

# Tracing Anonymous, Peer-to-Peer VoIP Calls on the Internet

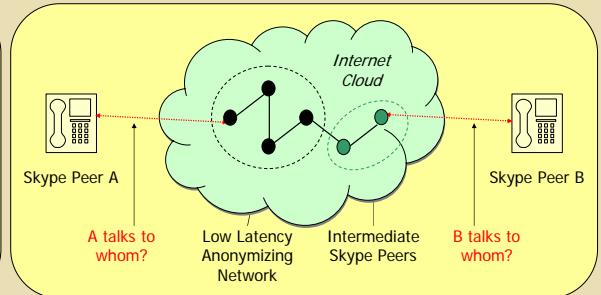


Xinyuan Wang, George Mason University, <http://ise.gmu.edu/~xwangc>

## Motivation

VoIP has made it much easier to achieve confidentiality and anonymity in voice communication

- Use end-to-end encryption
- Use peer-to-peer communication, rather than centralized service
- Use proprietary signaling protocol (e.g. Skype) that does not have phone number at all
- Route the VoIP traffic through low-latency anonymous communication systems



Traditional approach to track PSTN calls is based on the signaling protocol, and it can not track anonymous, peer-to-peer VoIP calls. Many people thought their VoIP call is anonymous when it is encrypted and routed through anonymous communication systems.

## Questions to be answered

- Does existing low-latency anonymous communication system really make VoIP flow anonymous?
- Is it possible to track such kind of anonymous and peer-to-peer VoIP calls on the Internet?

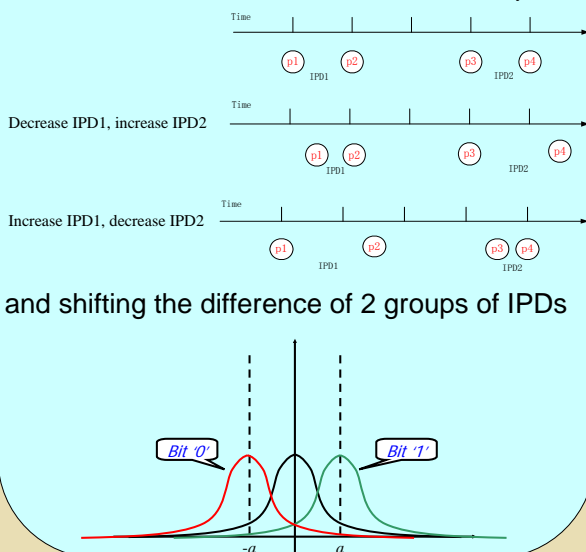
### Novel Ideas

- Track VoIP calls based on the VoIP flow itself rather than the signaling
- Deliberately (and yet subtly) make each VoIP flow unique by injecting unique call-identifying code or watermark into the packet timing domain

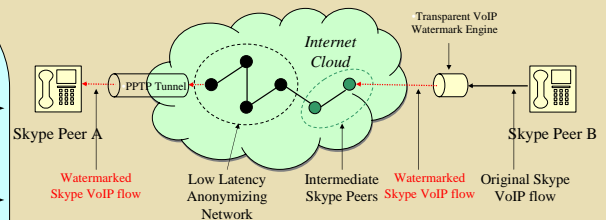
### Advantages

- Can be effective no matter what signaling protocol is used to setup the VoIP call
- Compatible with all existing and future VoIP protocols
- There is no bandwidth overhead

Embedding watermark bit by adjusting the IPD (the Inter-Packet Delay of  $P_i$  and  $P_j$ )



and shifting the difference of 2 groups of IPDs



### Our Findings:

- The use of strong end-to-end encryption and low-latency anonymizing network does not necessarily make peer-to-peer VoIP call anonymous
- Tracking encrypted peer-to-peer VoIP calls on the Internet is feasible even if they are anonymized by low-latency anonymizing network
- Existing low latency anonymizing service is vulnerable to timing attack