An analysis of anonymity and unlinkablility for a VoIP conversation

Ge Zhang
ge.zhang@kau.se
Karlstad University

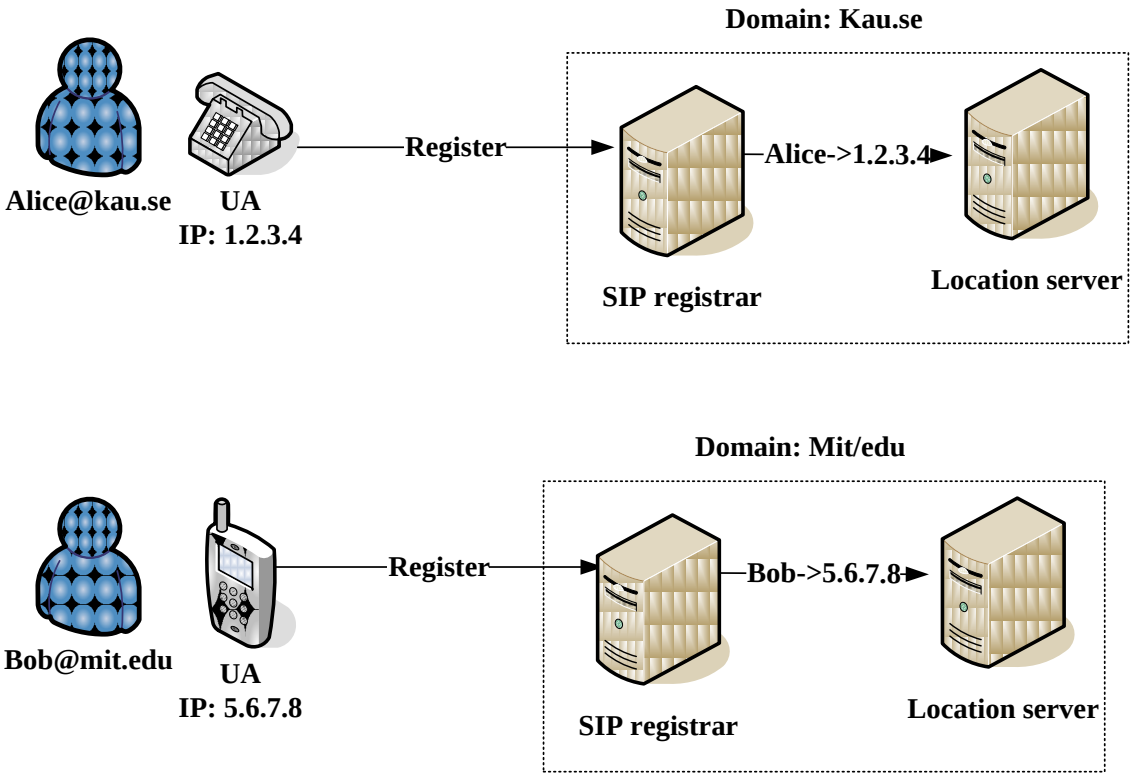
Outlines

- Background of VoIP
- Previous work
- Analysis of caller/callee anonymity
- Requirement on a VoIP Anonymization Service (VAS)
- Conclusions and future work

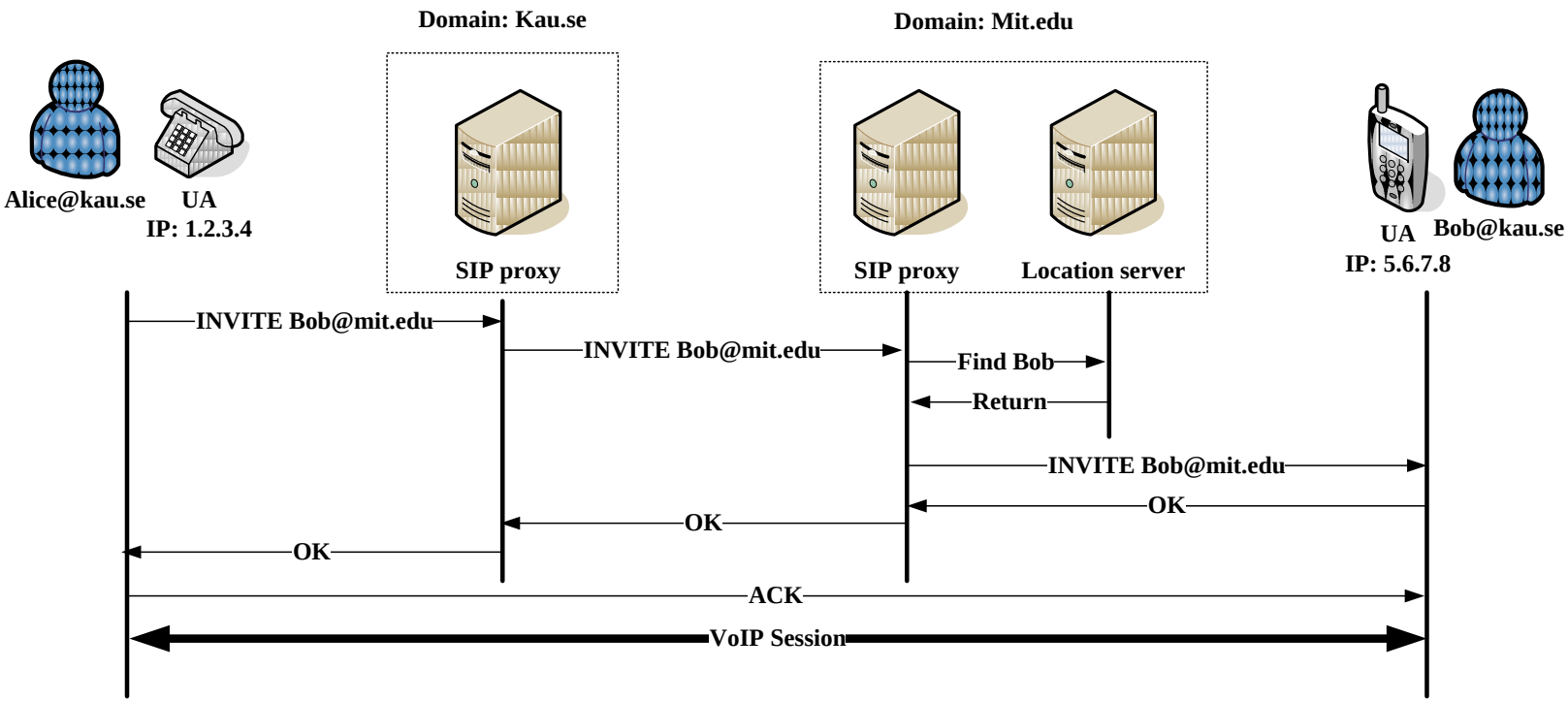
Backgournd of VoIP (1)

- VoIP procotcols, By IETF, Not SKYPE!
  - SIP: Session Initiation Protocol
  - SDP: Session Desicription protocol
  - RTP: Realtime Transport Protocol
- Pro and con of VoIP

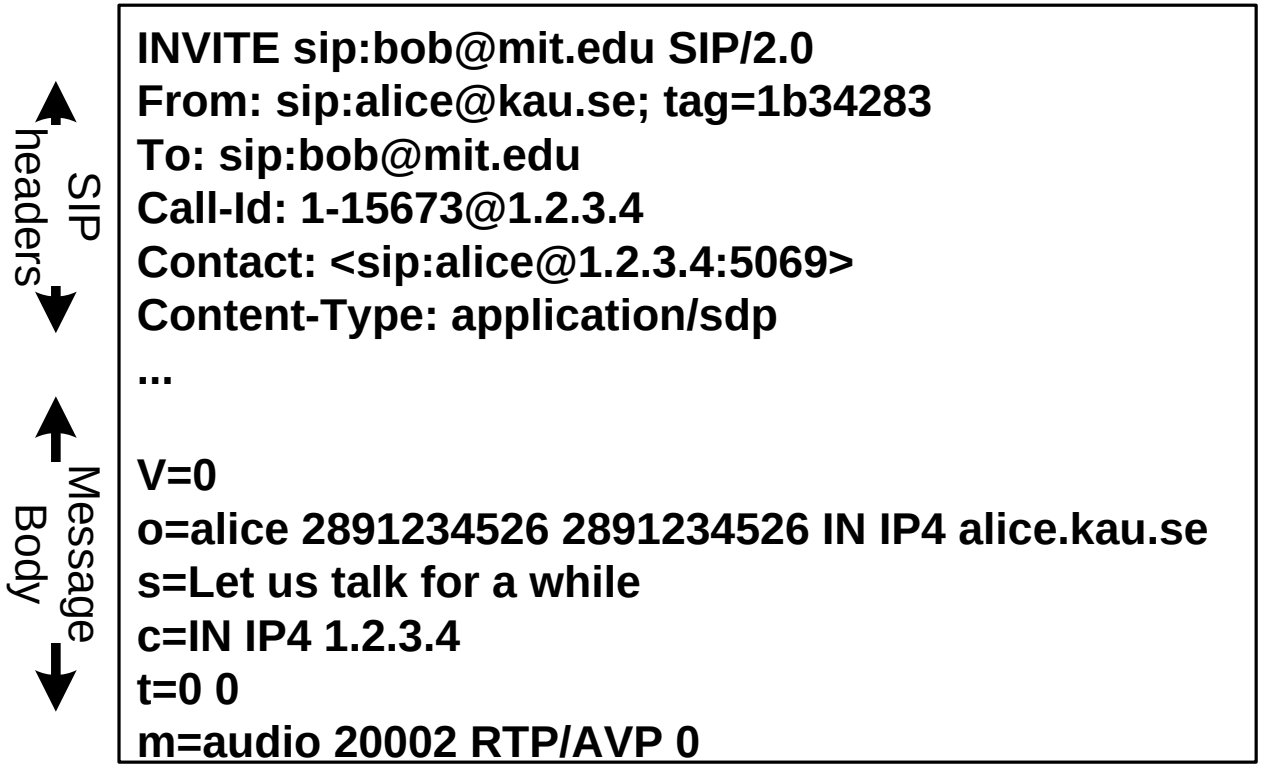
Backgournd of VoIP (2)



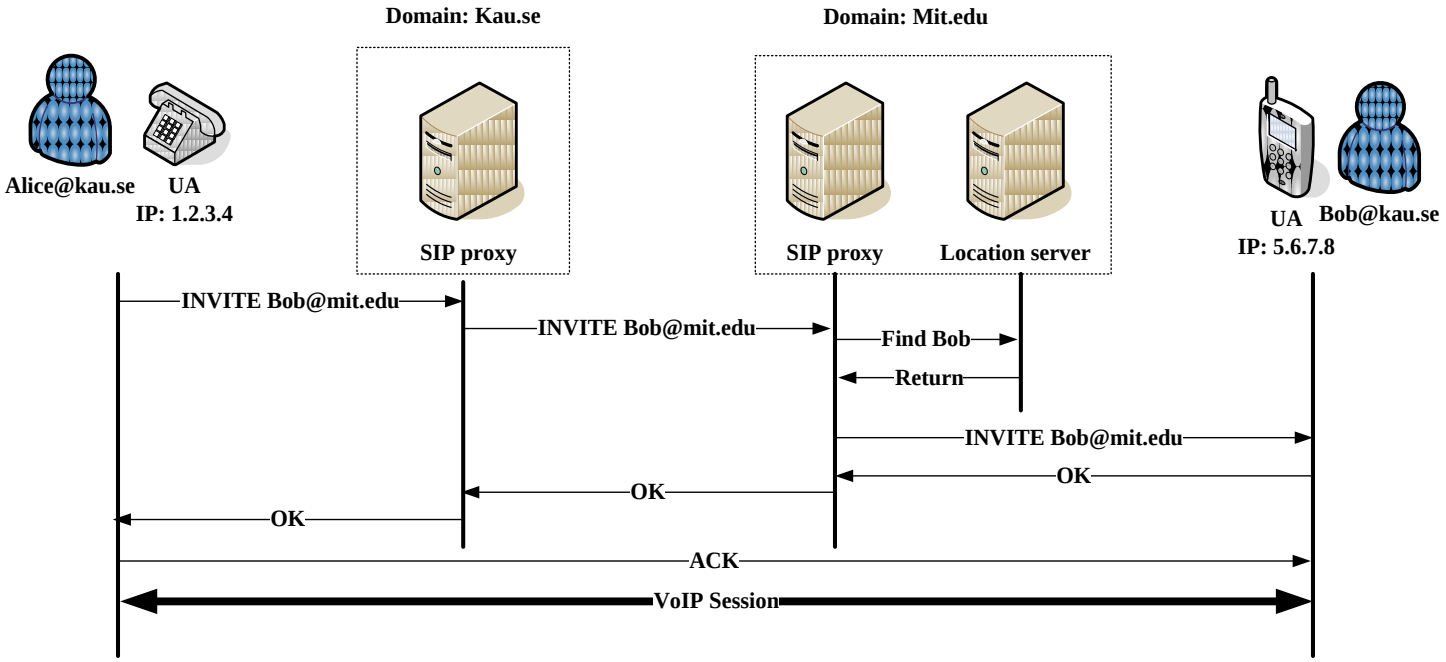
Backgournd of VoIP (3)



Backgournd of VoIP (4)



Backgournd of VoIP (3)



- Signaling level: the caller, the intermediaries, the callee
- Session level: the caller and the callee

Previous work (1)

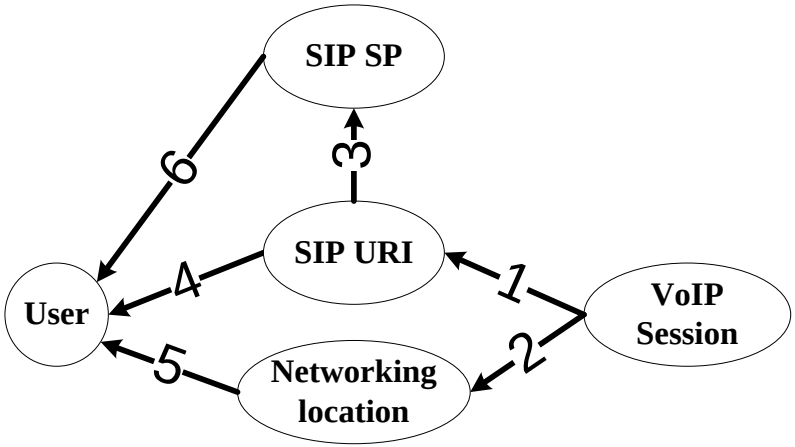
- J. Peterson, “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, RFC 3323, Nov, 2002.
- Caller anonymity (3 privacy preferences)
  - vs. callee
  - vs. intermediaries
  - vs. both of them
- 2 methods to reach privacy protection
  - User provided privacy (minimize PII in a SIP request)
  - Networking provided privacy (a TTP)

Previous work (1)

- The problem of RFC 3323
  - Have to trust a single TTP
  - There is no detailed privacy analysis.
  - Only caller anonymity, no callee anonymity

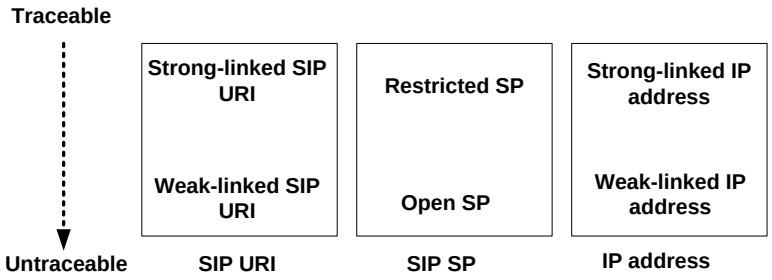
Analysis of caller/callee anonymity (1)

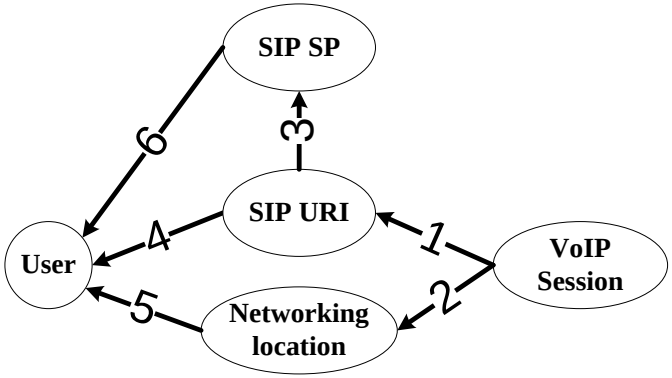
- Item of Interest (IOI)
- Attackers
- Links
  - 1,2,3: contain
  - 4:contain, calling records
  - 5: WHOIS lookup, IP-location database, transaction links.
  - 6: relationship



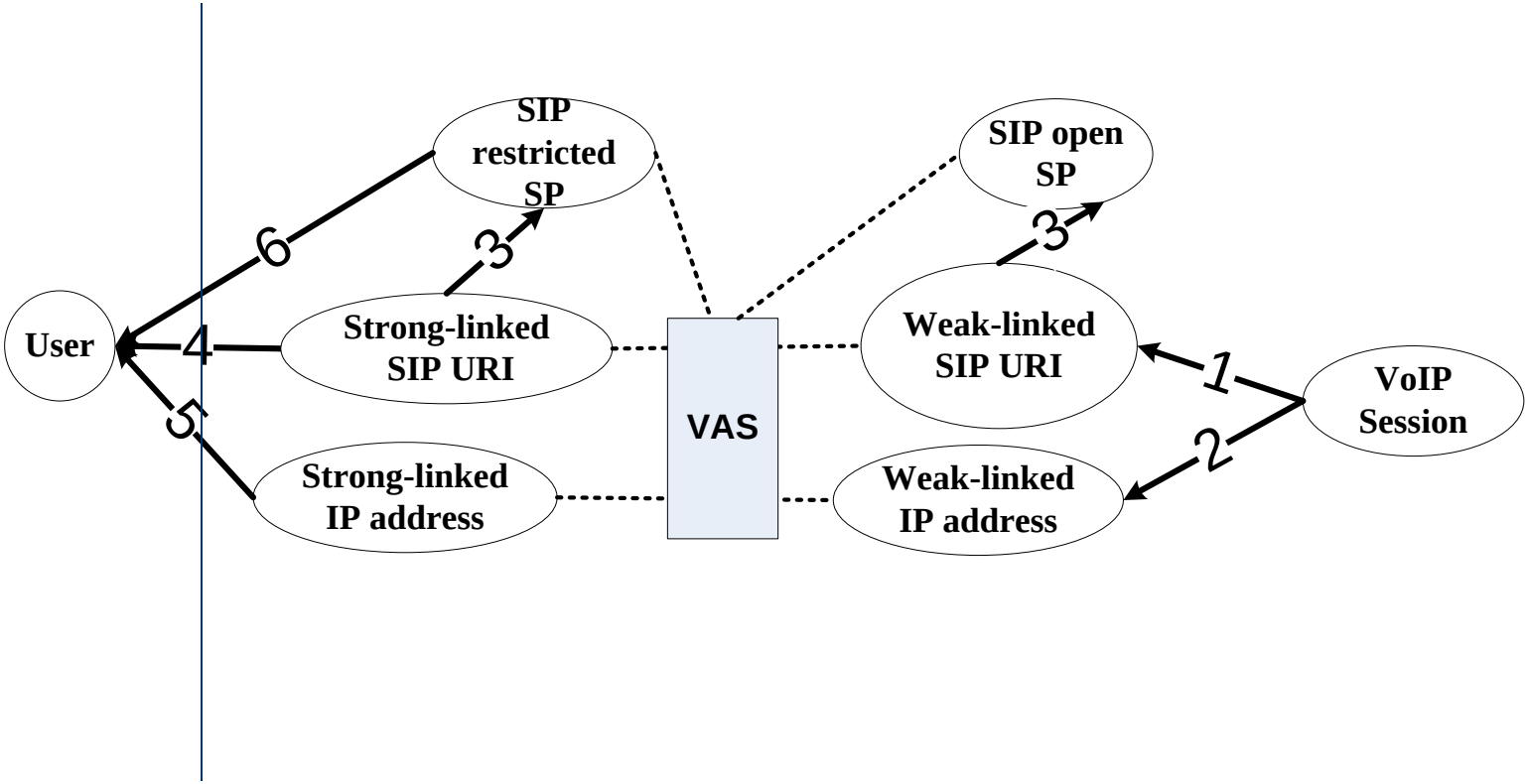
Analysis of caller/callee anonymity (2)

- To break links
  - 1, 2, 3: unlikely
  - 4: weak-linked SIP URI
  - 5: weak-linked IP address
  - 6: Open SP





Analysis of caller/callee anonymity (3)



Requirements on a VAS

- Basic requirements
  - Compliant to VoIP protocols
  - UDP support
  - No single TTP
- Requirements on performance
  - Network delay: <400ms.
- Requirements on usability
  - Predefined privacy settings
  - Less waiting time

Conclusion and future work

Conclusion

- Problems of previous mechanism
- An anlysis of VoIP anonymity
- Summarized further requirements for a VoIP anonymization service.

Future work

- Which topology should be employed?
  - Core-based? (like Tor, JAP)
  - P2P-based? (like Tazan, Crowds)
- Performance optimization: (1) a metrics to model performance and anonymity; (2) a heuristic algorithm to trade off performance and anonymity by nodes selection