

Providing Privacy in P2PSIP- based Communication Systems

-----Xianghan Zheng
Vladimir Oleshchuk

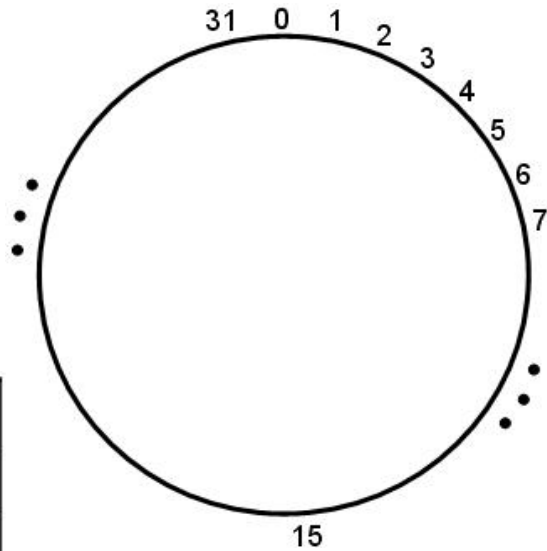
Introduction

- P2PSIP network and system is a future trend. P2PSIP peers in the overlay cooperate each other to locate the peer/resource.
- Cooperative character brings a few problems:
 - The peers might contact with the intermediate peers that is not trusted
 - Any peers can passively spy the P2PSIP messages and receive some private information, e.g. identifiers of the source, destination, and the previous intermediate peers, etc.

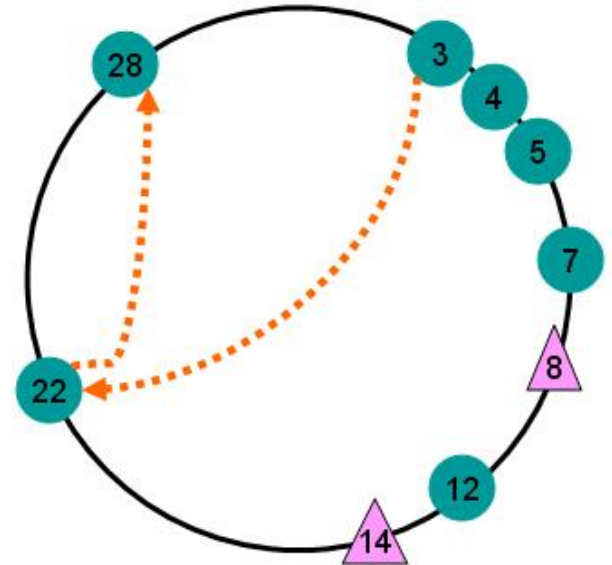
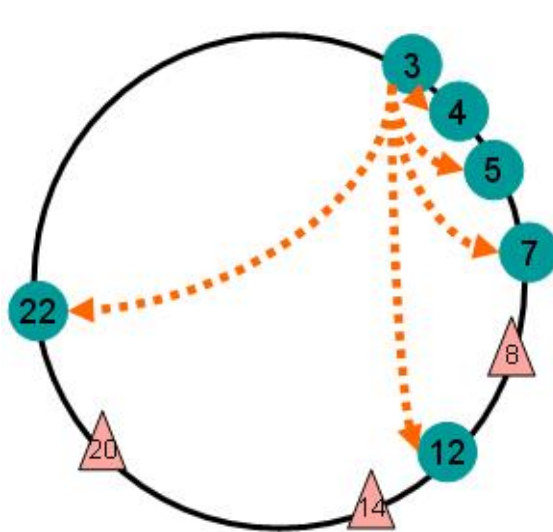
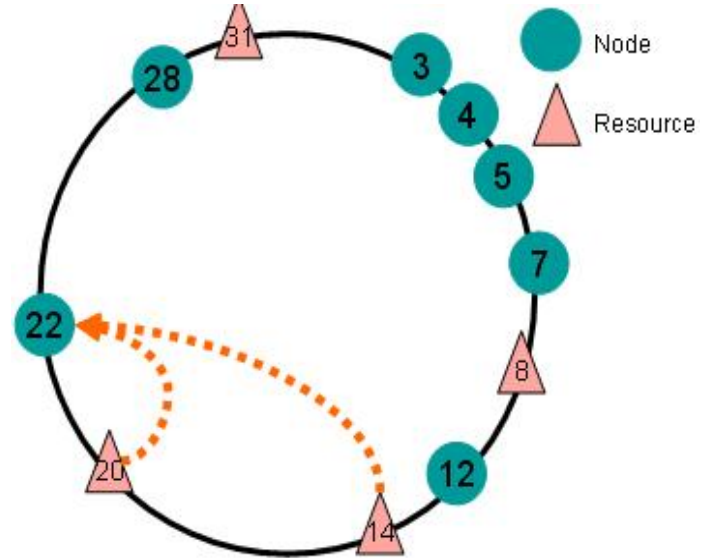
Peer-to-Peer SIP

- P2PSIP is a future trend that combines internet protocol with the telecommunication protocol.
- Three type of solutions:
 - **P2P over SIP**, uses SIP message to build and maintain the P2P overlay.
 - **SIP over P2P**, A separated P2P protocol is proposed to manage the network overlay activities.
 - **P2P and SIP**. Use link layer to maintain the overlay, while defines some SIP extension to enhance the session services

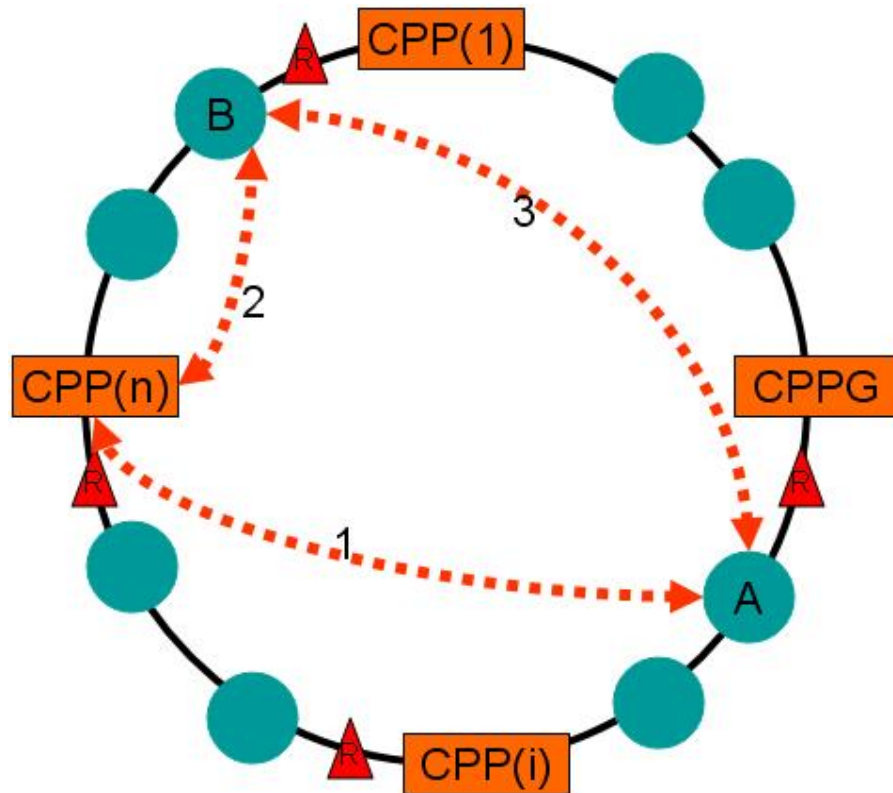
Chord



Index	Point Value	Node
f[0]	Points to $3+2^0=4$	4
f[1]	Points to $3+2^1=5$	5
f[2]	Points to $3+2^2=7$	7
f[3]	Points to $3+2^3=11$	12
f[4]	Points to $3+2^4=19$	22

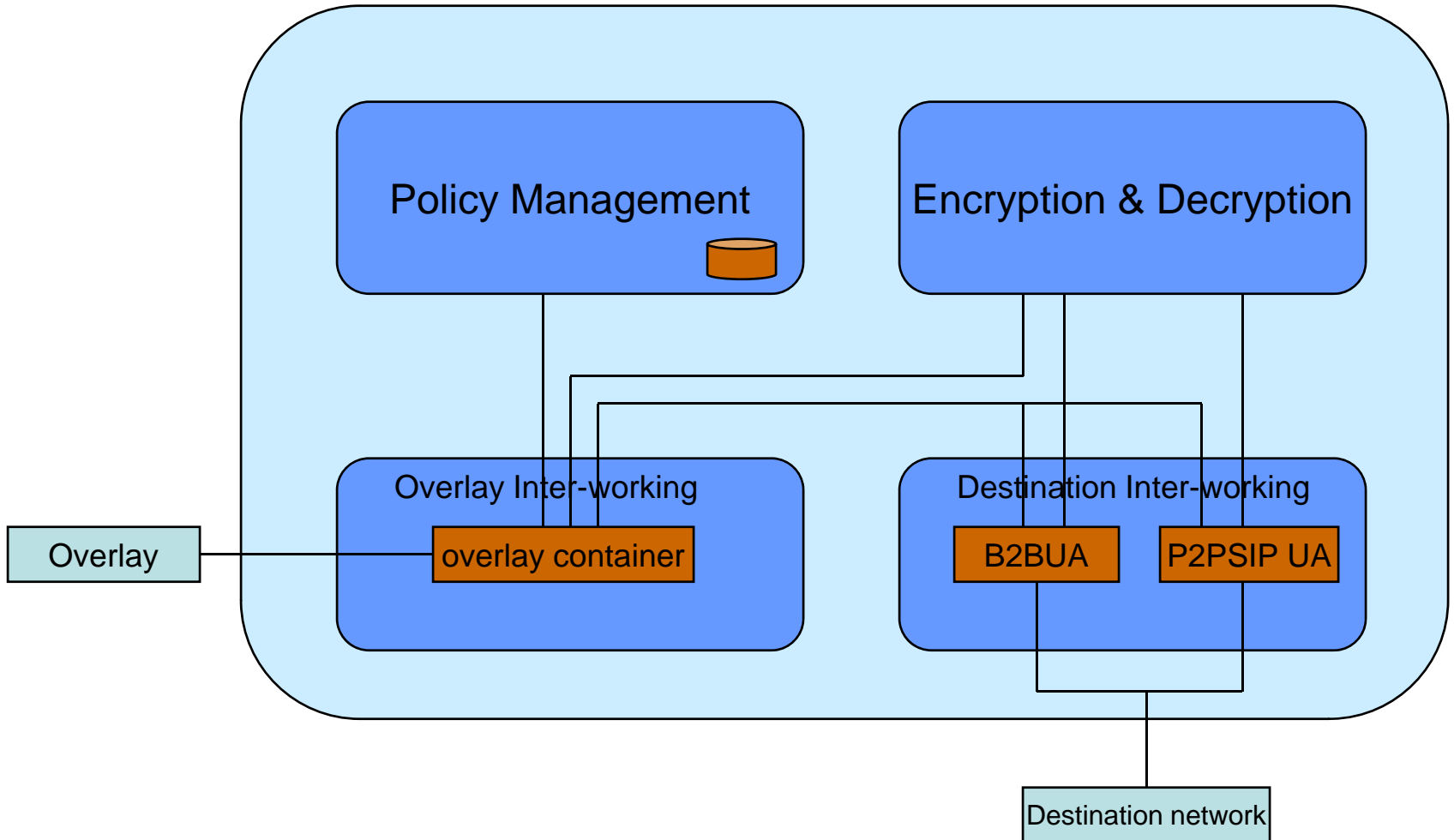


Privacy Service Architecture



- Chord Privacy Proxy (CPP) is the privacy service proxy that helps the source peer locate the destination peer.
- We logically defines source network (Step 1) and destination network (Step 2)

CPP Inside



Encryption & Decryption

- Provides the Encryption & Decryption mechanism for the Overlay Inter-working, Destination Inter-working components.

Overlay Inter-working

- Receive the P2PSIP request messages:
e.g. INVITE, MESSAGE, etc
- Forwards the P2PSIP response message
back to the source peers

Policy Management

---Privacy-hdr = "Privacy" HCOLON priv-value *(";" priv-value)

---Priv-value = "none" / "critical" / "anonymity"

- E.g. A privacy header:

--- Privacy: none/critical/proxy.....

none: The user requests that a privacy service apply no privacy functions to this message, regardless of any pre-provisioned profile for the user or default behavior of the service. User agents can specify this option when they are forced to route a message through a privacy service which will, if no Privacy header is present, apply some privacy functions which the user does not desire for this message. Intermediaries MUST NOT remove or alter a Privacy header whose priv-value is 'none'. User agents MUST NOT populate any other priv-values (including 'critical') in a Privacy header that contains a value of 'none'.

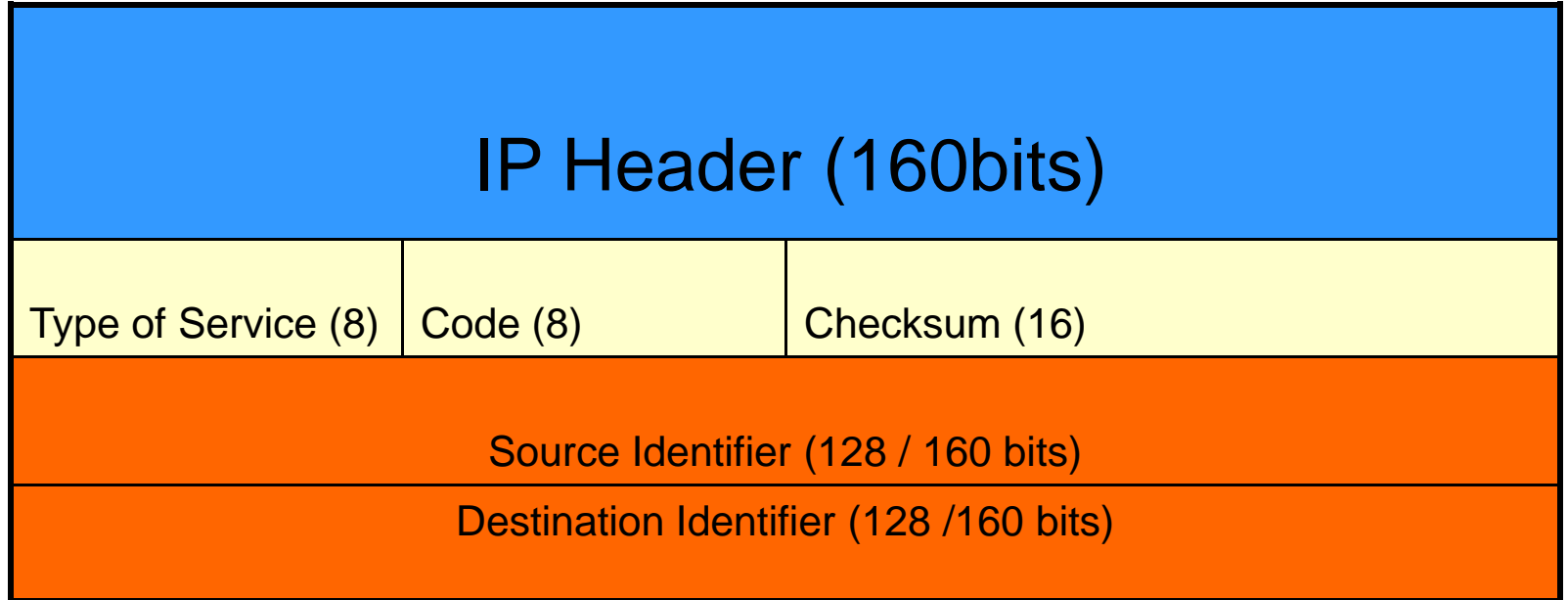
critical: The user asserts that the privacy services requested for this message are critical, and that therefore, if these privacy services cannot be provided by the network, this request should be rejected. Criticality cannot be managed appropriately for responses.

anonymity value requests that the CPP should hide all the source privacy information to any other peers, including the destination peer. The request should be rejected if the privacy service can not be supported.

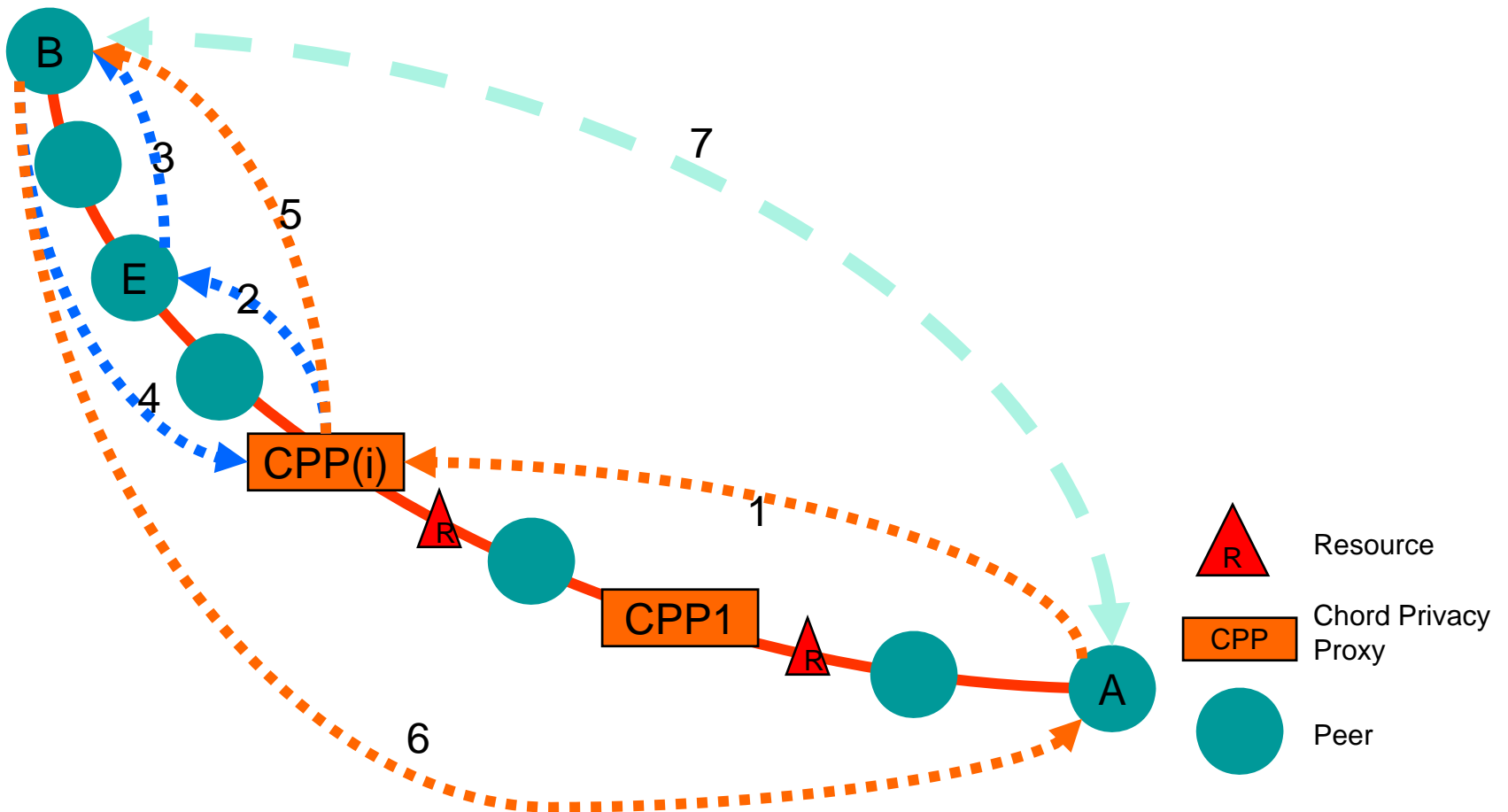
Destination inter-working

- Back-to-Back User Agent (B2BUA)
 - sends a Hello request message to the Destination
 - receives the Destination response
 - forwards the real P2PSIP request msg
- P2PSIP UA
 - forwards the P2PSIP ping msg

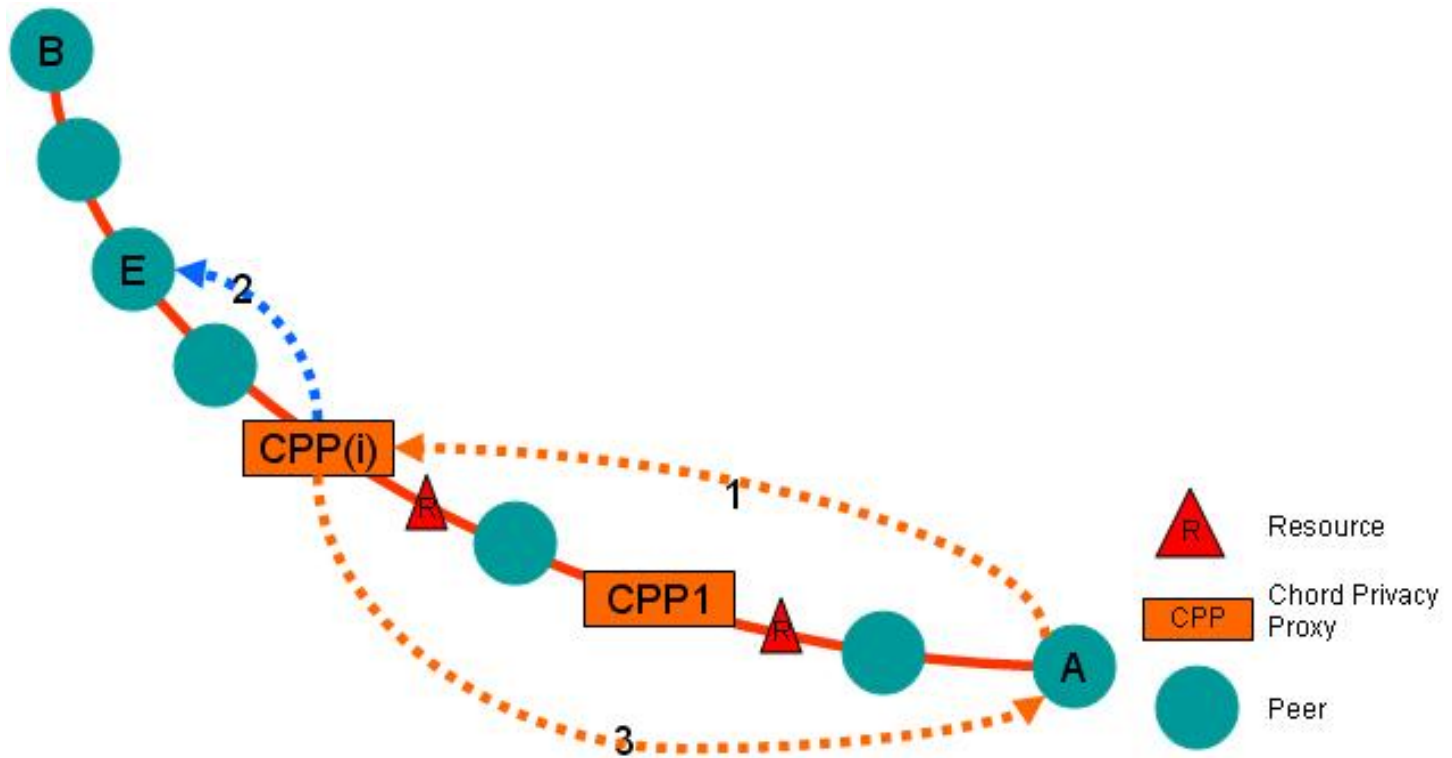
P2PSIP Ping Message



Use Scenario



Error Use Scenario



Security & Privacy evaluation

- This CPP architect can provide good privacy mechanism, reduce the security problem, but not eliminate.
- The intermediate peer in the destination network can receive the Hello message, However, it does not get any privacy information of the source.
- The more CPPs, the better security

Num-of-the hops, Message flows

Table 2
Number-of the hop comparison

	Chord overlay	CPP system
Number of Hop (at most)	$\text{Log}(N)$	$1 + \text{Log}(N/R)$
Num of hop (in average)	$\log(N)/2$	$1 + \log(N/R)/2$

Table 3
Number-of the message comparison

	Iterative	Semi-Recursive
Num-of-Message (at most)	$1 + 2\text{Log}(N/R)$	$4 + \text{Log}(N/R)$
Num-of-Message (In average)	$1 + \log(N/R)$	$4 + \text{Log}(N/R)/2$

Conclusion and Open Issues

- This architect protect the privacy information of the source peer, but not the Destination peer. (a malicious peer can collect the destination peers information)
- No easy to implement this architecture.
- The enryption & decryption might cause more delay.
- The Chord lookup algorithm should be further improved.