A Null Space Based Defense for Pollution Attacks in Network Coding

Andrew Newell, Cristina Nita-Rotaru

Abstract

A network coding system allows intermediate nodes of a network to code packets together which ultimately results in better network performance. Due to the nature of network coding, it is difficult to impose hop-by-hop data integrity as intermediate nodes change packet contents. Without hop-by-hop data integrity, a byzantine adversary can mount a denial of service attack (pollution attack) which cripples a network coding system. Much work has focused on pollution defenses, but they all have limitations in terms of time synchronization, expensive computations, and large coding headers. A recent solution based on null spaces [3] has the potential to escape the aforementioned limitations. However, their solution does not work for arbitrary network topologies. We propose a new protocol with a novel null space splitting technique that ensures practical defense for arbitrary topologies.

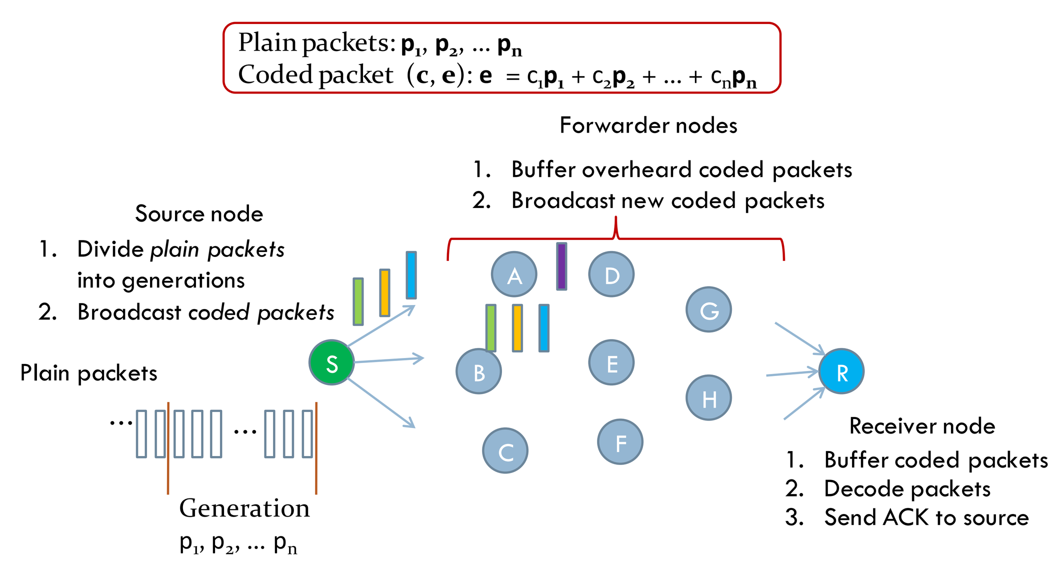
1. Network Coding

Network coding:

New paradigm for routing protocols.

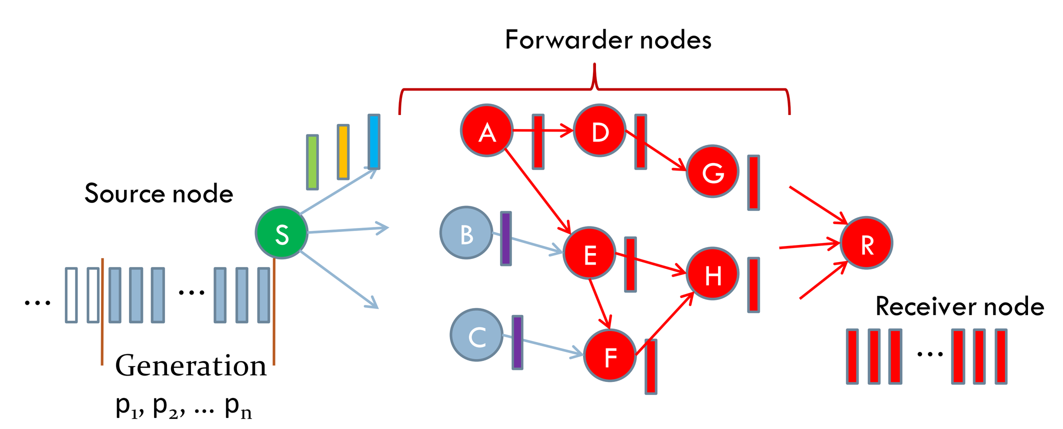
Intra-flow network coding:

Coding packets together within a single flow, e.g., MORE protocol:



- Higher throughput
- Reliability
- Energy efficiency

Pollution attack:



- Epidemic spreading
- Late discovery
- Cannot easily verify coded packets

2. Null Keys

Rowspace and null space:

- Rowspace of **A**: all linear combinations of the rows of **A**, i.e., a linear subspace
- Null space of **A**: all column vectors **x** s.t. $\mathbf{y} * \mathbf{x} = 0$ where $\mathbf{y} \in$ Rowspace of **A**

Null space pollution defense:

All coded packets in an intra-flow network coding system are linear combinations of a matrix **A**.

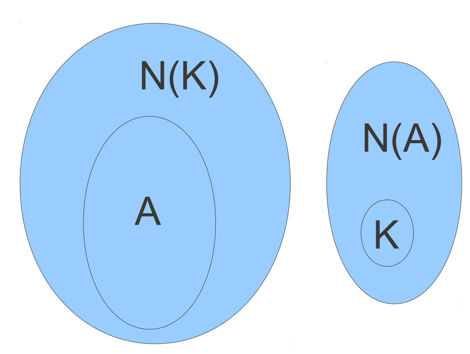
$$\mathbf{c} = \mathbf{r} * \mathbf{A}$$

Given a subspace of the null space as a matrix **K** (a null key) the following verification can occur for any coded packet.

$$\mathbf{c} * \mathbf{K} \stackrel{?}{=} \mathbf{0}$$

Null key size trade-off:

Small null keys are easier to distribute to forwarder nodes.



Large null keys reduce the probability that a byzantine adversary can pollute.

3. Splitting the null key

Motivation:

- Null keys are large
- Forwarders need a new null key each generation
- Each forwarder needs its own unique null key

Splitting a null space:

Let $\mathbf{A} = [\mathbf{I}|\mathbf{X}]$ where **X** is the data for a generation and $N(\mathbf{A})$ be represented by the column space of **B**. We show that a large portion of **B** can remain constant for multiple generations.

$$\begin{aligned} \mathbf{A} * \mathbf{B} = \mathbf{0} &\Rightarrow [\mathbf{I}|\mathbf{X}] * [\mathbf{S}^t|\mathbf{I}]^t = \mathbf{0} \\ &\Rightarrow \mathbf{I} * \mathbf{S} + \mathbf{X} * \mathbf{I} = \mathbf{0} \\ &\Rightarrow \mathbf{S} + \mathbf{X} = \mathbf{0} \\ &\Rightarrow \mathbf{S} = -\mathbf{X} \end{aligned}$$

Splitting null keys:

- Null key: 1500 bytes per column
- Generation independent portion: 1468 bytes per column
- Generation dependent portion: 32 bytes per column

Protocol strategy:

1. Initially, source distributes generation independent null keys
2. Each generation, source distributes generation dependent null keys
3. Each generation, forwarders receive generation dependent null keys, combine with generation independent null keys to obtain the full null key **K**
4. Upon receiving coded packets, forwarders verify $\mathbf{c} * \mathbf{K} = \mathbf{0}$

4. Evaluation

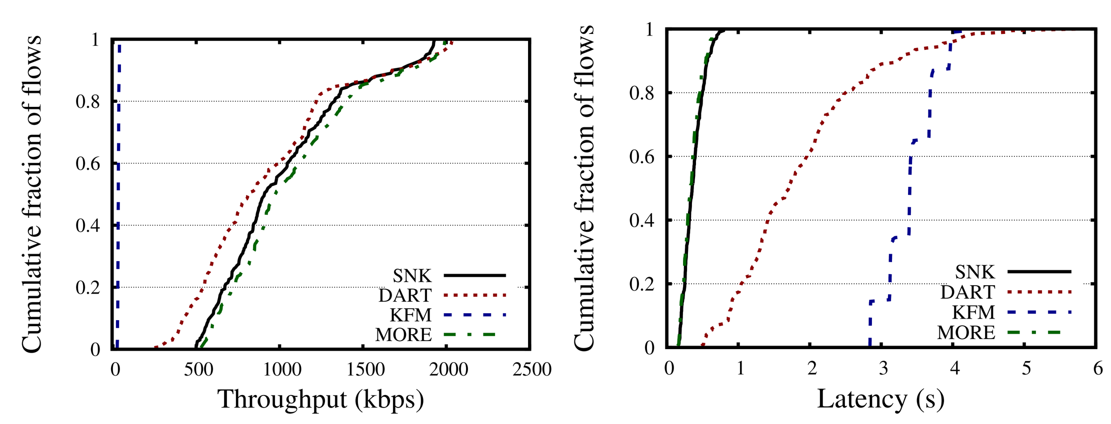
Simulation methodology:

- Simulator: GlomoSim
- Topology: RoofNet 38 node network
- Simulation run: random source-destination pair, 400 second transfer
- Experiment: 200 simulation runs, metrics plotted as CDF

Simulated protocols:

- MORE: standard intra-flow network coding protocol [1]
- SNK: our split null key protocol
- KFM: representative cryptographic-based protocol [4]
- DART: alternative time-based pollution defense protocol [2]

Simulation results:



References

[1] Szymon Chachulski, Michael Jennings, Sachin Katti, and Dina Katabi. Trading structure for randomness in wireless opportunistic routing. In *Proc. of ACM SIGCOMM '07*, 2007.

[2] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru. Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks. In *Proc. of WiSec*, 2009.

[3] E. Kehdi and Baochun Li. Null keys: Limiting malicious attacks via null space properties of network coding. In *Proc. of IEEE INFOCOM*, 2009.

[4] M. Krohn, M. Freedman, and D. Maziéres. On-the-fly verification of rateless erasure codes for efficient content distribution. In *Proc. of S&P*, 2004.