# Round-Efficient Broadcast Authentication Protocols for Fixed Topology Classes

**Haowen Chan**, Adrian Perrig
Carnegie Mellon University

1

## Talk Outline

- Background / Motivation
- Optimizations for the Path Topology
- Summary of Other Results

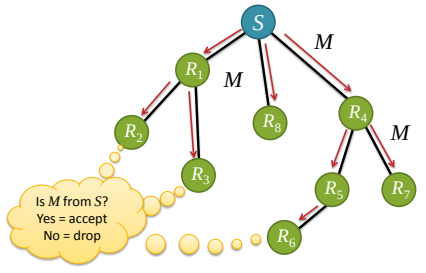
2

## Talk Outline

- Background / Motivation
- Optimizations for the Path Topology
- Summary of Other Results

3

## Multi-receiver Authentication in Sensor/Ad-hoc Networks




4

## Authentication Methods

- Signature: Sender S signs M using private key
  - Need support for public key crypto
- Multi-receiver Message Authentication Codes
  - Additional O(n) overhead in message size
- TESLA [Perrig et al, 2002]:
  - Need time synchronization
- **Communication-Efficient with Minimal Assumptions**
  - Guy Fawkes [Anderson et al. 1998]
  - Hash Tree-based [Chan & Perrig 2008]

5

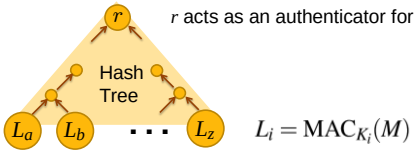
## Assumptions

- Sender knows full network topology
- Sender shares a unique symmetric key $K_i$ with each receiver $R_i$

6

## Hash Tree Based Broadcast

- Construct a hash tree with MACs at the leaves

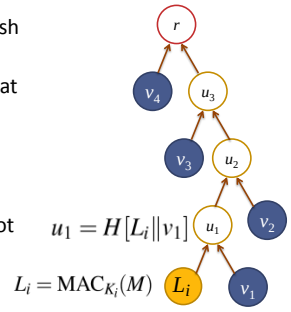



- Idea: Adversary can't compute $r$ for forged $M'$ since it does not know any of the MAC values of the legitimate nodes

7

## Receiver Verification

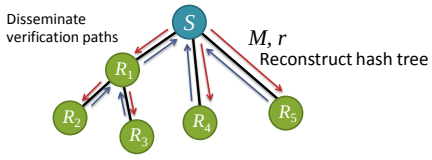
- Given Message $M$, hash tree root vertex $r$
- Receiver $R_i$ verifies that $L_i = \mathrm{MAC}_{K_i}(M)$ is a leaf in hash tree with root $r$
- Verification path = all siblings on path to root




8

## General Tree Topology: 3 Passes

1. Sender broadcasts message M with hash tree root $r$
2. Receivers reconstruct hash tree with leaves $L_i = \mathrm{MAC}_{K_i}(M)$
3. Verification paths disseminated



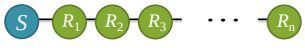

9

## Talk Outline

- Background / Motivation
- Optimizations for the Path Topology
- Summary of Other Results

10

## Path Topology




- Common applications
  - Actual linear topologies (roadway, corridor)
  - Path from leaf to root in spanning tree
  - Along a routing path
- 1 round = one interaction between neighbors
- Message from $S$ to $R_n$ takes $n$ rounds
- Unoptimized: 3 passes = $3n$ rounds

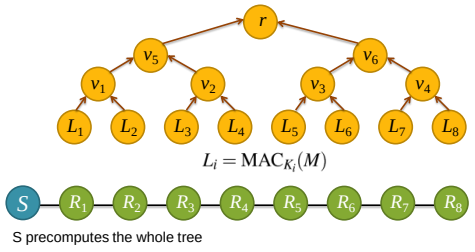
11

## Observation

- Can start reconstructing the hash tree immediately upon receiving $M$
- "Piggy-back" the two outgoing passes together
  - Achieve $2n$ rounds
  - Outgoing pass: left-siblings computed
  - Incoming pass: right-siblings computed

12

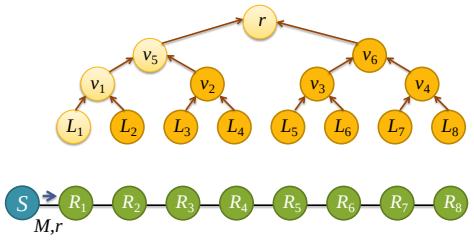
## 2*n*-Round Protocol




S precomputes the whole tree

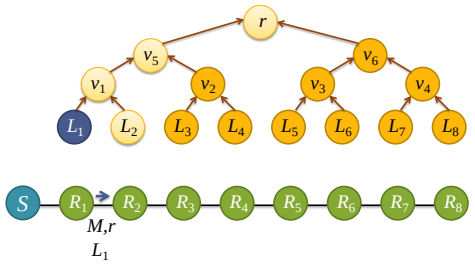
13

## 2*n*-Round Protocol



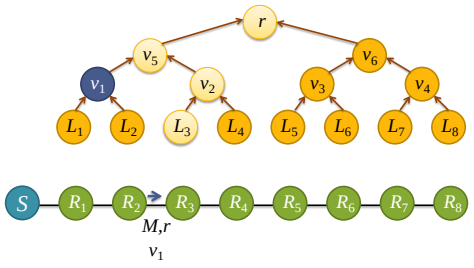

14

## 2*n*-Round Protocol



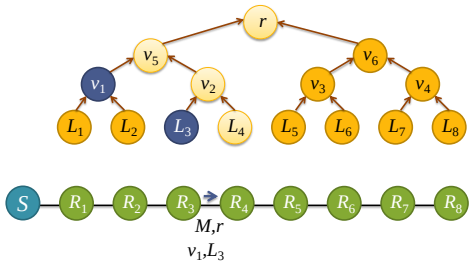

15

## 2*n*-Round Protocol



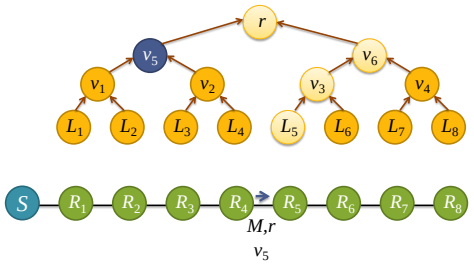

16

## 2*n*-Round Protocol



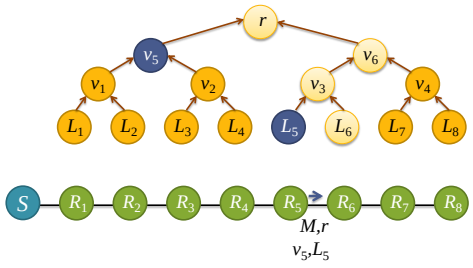

17

## 2*n*-Round Protocol



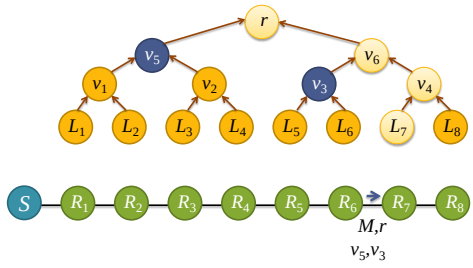

18

## 2*n*-Round Protocol



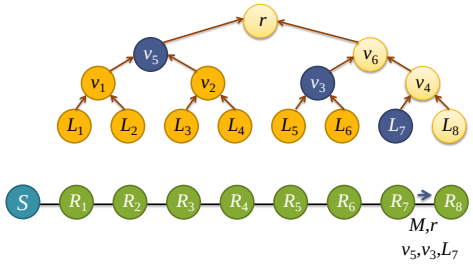

19

## 2*n*-Round Protocol



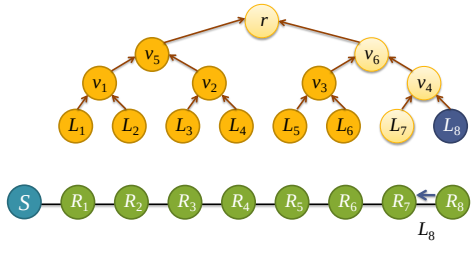

20

## 2*n*-Round Protocol



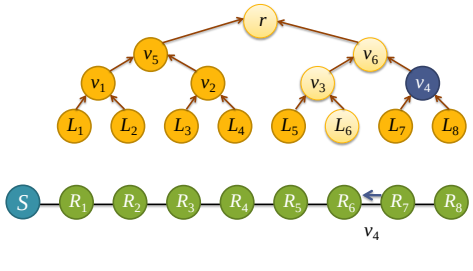

21

## 2*n*-Round Protocol



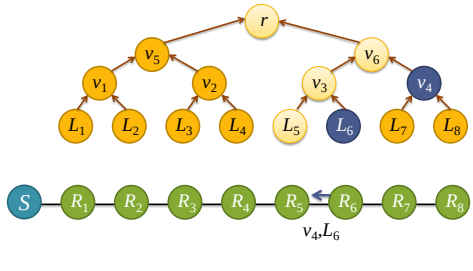

22

## 2*n*-Round Protocol



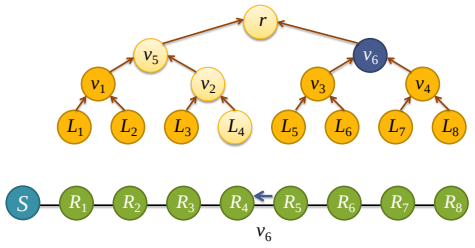

23

## 2*n*-Round Protocol



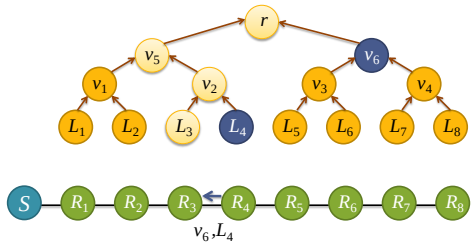

24

## 2$n$-Round Protocol



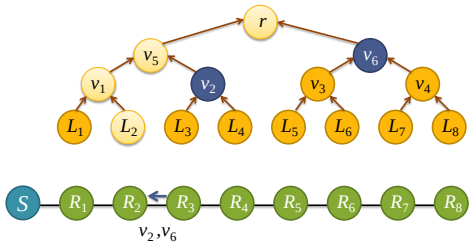

25

## 2$n$-Round Protocol



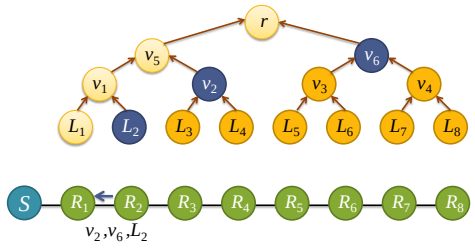

26

## 2$n$-Round Protocol



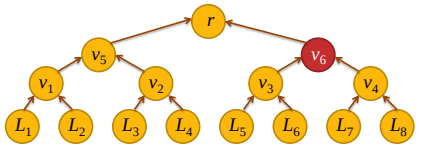

27

## 2$n$-Round Protocol




28

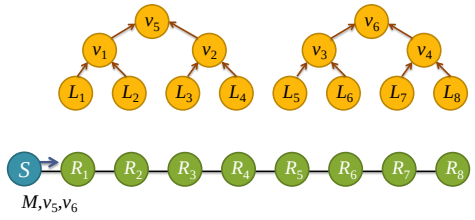
## Further Optimizations




- Computation of Node $v_6$ causes delay
- If Sender precomputes and sends $v_6$
  - Nodes 1-4 can build verification paths *independently* of 5-8
  - Split apart the two subtrees

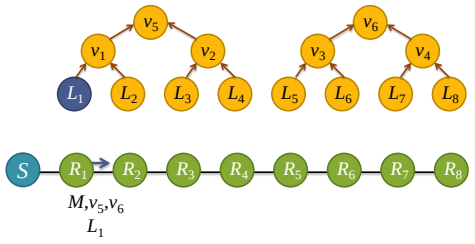
29

## 1.5$n$-Round Protocol



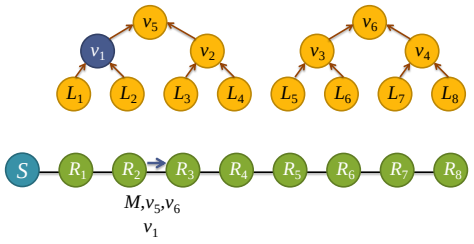

30

## 1.5$n$-Round Protocol



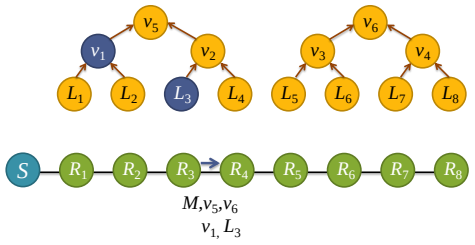

31

## 1.5$n$-Round Protocol



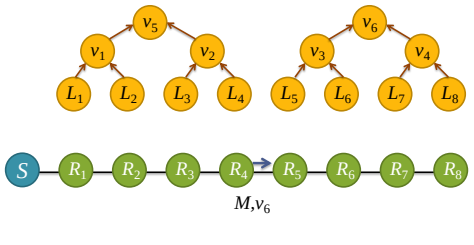

32

## 1.5$n$-Round Protocol



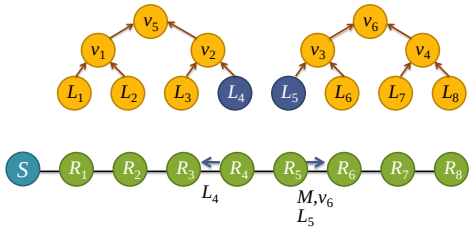

33

## 1.5$n$-Round Protocol



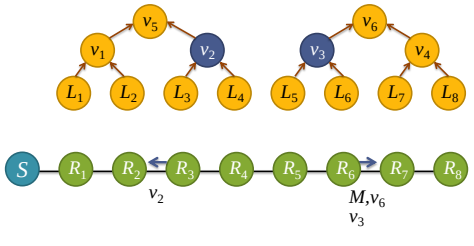

34

## 1.5$n$-Round Protocol



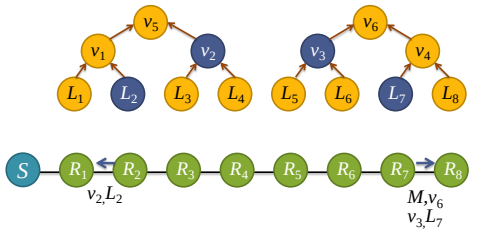

35

## 1.5$n$-Round Protocol



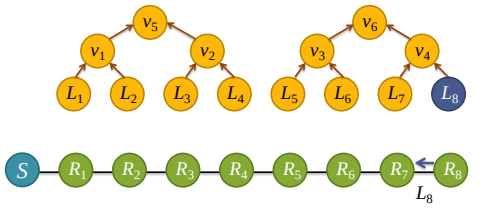

36

## 1.5$n$-Round Protocol



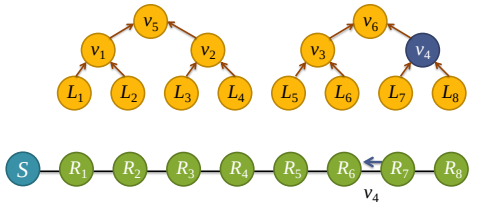

37

## 1.5$n$-Round Protocol



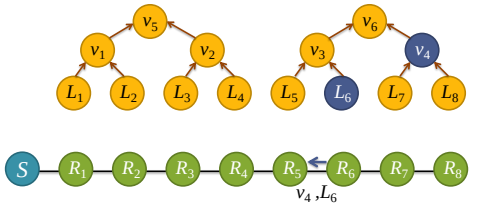

38

## 1.5$n$-Round Protocol



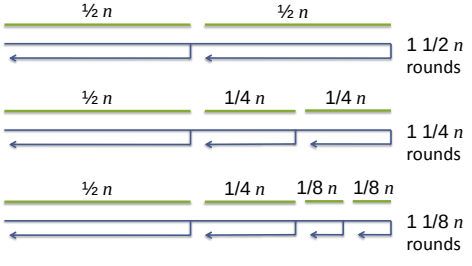

39

## 1.5$n$-Round Protocol




40

## General Optimization




41

## $n$-Round Protocol

- Break the receiver set into log $n$ groups
- Doubles communication overhead but halves the number of rounds
- No protocol can be faster than this

42

## Talk Outline

- Background / Motivation
- Optimizations for the Path Topology
- Summary of Other Results

43

## Guy Fawkes on the Path Topology

- Optimization to reduce Guy Fawkes to $2n$ rounds
- Reduce that to $n$ rounds using the same divide-and-conquer technique

44

## Round Complexity Lower Bounds

- Any Signature-free Broadcast Authentication Protocol that completes in $(2\text{-}\rho)\log n$ rounds for $0 < \rho \leq 1$ must have $\Omega(n^{\rho})$ comm. overhead per node
- Proven using a reduction to a known result for multi-receiver MACs
- Protocols with polylog communication overhead must take 2 log n rounds or more

45

## Tightness of the Bound

- Optimization of protocols for fully connected topologies
- Achieves $2\log n$ rounds with $O(\log^2 n)$ communication per node
- No protocol with polylog per node communication overhead can take fewer rounds

46

## Lower Bounds for Trees

- Any Signature-free Broadcast Authentication Protocol that completes in $(2.44\text{-}\rho)\log n + O(1)$ rounds in a tree topology must have $\Omega(n^{\rho})$ comm. overhead per node
- Strictly more than 2 passes are needed for trees
  - Known protocols are likely already optimal for trees

47

## Thank You!

**Haowen Chan**
haowenchan@cmu.edu

48