ARDEN

Attack model

1. Passive global eavesdropper
2. Active attacker can compromise a subset of nodes

Design goal

1. Sender/receiver Anonymity  
   Strong sender anonymity: even receiver doesn’t know the origin of the message
2. Unlinkability  
   The inability for adversary to determine that messages are being exchanged between two specific nodes
3. Latency  
   No additional delay as in Mix-net.
4. Redundancy  
   Balance between redundancy and anonymity through the use of multicast communication

Assumption

1. A node can obtain the IDs of a large proportion of nodes in the DTN from ABE admin or other nodes.
2. A node doesn’t need to have exact topological knowledge

ARDEN design

1. ARDEN relies on the underlying DTN routing protocol to deliver anonymous bundles.
2. Only the intended destination can remove the final layer of encryption
3. The intended receiver is not necessarily the final hop in the path
4. Trade off communication efficiency (latency, delivery rate) for communication anonymity
5. Trade off bandwidth (multicast) for latency (more chance to find out short path)

Group Partitioning and management

1. Attribute-Based Encryption
2. Attribute: Binary representation of Node ID
3. Access Structure: Logical AND of multiple attributes

Protocol

1. Notation
   1. APK (ABE public key): given to all nodes, AMK (ABE Master key): keep by ABE admin , ASK (ABE user secret key): given to each node , A (Access structure)
   2. AEncrypt(m, APK, A)
   3. ADecrypt(c, APK, ASK)
2. Network initialization
3. Defining groups
   1. ABE: attribute is a binary representation of node ID.
   2. All nodes are leaves of a binary tree whose positions are determined by shuffled node ID. Here “shuffle” seems to be static.
   3. Sender partitions groups based on the common prefixes of shuffled node IDs.  
      Therefore, nodes within a group share the common attributes.
   4. Connectivity between two sequent groups is not considered. May result in longer latency. Multicast and large group size would bring good connectivity between groups
4. Constructing bundles
5. Routing
   1. Relies on existing routing protocols
      1. Earliest delivery, single path routing
      2. Epidemic minimum estimated expected delay, replicative routing
   2. The paper says that every relay hop may consists of several intermediate nodes, as in Figure 2.   
      How? Who’s the destination of the bundle in this case?