

# Paths Towards Patching the Bundle Protocol's (Un)Reliability

- Wesley Eddy
- Verizon / NASA

# End-to-Endedness

- Bundle protocol may be end-to-end
  - at least nearly
- Many apps do/will assume delivered bundle payloads are correct
  - Custody Transfer
- Thus end-to-end principle applies w.r.t. reliability of bundles
  - Jerome H. Saltzer, David P. Reed, and David D. Clark, "[End-to-End Arguments in System Design](#)", ACM Transactions on Computer Systems 2 (4), November 1984.

Yet the Bundle Protocol Has  
**NO Checksums**

# Well the Convergence Layer Adapters Will Catch and Repair Errors ...

- Fantasy world
- Real world
  - Weak checksums: UDP & TCP 16-bit one's complement
  - Errors can (and will) occur **between** convergence layer adapters (in memory, disk, drivers)
    - Jonathan Stone, Craig Partridge, "[When the CRC and TCP Checksum Disagree](#)", Proceedings of ACM SIGCOMM 2000
    - Jonathan Stone, Michael Greenwald, Craig Partridge, James Hughes, "[Performance of Checksums and CRCs Over Real Data](#)", IEEE/ACM Transactions on Networking 6 (5), October 1998.

# Proposed Short-Term Fix

- [draft-eddy-dtnrg-checksum-00](#)
- New Bundle Block that simply holds a checksum over the contents of the Payload Block
  - field for identifying algorithm
- Yes, you **could** do this with the security framework ...

# Why The Security Framework is Sub-Optimal for Reliability

- Requirements language is too strong w.r.t RSA and other algorithms for many nodes
  - Code that's not needed for integrity
  - Code that might not be wanted in footprint
- For integrity, keyed hash constructions are overkill
  - and no key establishment protocol exists anyways
  - unkeyed hashes are required for integrity
- Do you really want a pure integrity mechanism to be confused with a security mechanism?

# Long-Term Proposal

- **DO NOT** wait to publish existing bundle-spec ...  
this proposal is future work
- In future revision:
  - **Add a (optional) checksum to the canonical block format**
    - indicate presence with flag
    - capable of update as blocks are altered in-flight