draft-petithuguenin-p2psip-reload-anonymous

Marc Petit-Huguenin
2012/11/06

Motivation

- (IPR disclosed for this draft)
- A privacy issue was found during the work on VIPR. VIPR uses a unique RELOAD overlay to store mapping between phone numbers and indirect IP addresses.
- A sketch of this solution was presented in Paris.

Goals

- Permits a node to anonymously store data.
- Permits end to end anonymous and confidential exchanges.
- Can be deployed on existing overlays
- Reuse existing technology

Traceable Anonymous Certificate

- First step is to separate the certificate used for routing messages from the certificate used to sign StoreReq message and content.
- Traceable Anonymous Certificate (RFC 5636) is used only for anonymous request and data signing.
- The standard certificate is used for routing.
- This requires a way to tunnel the StoreReq.

Onion-ID

- An Onion-ID is a new type of ID, recognized only by Onion Nodes. It contains:

  1. The index of a session key negotiated between an anonymous Node and an Onion Node.

  2. A Destination list encrypted with that key.

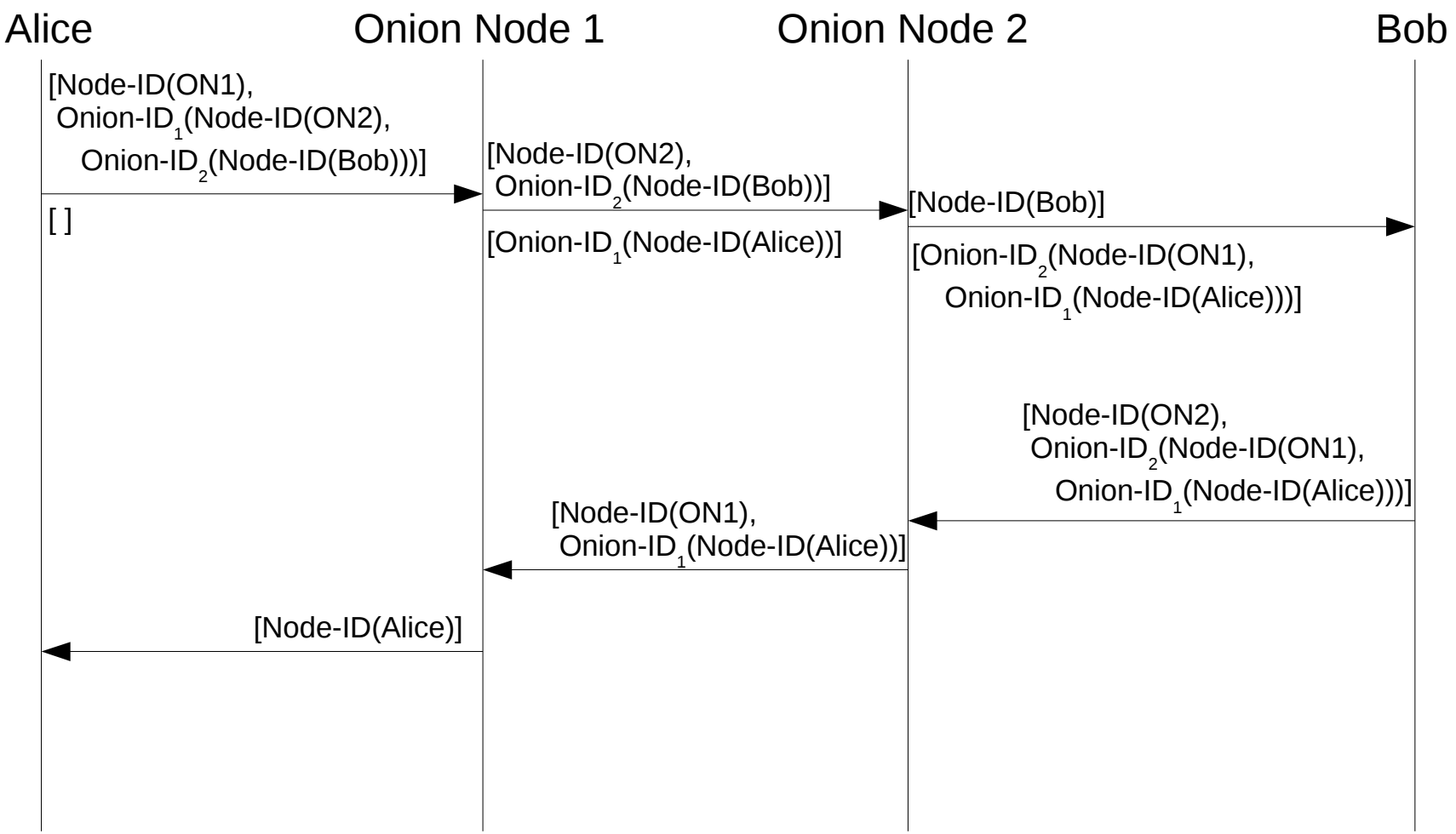
- An Onion-ID can itself contain Onion-IDs.

Onion Routing

- An Onion Node receiving a message with an Onion-ID on top of the destination_list (after removing its own Node-ID) will decrypt it using the index and route the message with the new destination_list but without end to end retransmission.

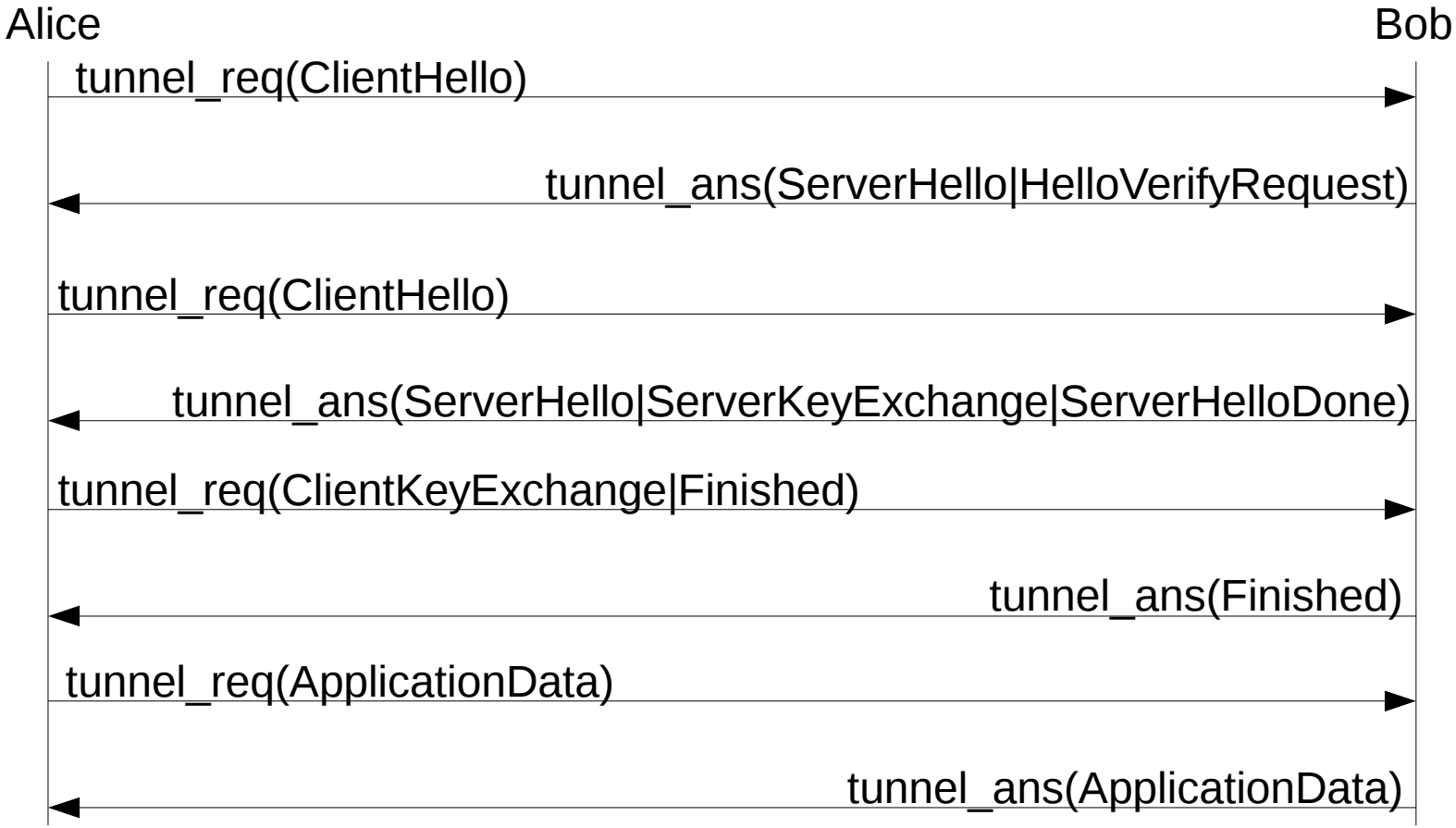
- Only for request, after adding the previous Node-ID, the via_list is encrypted with the same key and encapsulated in an Onion-ID, which replace the via_list.

Onion Routing Example



End to end encryption

Defines a new RELOAD transaction called Tunnel, which carries DTLS (RFC 6347) messages.

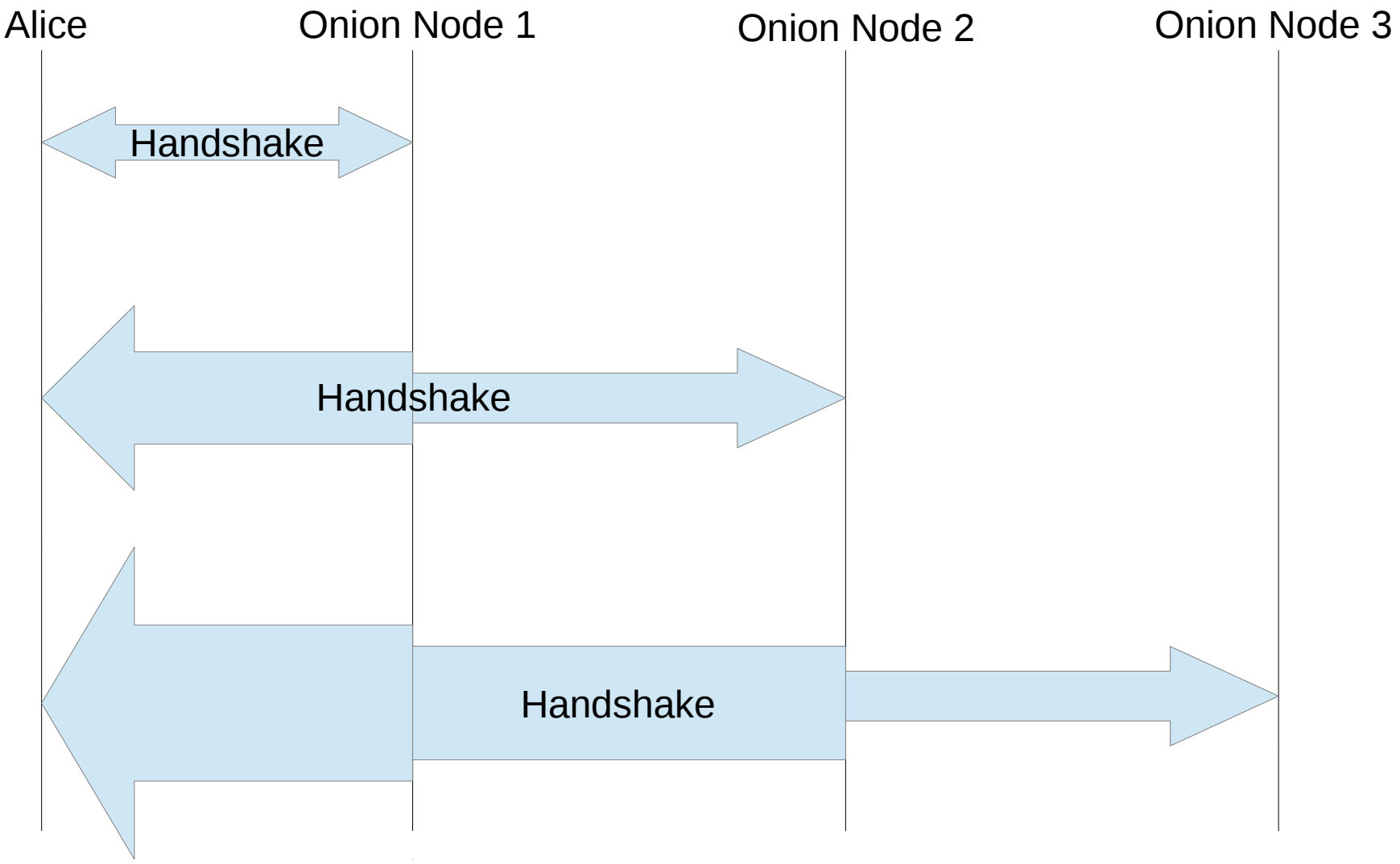


Building the telescopic path

- Asking each Onion Node to create sessions key does not work because the exit node would know the identity of the anonymous node.

- So instead we use the onion routing capability to request a session key through the previous Onion Node, creating what is called a telescoping path in TOR

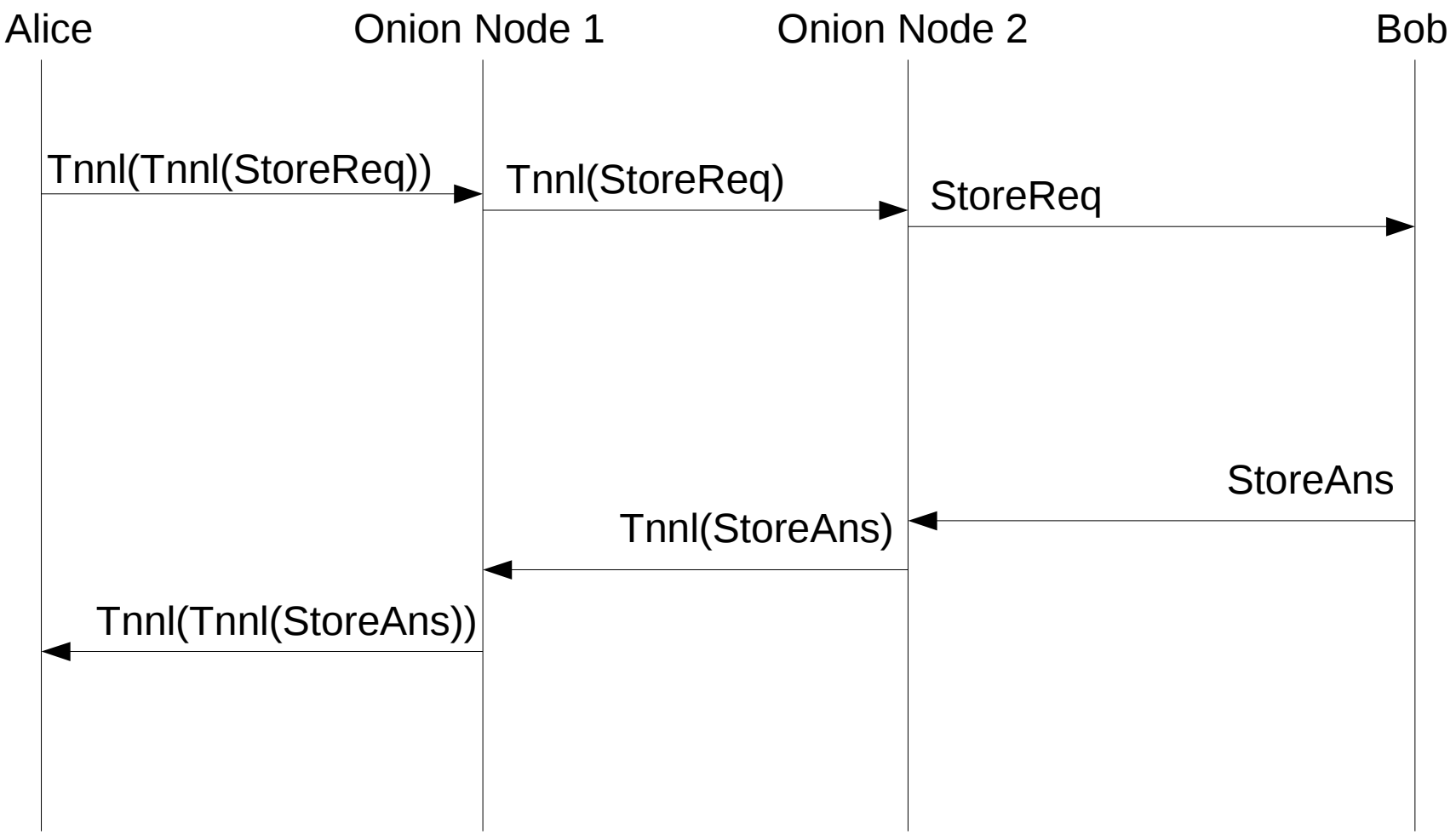
Telescoping Path Example



Onion Routing Rules for Messages

- If the Tunnel message contains an ApplicationData message and if the signer of a Tunnel message matches the index, then the content is decrypted and replaces the Tunnel message. If the decrypted message is Tunnel, the message is signed by the node, else the Header and SecurityBlock are also decrypted.
- Else the message is encrypted, encapsulated in a Tunnel message and replaces the message. If the encrypted message is not Tunnel, then the Header and SecurityBlock are encrypted. The message is signed by the node.

Anonymous Sending Example

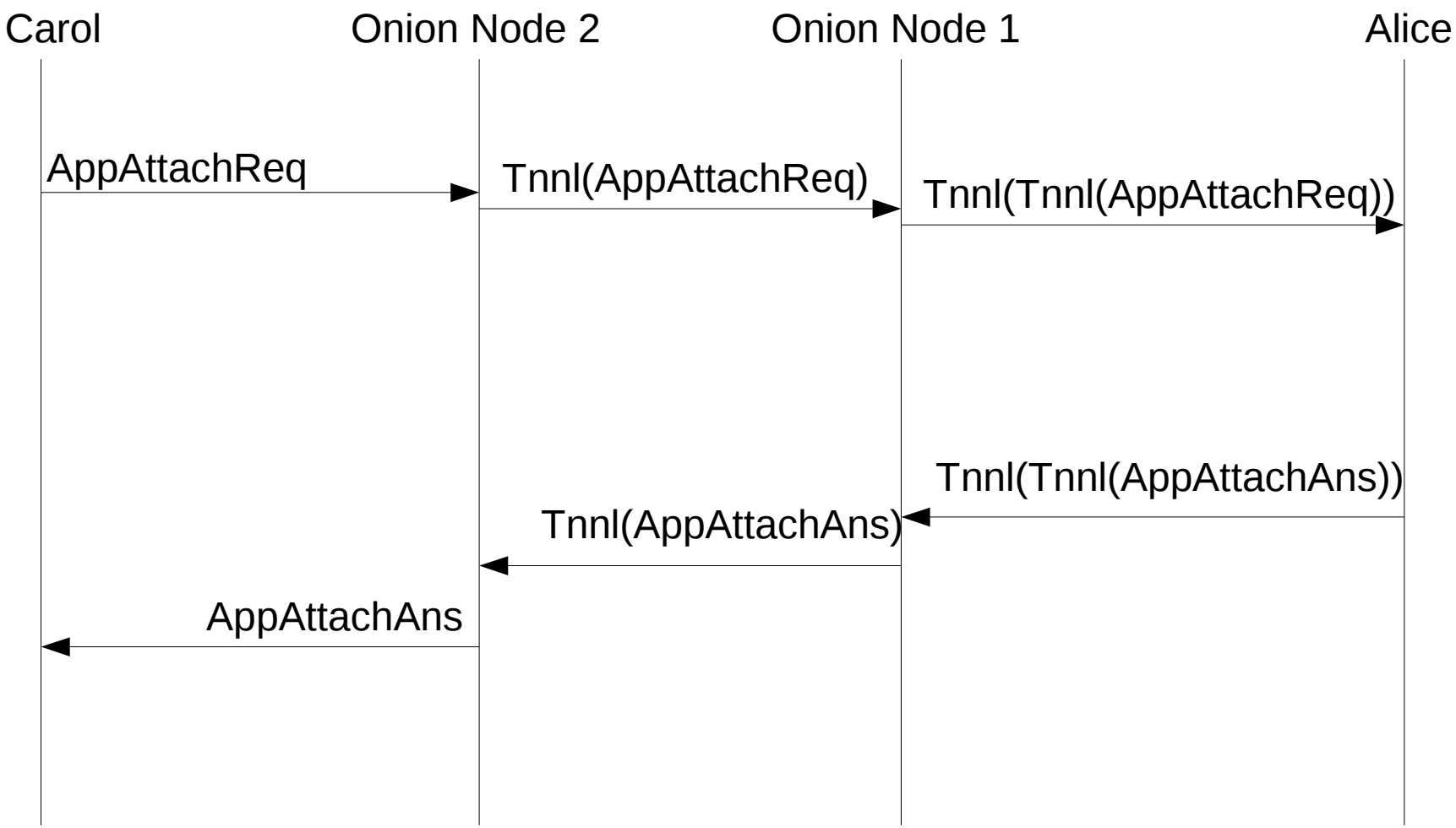


Anonymous Receiving

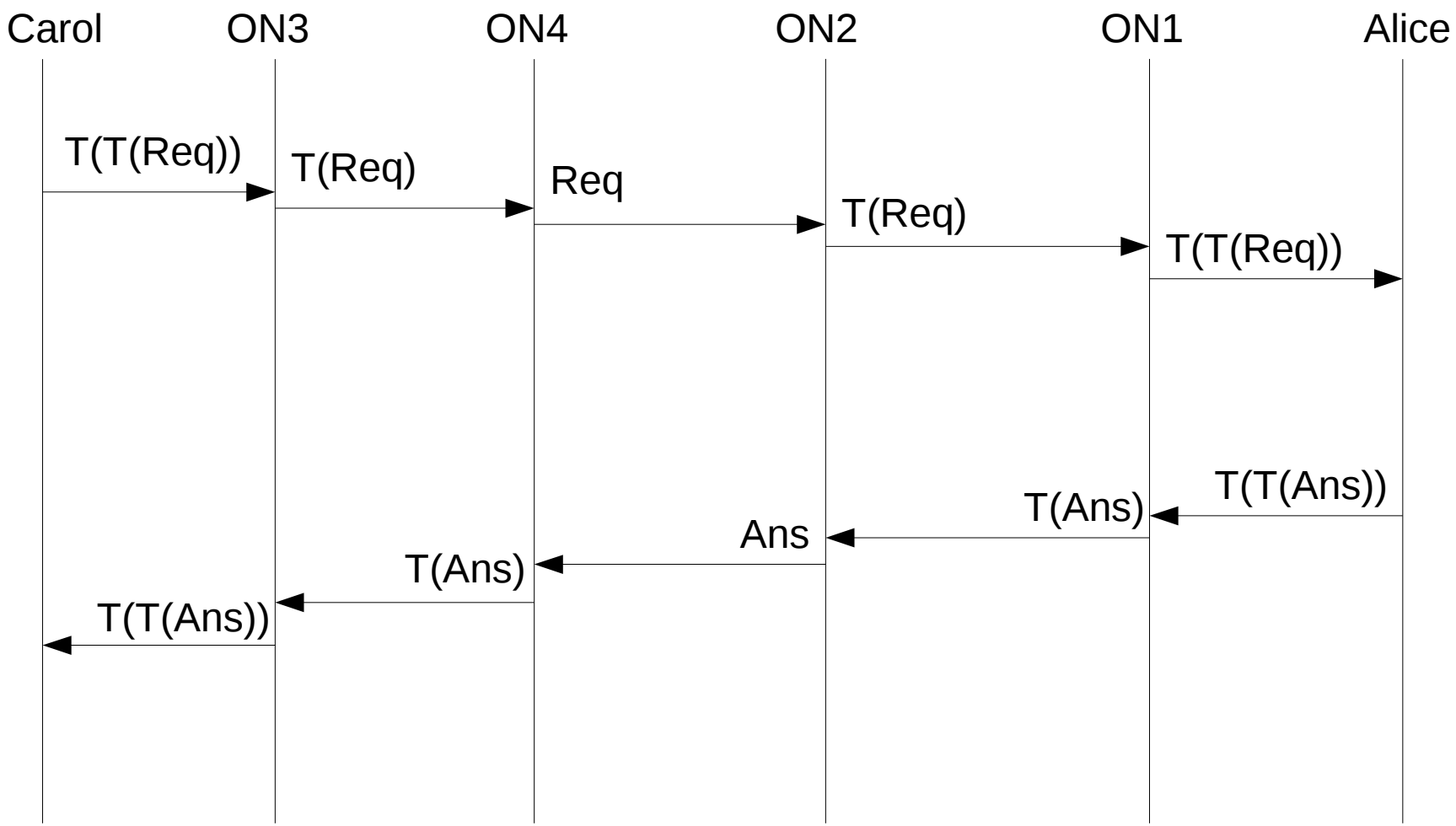
- The same mechanism can be used to store an anonymous Destination list in the overlay.

- This is the reason why a Destination list is better than a simple Node-ID in StoredData (also because of RELOAD clients)

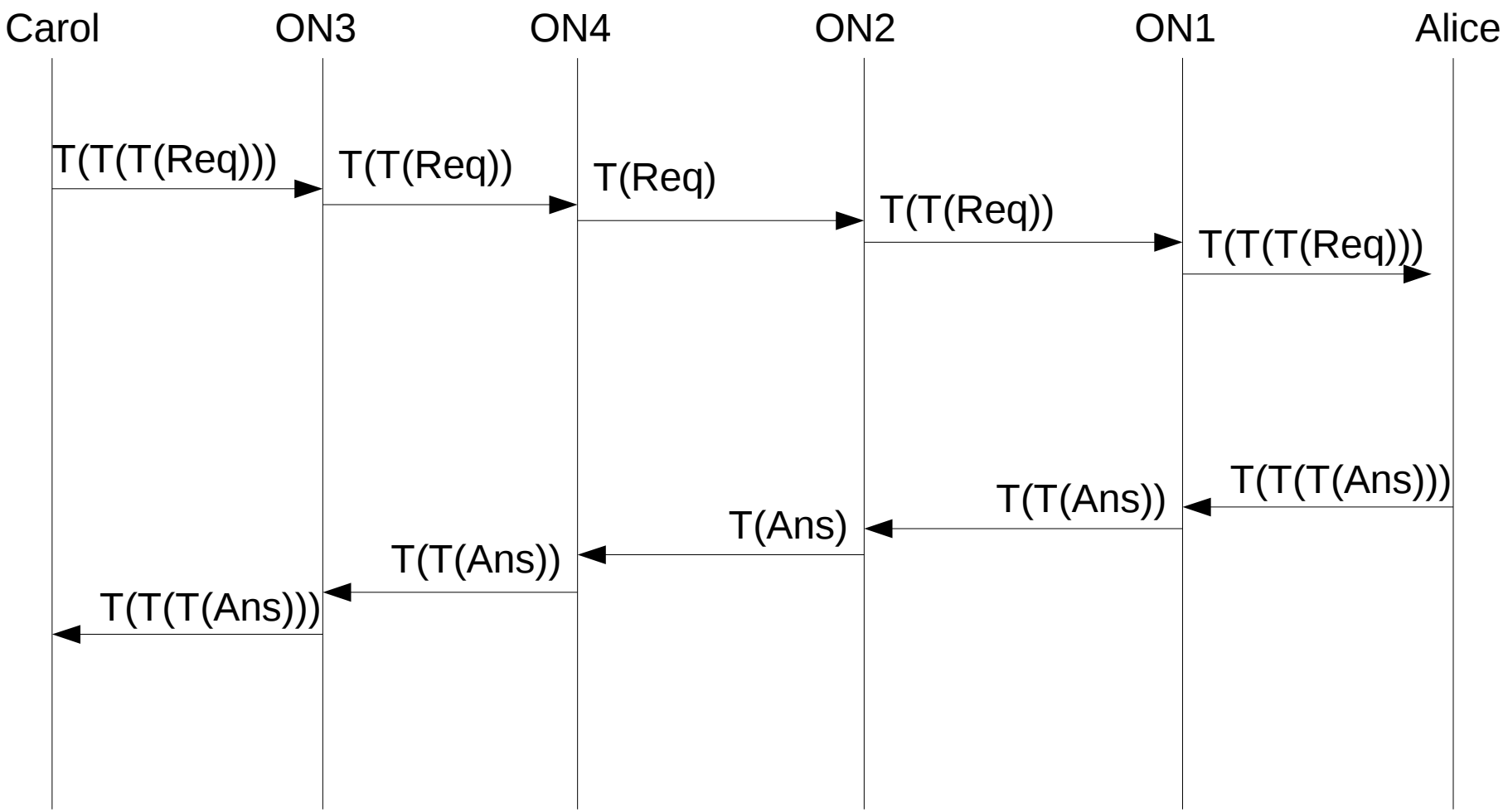
Anonymous Receiving Example



Both Sides Anonymous Example



Anonymous and End to End Encrypted Example



Conclusion

- Permits a node to anonymously store data.
  Node use telescopic path to store data signed with TAC.
- Permits end to end anonymous and confidential exchanges.
  Telescopic path on both sides + end to end encryption.
- Can be deployed on existing overlays
  Only anonymous nodes and onion nodes needs to implement this. Onion nodes can be found using REDIR.
- Reuse existing technology
  Use of RELOAD and DTLS.

2nd RELOAD Interoperability Testing Event

- July 27 & 28 in Berlin, Germany - just before IETF 87th.

  9 months from now, so still time to start working on implementation.

  Registration details will be announced after IETF 86.

- RELOAD implementers mailing-list: http://implementers.org/mailman/listinfo/reload

- Configuration & Enrollment service available for free for RELOAD implementers.