Anonymous DTN Routing

Goal

1. Sender/receiver anonymity and unlinkability
2. Reasonable efficiency (delay, bandwidth)
   1. Compare to underlying existing routing protocol
   2. Compare to other anonymous routing protocol (ARDEN, TOR), if possible

Assumption

1. Target DTN model: Special node (such as gateway) is not necessary.
2. Each node has different set of trusted nodes and knows IDs of trusted nodes
3. Loose time sync between nodes

Problems to solve

1. Ephemeral address generation/dissemination method
2. Epoch sync between trusted nodes
3. Anonymous routing using ephemeral address

Applying EbN to DTN

1. In DTN, two untrusted nodes need to communicate. Therefore, paring using beacon in EbN is not necessary.
2. We may generate ephemeral ID using a function similar to GenHSBeacon() in EbN.  
   However, if node A wants to generate a current ephemeral address of a trusted node B, node A should know a set of trusted IDs of the node B. -> not scalable
3. We can include bloom filter encoding of a trusted node IDs in each bundle so that relaying node can recognize trusted nodes of the owner of the bundle.

Ephemeral address generation/dissemination method

1. Each node generates its own ephemeral address using a hash function

ephemeral\_address <- GenEphemeralID(epoch\_counter, private\_seed)

1. A node generates bundles containing Bloom Filter encoding of IDs of trusted nodes.
2. If two nodes A and B encounter, each can determine if the opponent is a trusted node or not.
   1. If node A trusts node B,
      1. Node A shares <epoch\_counter, remaining\_time, private\_seed> with B
      2. Any node that has above parameters (B in this case) can generate current ephemeral ID of a trusted node (A in this case) using a function GenEphemeralID()  
         Problem: Epoch sync between nodes.
3. Two nodes A and B encounter and they have bundles to relay or to send out
   1. Node A determines if the opponent node B should be trusted for each bundle, based on bloom filter encoding of IDs contained in bundles.
      1. If B is trusted node of the owner of the bundle, A share <epoch\_counter, remaining\_time, private\_seed> of the owner of the bundle (only if the parameter set of A is newer than that of B)  
         Problem: How to determine which parameter set is more precise?
   2. Node A sends the bundle to node B, according to our anonymous routing policy (which is not yet ready).