ARDEN

7/15/2013

Goals

- Sender anonymity
  - Strong sender anonymity: even receiver doesn’t know the origin of the message (reply path is given by sender)
- Receiver anonymity
- Unlinkability
- Low latency
  - Lower than traditional onion routing

- **Location anonymity is not a goal of ARDEN**

Attack model

- Passive global eavesdropper
- Active attacker can compromise a subset of nodes
  - Compromising nodes within every group along the routing path will reveal a the source, not the destination

Assumption

- Sender knows IDs of a large proportion of nodes in the DTN
  - From ABE(Attribute-Based Encryption) administrator or from other nodes
- Topological knowledge is not assumed.

ARDEN Design

- Base: Onion routing
  - Single path with specific onion proxy nodes
  - Traditional Onion routing doesn’t fit for disconnected environment

- Modification to Onion routing
  - Single-node proxy is replaced with a group of nodes
  - Multicast from a group to next group
    - Better successful delivery rate from sender to destination
    - Better chance to find a shorter route

Group partitioning/management through ABE

- Basics
  - Attribute: Binary representation of node ID
  - Access structure: Logical AND of attributes of nodes in a group
    - Access structures of groups on the path are included in bundles to indicate next group
  - ABE(Attribute-Based Encryption)
    - Sender encrypts each layer of a packet using APK (ABE public key) and an access structure of a group of nodes
    - Each layer of an encrypted packet can only be decrypted by nodes of the designated group

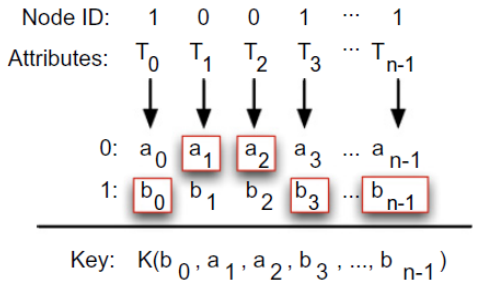
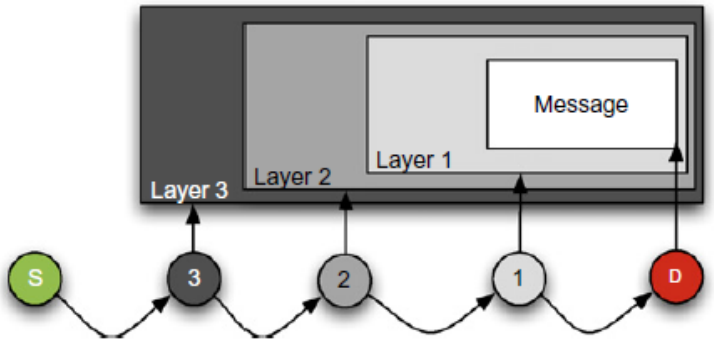


Fig. 3. The mapping between node ID, attributes and ABE user secret key.



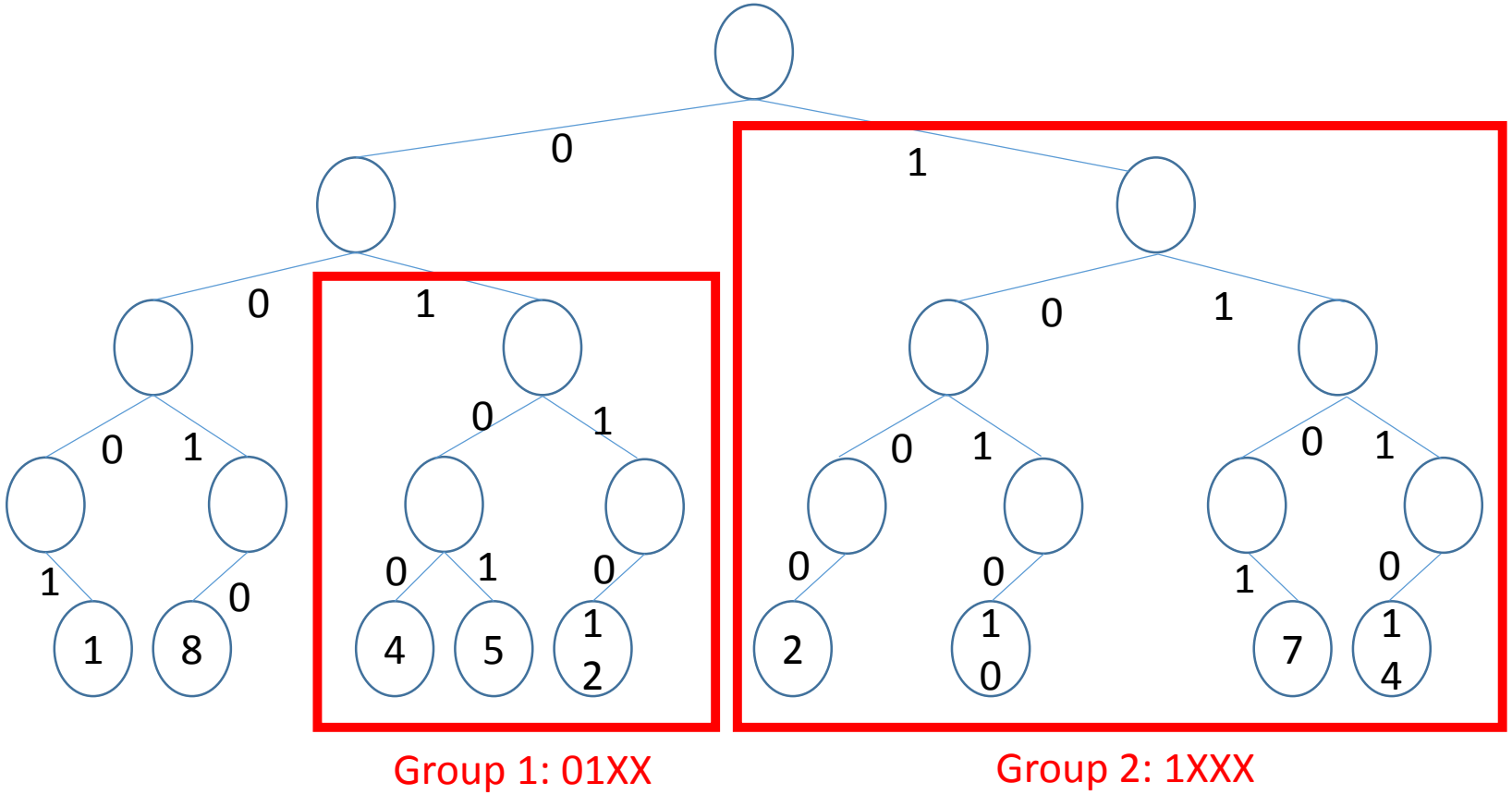
Group partitioning/management through ABE

- Partitioning
  - Sender builds a binary tree where all nodes are leaves of the tree
    - Position of a node is determined by shuffled node ID.
  - Sender partitions groups based on the common prefix of shuffled node IDs
  - (Example on the next slide)
- Connectivity between two consequent groups is not considered.
- Destination node may not be in the last group on the route.

Group partitioning/management through ABE

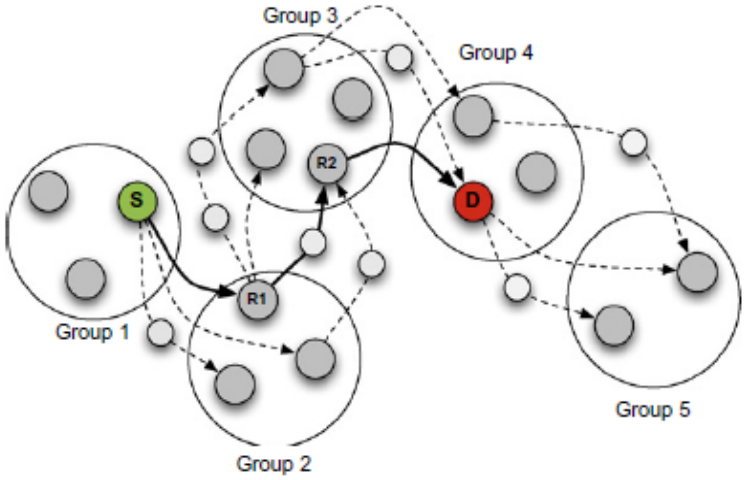
- Shuffle function: Switch first bit and third bit of node ID
- Group size: 3

Node ID	Node ID (Bit string)	Shuffled Node ID (Bit string)
1	0001	0001
2	0010	1000
4	0100	0100
5	0101	0101
7	0111	1101
8	1000	0010
10	1010	1010
12	1100	0110
14	1110	1110



Routing

- Relies on existing routing protocols
  - Earliest delivery (single path routing)
  - Epidemic minimum estimated expected delay (replicative routing)
- Forwarding Procedure
  - Intermediate node decrypts a received packet and gets the access structure for the next group
  - Intermediate node forwards the packet to nodes of the next group, based on the access structure
- One or more additional nodes may exist between two consequent groups
  - The paper doesn’t state when and how a relay node relays bundles to the nodes not in the next group



Offline/Online protocol

- Offline
  - Distribution of ABE-related keys
  - Distribution of node IDs
- Online
  - Sender
    - Grouping (through building a binary tree)
    - Multiple ABE encryptions (65ms w/ 2^4 nodes, 393ms w/ 2^{20} nodes per encryption)
  - Intermediate nodes
    - ABE Decryption (44ms w/ 2^4 nodes, 214ms w/ 2^{20} nodes per decryption)