Replay Detection and the DTN Retransmission Block

Susan Symington
susan@mitre.org

Denial of Service Threat in DTN

- Unauthorized access and use of DTNs is a serious concern
  - DTNs are characterized by resource scarcity
- Use of the Bundle Authentication Block (BAB) already protects against unauthorized use:
  - The BAB enables bogus or modified bundles to be detected and discarded at the first node at which they are received
- Some networks may require measures to actively detect and delete replayed bundles
  - Replayed bundles cannot be detected by using the BAB
  - Replayed bundles will be deleted when they expire, but this may not be soon enough

Current Duplicate Detection in DTN: only for delivery

- The Bundle Protocol (BP) has an "at-most-once-delivery" registration option to protect applications from having duplicate bundles *delivered* to them.
- The BP does not have an option to prevent nodes from *forwarding* duplicate bundles.
- Detecting duplicate bundles is a local matter; a node must keep a list of the
  - Source EID,
  - Creation timestamp, and
  - Fragment Offset (if any)

of every bundle it receives, and compare newly received bundles against this list.

Unsolved: distinguishing legitimate duplicates from illegitimate replays

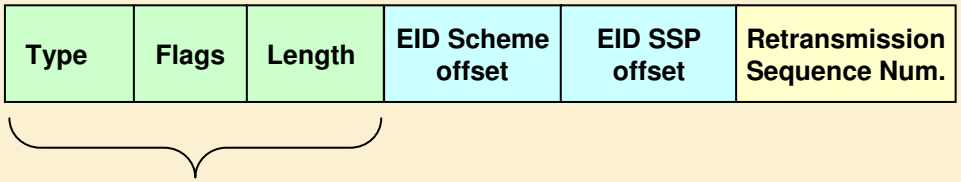
- Replay detection and deletion is more complicated than just the local matter of detecting and deleting duplicate bundles.
- Not all duplicates are illegitimate replays
- Some duplicates are legitimate and desirable:
  - The optimal path to a destination may involve a routing loop
  - Custody-based bundle retransmission results in duplicates
- A mechanism for distinguishing legitimate duplicates from illegitimate replays is required in order for a network to suppress illegitimate replays while supporting the transmission of legitimate duplicates.

Distinguishing legitimate duplicates from illegitimate replays (continued)

- Replay detection may need to be specified and enforced as part of the routing algorithm used
  - Accommodate intentional routing-protocol-stimulated replays but suppress replays resulting from routing protocol errors
  - Such replay-detection mechanisms would most likely be specific to the routing protocol and are not addressed here
- A mechanism for marking bundles that are custodial retransmissions is required
  - Accommodates the custodial transfer of bundles but enables replays to be suppressed
- Proposal: Optional DTN Retransmission Block
  - Marks bundles that are custodial retransmissions to make them distinguishable from illegitimate replays

DTN Retransmission Block (RB) Format

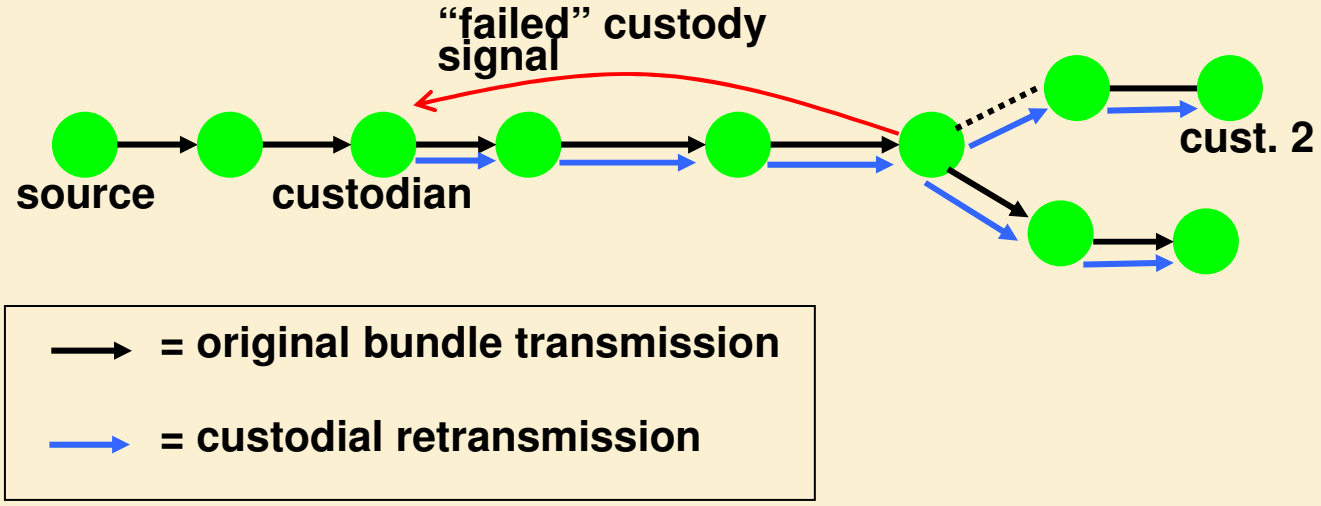
Retransmission Block Structure:



- Type, Flags, and Length fields are as defined in all non-primary-bundle blocks
  - The "Block must be replicated in every fragment" flag must not be set
- EID Scheme and SSP offsets point to the EID of the retransmitting custodian (in the dictionary)
- Retransmission Sequence Number – number of times this bundle has been retransmitted by this custodian (it has a value of 1 or greater)

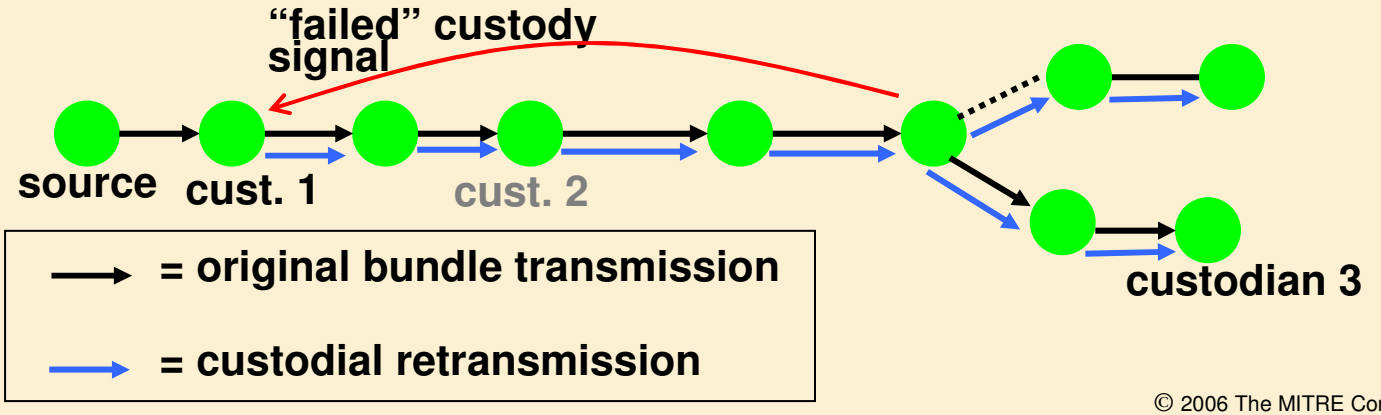
Retransmission Block (RB) Creation at RB-supporting Nodes

- If a custodian retransmits a bundle due to a custody transfer failure, the custodian must insert a RB into the bundle.
- The RB will contain the custodian's EID and a retransmission sequence number initialized to 1.
- The custodian must increment the retransmission sequence number in the RB every time it retransmits the bundle.



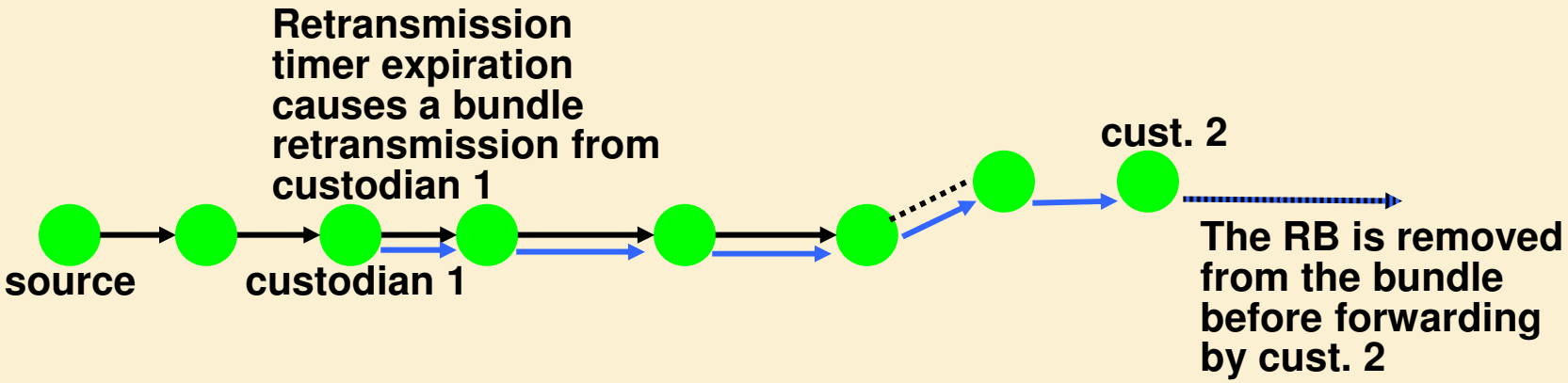
Retransmission Block (RB) Processing at RB-supporting Nodes

- Nodes that suppress replays must delete received duplicates that cannot be custodial retransmissions i.e., a received duplicate must be deleted if:
  - The receiving node is custodian of the previously-received duplicate (this is already specified in the Bundle Protocol),
  - The received duplicate has the same custodian as the previously-received duplicate, but it does not have a RB that was inserted by that custodian,
  - The received duplicate has the same custodian and RB as the previously-received duplicate



Retransmission Block (RB) Deletion at RB-supporting Custodians

- An RB is only valid from one custodian to the next.
- A node accepting custody of a bundle must delete the bundle's RB (if it has one).

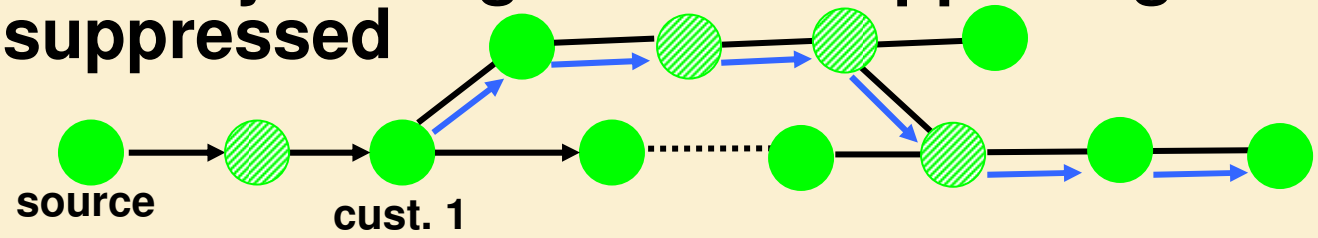


DTN Retransmission Block (RB): optional versus mandatory

- The Retransmission Block is optional
  - Nodes are not required to support it
- Whether or not replays should be suppressed must be an aspect of Local Security Policy
* A network cannot completely support both replay suppression and custodial retransmission if some of its nodes do not support the RB
- The next slide shows how we recommend replay suppression be handled in networks that include nodes that do not support the RB

Preserving custodial retransmission and maximizing replay suppression if some nodes don't support RBs

- Configure RB-supporting nodes to delete replays
- Configure non-RB-supporting nodes to forward duplicates (and leave the RB in the bundle)
  - preserves custodial retransmissions
- Configure non-RB-supporting nodes to not take custody of bundles
  - preserves custodial retransmissions
- All replays except for those circulating exclusively among non-RB-supporting nodes will be suppressed



= original bundle transmission (does not contain an RB)

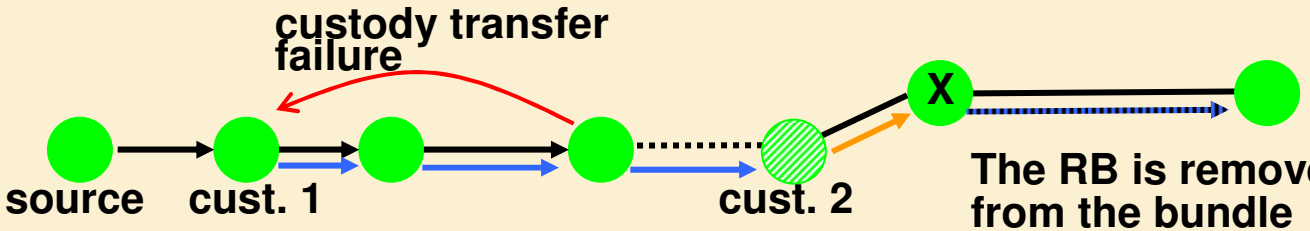
= custodial retransmission (contains an RB inserted by custodian 1)

DTN Retransmission Block (RB): optional versus mandatory

- Backup slides

Retransmission Block (RB) Deletion at RB-supporting Non-custodial Nodes

- Node's that do not support RBs may take custody without deleting the RB, so
- When any bundle is received at any RB-supporting node, its RB is deleted if the EID in the custodian field isn't the same as the EID in the RB.



The RB is removed from the bundle before forwarding by node X because cust. 1's EID is in the RB, but cust. 2 is the custodian of the bundle

= node that supports RBs

= node that doesn't support RBs

= original bundle transmission

= custodial retransmission

= bundle with new custodian, but with old RB

= bundle with new custodian, but without the RB

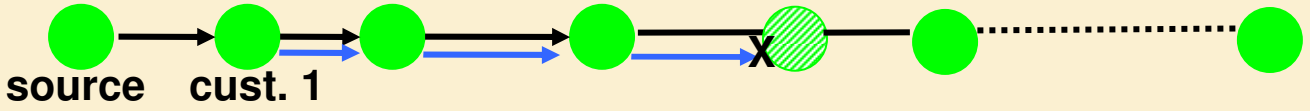
Whether or not replays should be suppressed must be an aspect of Local Security Policy

- If replay forwarding is allowed at a node, the node does not have to detect or delete duplicates.
- If replay forwarding is not allowed according to a node's local security policy, then:
  - BAB use should be required at that node (common sense)
  - The node must log each valid bundle's identifying information for comparison with future received bundles
  - A node that supports RBs must delete all duplicates that it receives that cannot be custodial retransmissions
  - A node that does not support RBs must delete all duplicate bundles it receives (at the cost of deleting legitimate custodial retransmissions received)*

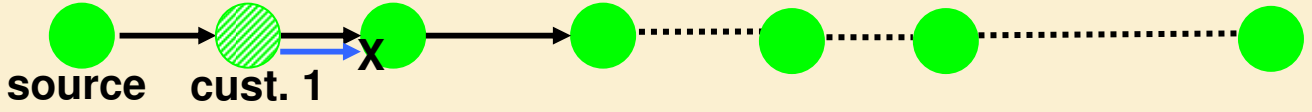
* A network cannot completely support both replay suppression and custodial retransmission if some of its nodes do not support the RB

Non-RB-supporting nodes break custodial retransmission if replays are suppressed

- DTN nodes that do not support the (optional) Retransmission Block cause custodial retransmissions to be deleted in two ways:
  - If a Non-RB-supporting node is configured to delete replays, it will (incorrectly) delete legitimate custodial retransmissions (because it will not recognize their RBs)

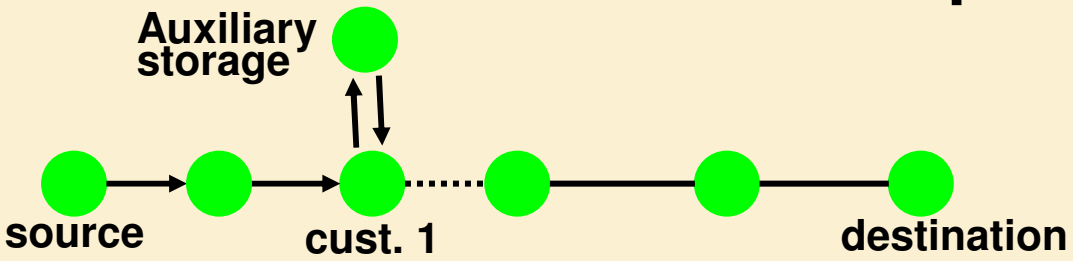


  - A non-RB-supporting custodial node will fail to insert an RB into a bundle that it custodially retransmits (thereby dooming the bundle for downstream deletion by any node that suppresses replays, even if that node supports the RB)



Replays vs. Loops

- These procedures will delete not only replays, but also bundles that are in routing loops
- To preserve bundles in intentional routing loops, additional measures will be required, e.g.



- When bundle returns to cust. 1, the duplicate will not be deleted, but if the bundle loops to auxiliary storage again, it may be deleted as a duplicate.
- Special configuration regarding aux. storage nodes could prevent this deletion.
- Only loops known a priori can be accommodated; bundles in opportunistic loops might be deleted