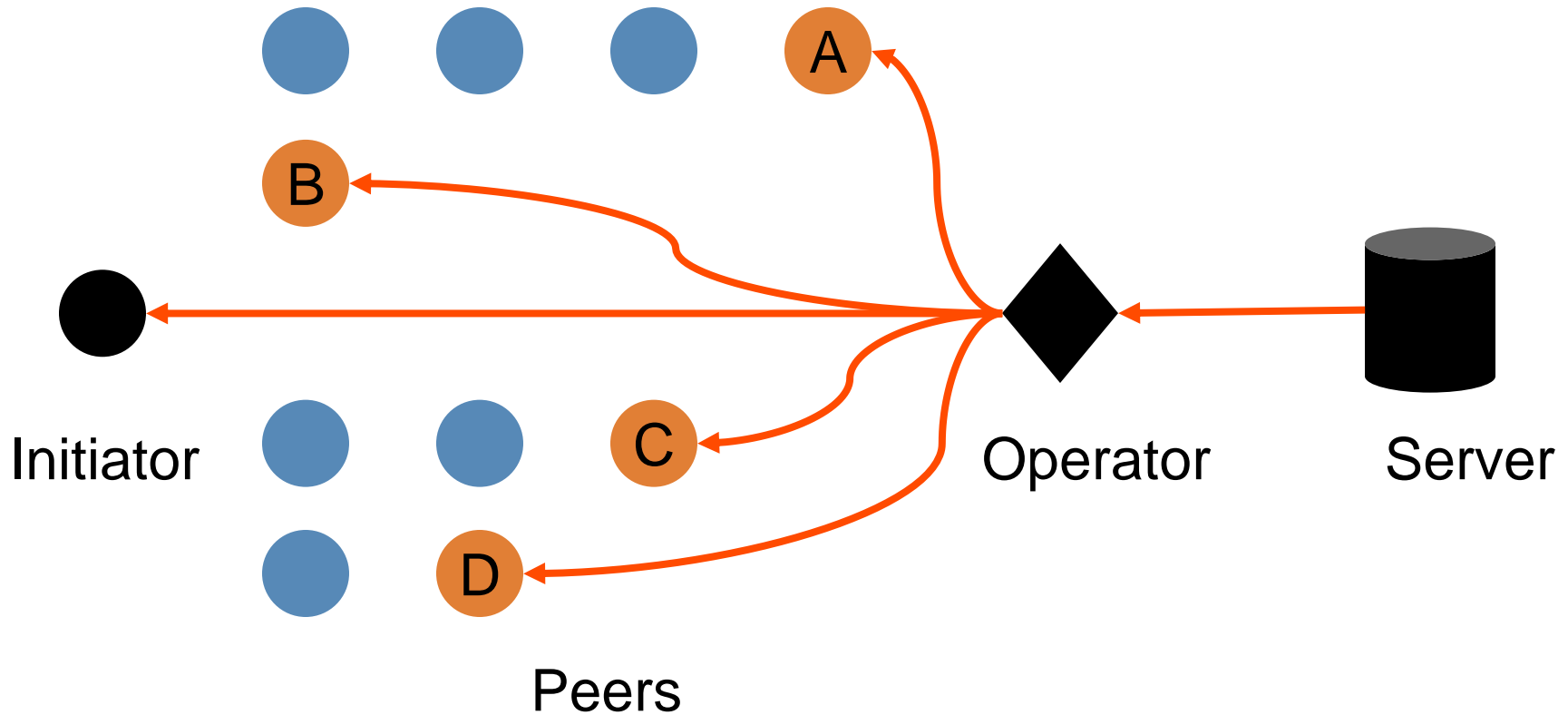


P2P network can't be observed by the operator, so peers can achieve “crowd” based anonymity.

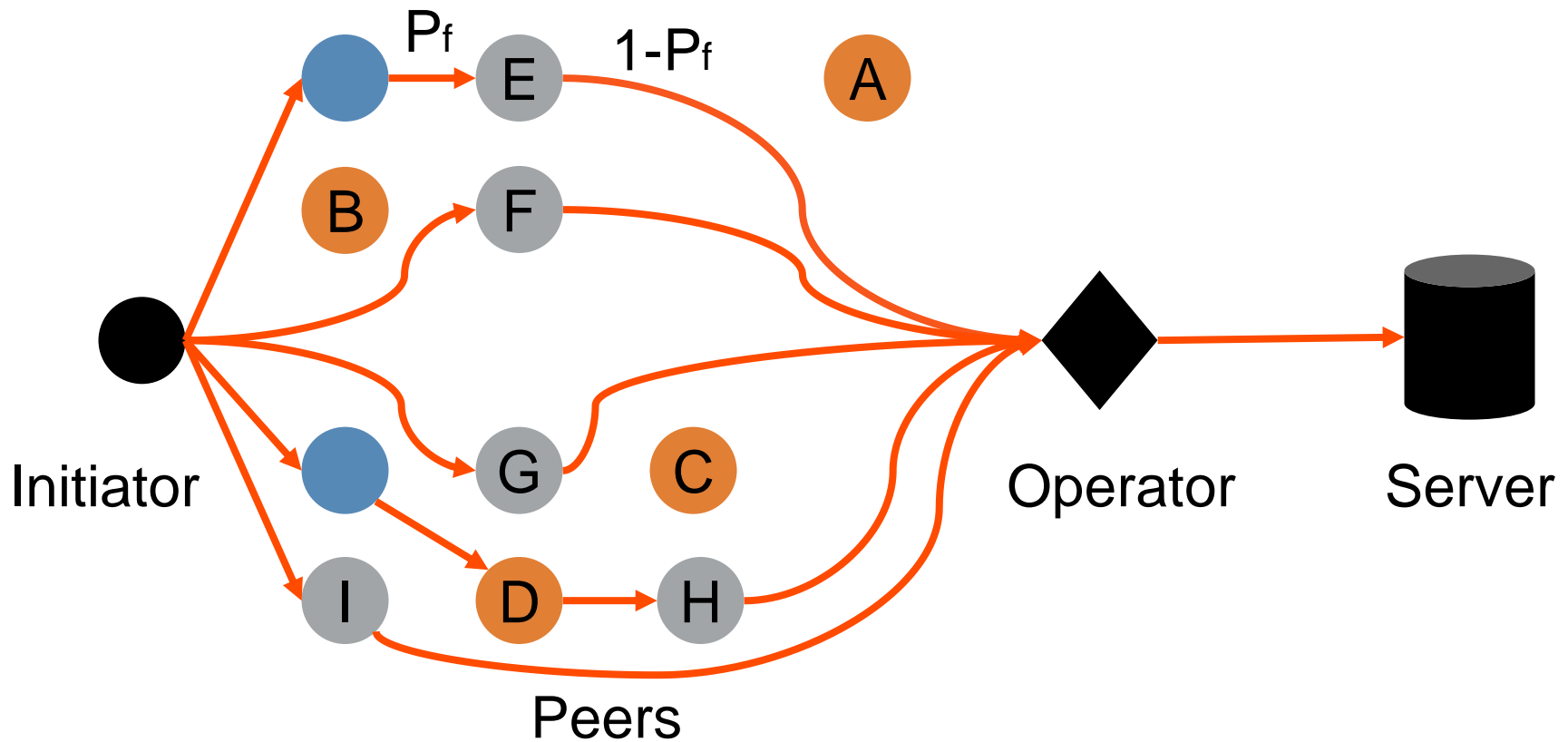
Connection Establishment Request



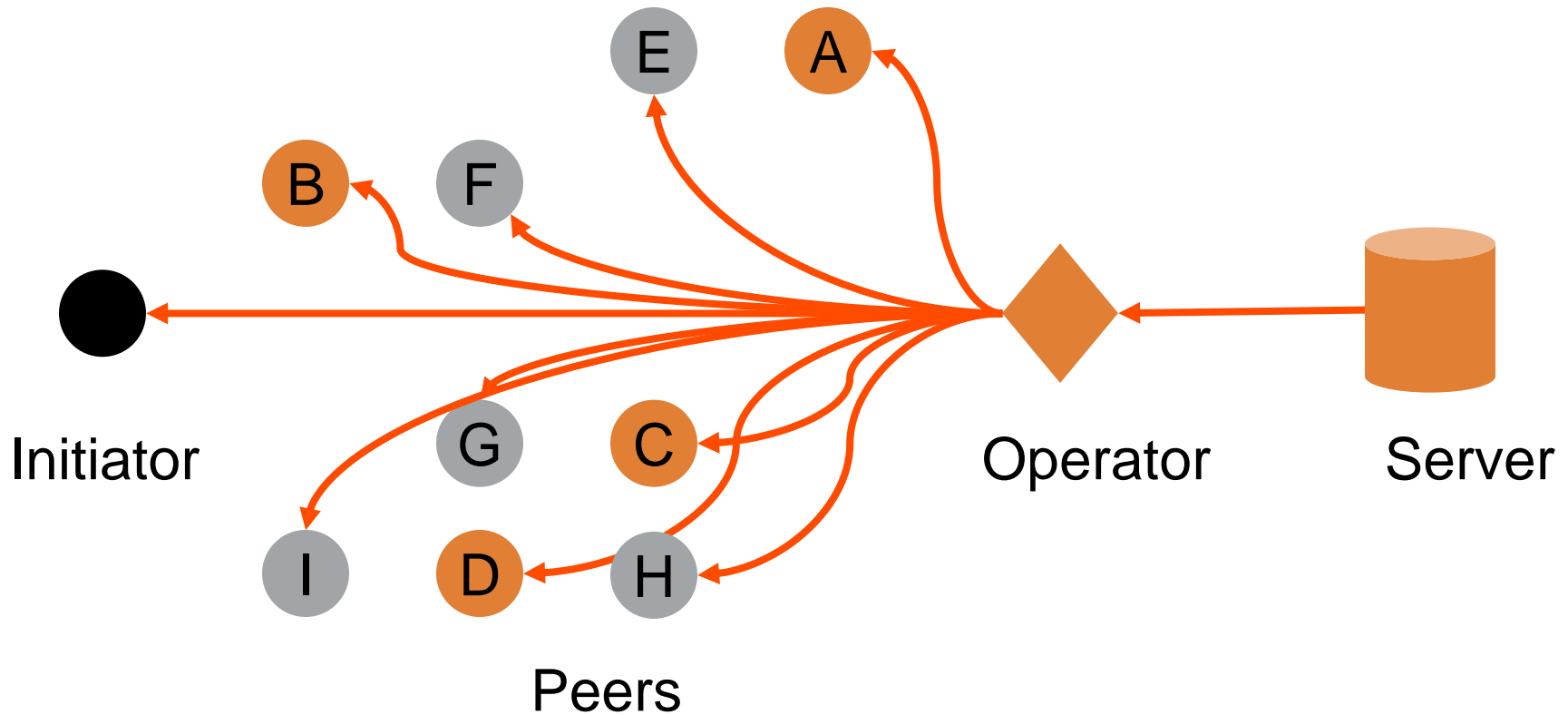
Connection Establishment Response



Service Access Request



Service Access Response



Potential Improvements

- 1) Position Attacks for Multiple Requests-Responses:** Since nodes are mobile and the network operator has access to every nodes' position, the operator can infer who the initiator is if he does not remain “near” a subset of the original peers for the entirety of the exchange.
- 2) New Server Protocol:** Requires servers to assemble full packets from k sub-packets. This is not currently part of the standard web protocol.

References

- 1) Ardagna, Claudio A., et al. "Providing users' anonymity in mobile hybrid networks." *ACM Transactions on Internet Technology (TOIT)* 12.3 (2013): 7.
- 2) Bamba, Bhuvan, et al. "Supporting anonymous location queries in mobile environments with privacygrid." Proceedings of the 17th international conference on World Wide Web. ACM, 2008.
- 3) Reiter, Michael K., and Aviel D. Rubin. "Crowds: Anonymity for web transactions." *ACM Transactions on Information and System Security (TISSEC)* 1.1 (1998): 66-92.
- 4) Chow, Chi-Yin, Mohamed F. Mokbel, and Xuan Liu. "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments." *GeoInformatica* 15.2 (2011): 351-380.