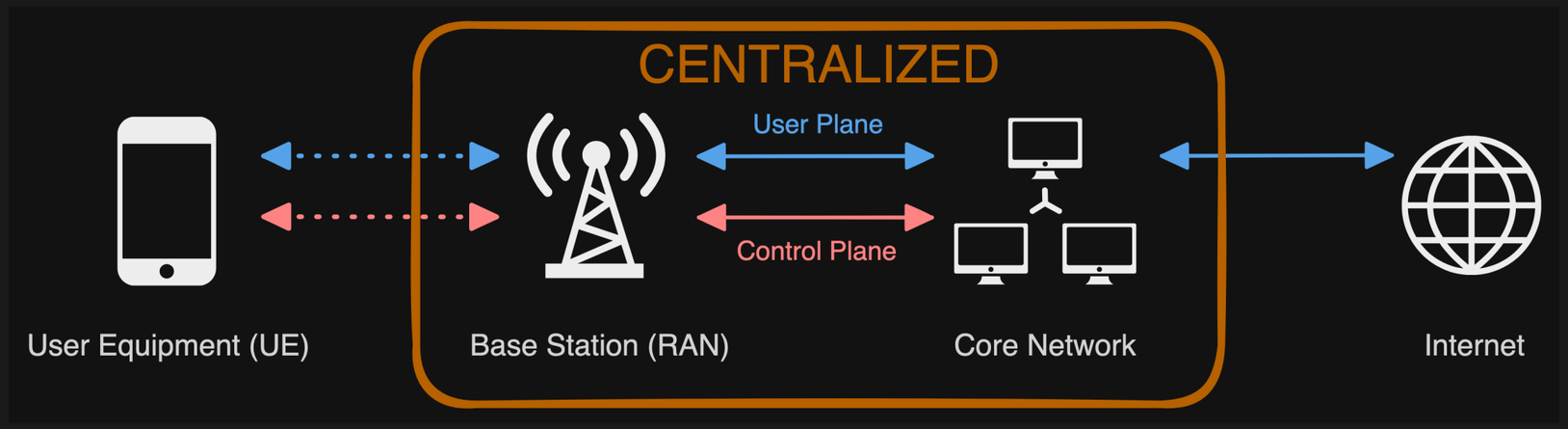
DNEXTG: A ZERO-TRUST DECENTRALIZED MOBILE NETWORK USER PLANE

Ryan W. West and Jacobus Van der Merwe, University of Utah

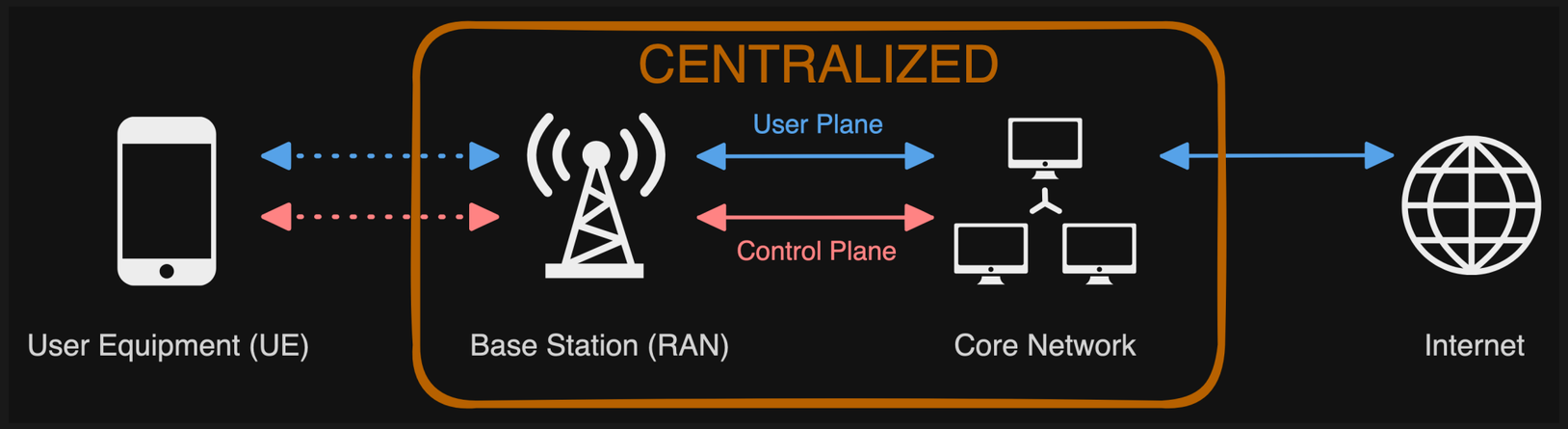
Presented by Ryan W. West (ryan@ryanwwest.com)

TODAY'S CELLULAR NETWORKS



- Mobile Wireless Networks mainly controlled by governments/large corporations
  - Licensed spectrum and nationwide wireless hardware is prohibitively expensive
  - Often limited to 2-3 providers that customers must trust

TODAY'S CELLULAR NETWORKS



- Mobile Wireless Networks mainly controlled by governments/large corporations
  - Licensed spectrum and nationwide wireless hardware is prohibitively expensive
  - Often limited to 2-3 providers that customers must trust
- New technology changes (NFV, COTS hardware) and regulatory changes (NIST zero-trust security focus, Citizens Broadband Radio Service public 5G spectrum):
  - Lower the mobile networking ecosystem barrier to entry
  - Emphasize heightened intra-network security
  - Allow **decentralized network models**

DECENTRALIZED MOBILE NETWORK MODELS

BENEFITS

- Distribute trust / decision-making authority away from one central actor
- Require **Zero-trust Security** - treat even internal network nodes as potential adversaries
- Allow affordable resource pooling and crowdsourcing

CHALLENGES

- Difficult to enforce these without a centralized authority:
  - Zero-Trust Security
  - Cooperation among nodes to provide good QoS
- 3GPP LTE/5G protects the network edge, not uncontrolled internal servers

DECENTRALIZED MOBILE NETWORK MODELS

BENEFITS

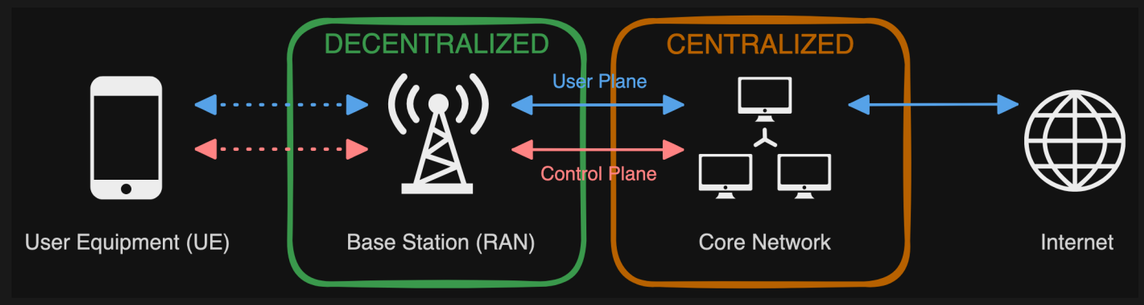
- Distribute trust / decision-making authority away from one central actor
- Require **Zero-trust Security** - treat even internal network nodes as potential adversaries
- Allow affordable resource pooling and crowdsourcing

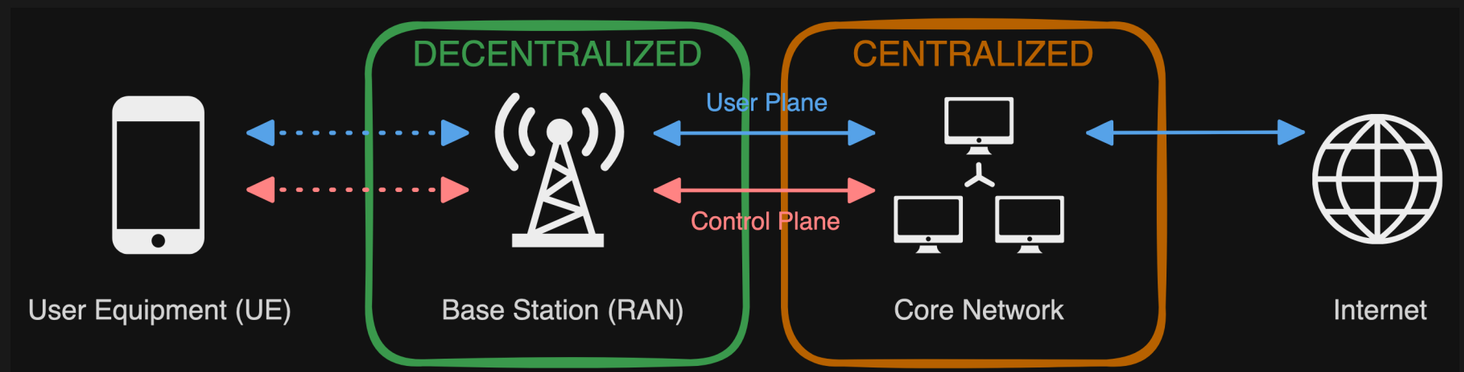
CHALLENGES

- Difficult to enforce these without a centralized authority:
  - Zero-Trust Security
  - Cooperation among nodes to provide good QoS
- 3GPP LTE/5G protects the network edge, not uncontrolled internal servers

REAL-WORLD DECENTRALIZED MOBILE RANS (RADIO ACCESS NETWORKS):

Helium Mobile™ POLLEN MOBILE

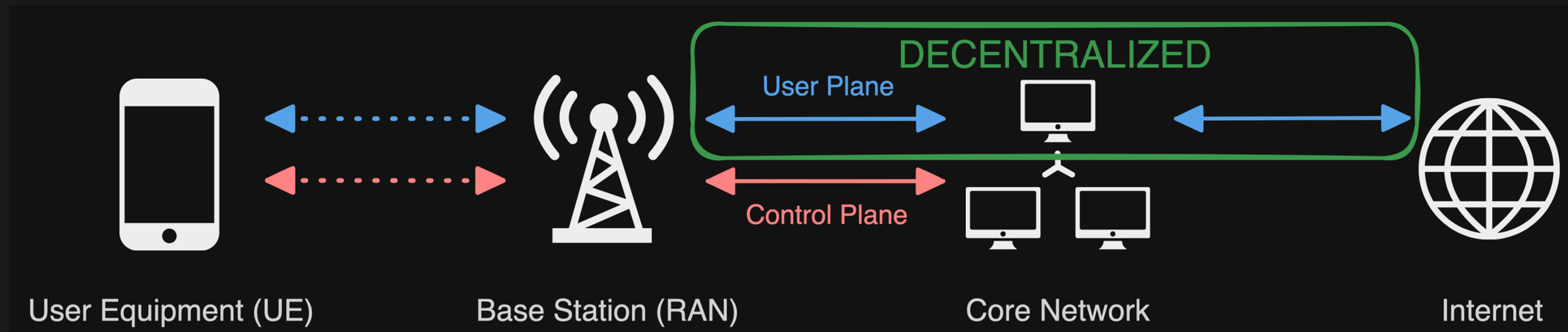




Can we decentralize more than just the RAN (Radio Access Network), to further extend decentralization's benefits (zero-trust security, distributed trust, affordable use cases)?

YES!

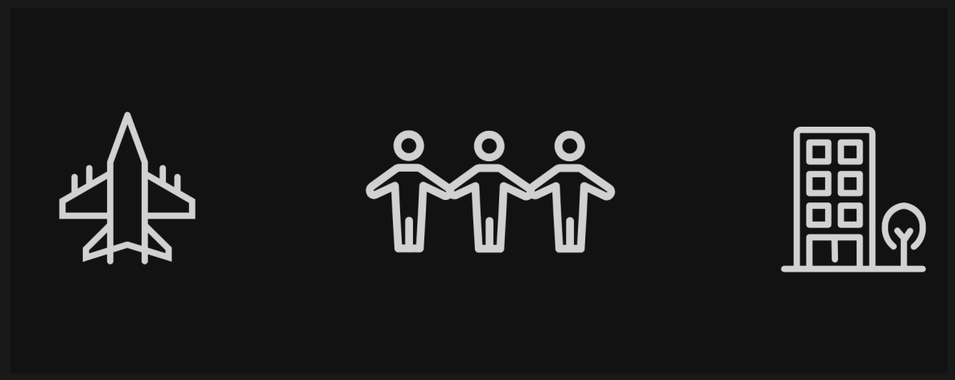
DNEXTG: A ZERO-TRUST DECENTRALIZED MOBILE NETWORK USER PLANE



- dNextG transforms a mobile network (5G) allowing its servers (nodes) to be independently run by adding a cooperative internal security monitoring framework
- Tracks reputation of each node based on random Core testing with blockchain
  - High reputation nodes are used more, low reputation nodes avoided/fixed
- Decentralizes the Core User (Data) Plane (90-95%+ of all traffic)
  - Affordable; could integrate with e.g. Helium/Pollen to add RAN decentralization

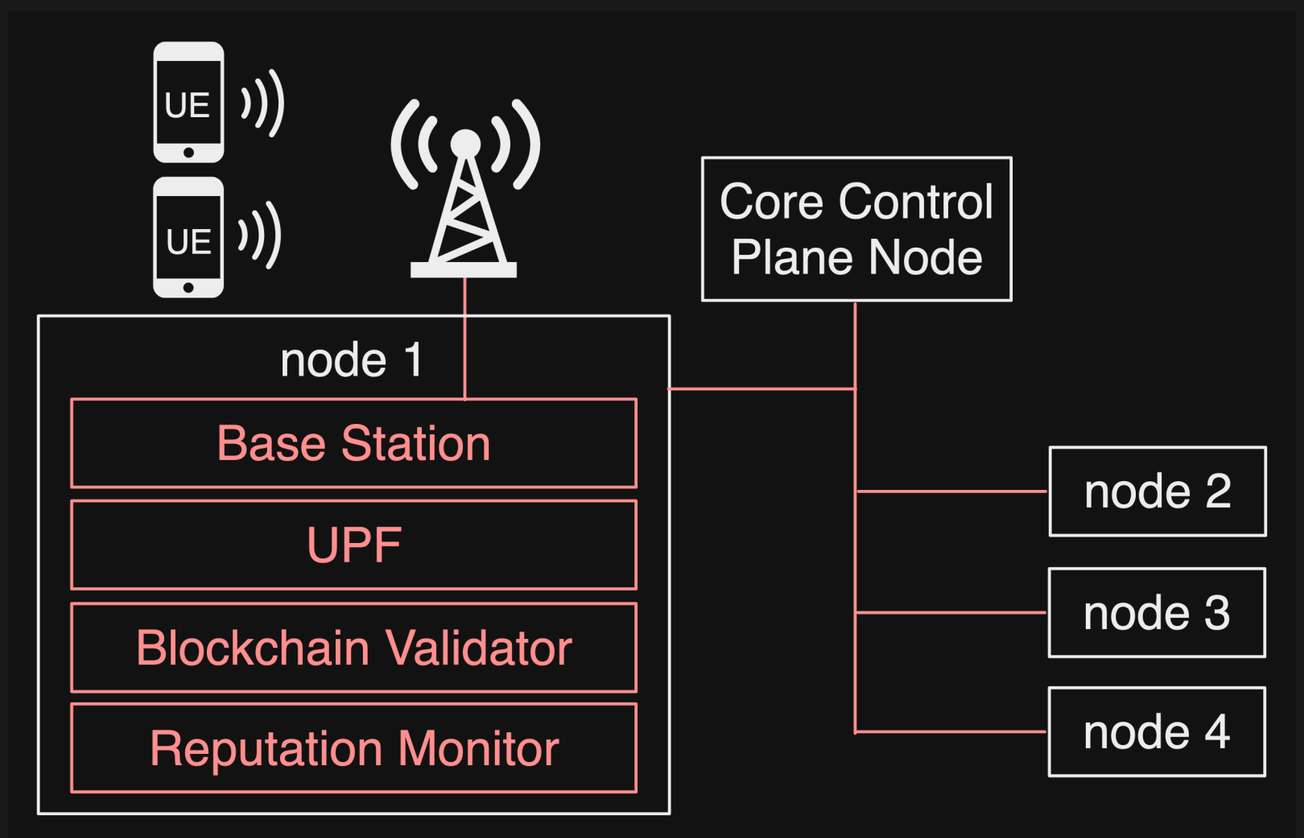
DNEXTG: USE CASES

1. **Coalition Military Network** - a nation deploys/shares a mobile network with ally nations for joint tactical missions
2. **Decentralized Community** - a group of people may each own base stations/servers and collectively offer a mobile network service (like Helium/Pollen) for profit
3. **Single Entity** - Centralized companies could use dNextG to improve zero-trust security



DNEXTG: ARCHITECTURE

- Each participant owns and operates a decentralized node running:
    1. Base Station (gNB in 5G RAN) - communicates wirelessly with UEs
    2. Core User Plane Function (UPF) - sends user traffic from gNBs ↔ internet
    3. Validator - maintains part of a BFT (Byzantine Fault Tolerant) blockchain
    4. Reputation Monitor - tests other nodes and reports to Validator
- Core Control Plane Node (authentication, billing, etc.)



DNEXTG: ENFORCING GOOD BEHAVIOR

- All decentralized nodes run a **network-wide reputation system** via blockchain
  - Node monitor each other to verify correct UPF operation via **reputation tests**
    - node psuedo-UEs try to connect through another node's UPF to the internet
  - Test results shared via BFT blockchain, form average reputation for each node
    - Past reputation test results cannot be edited (immutability) and up to 1/3 of nodes can be malicious to blockchain and reputation network will stay up
  - Improperly handling user data/breaking reporting rules lowers reputation

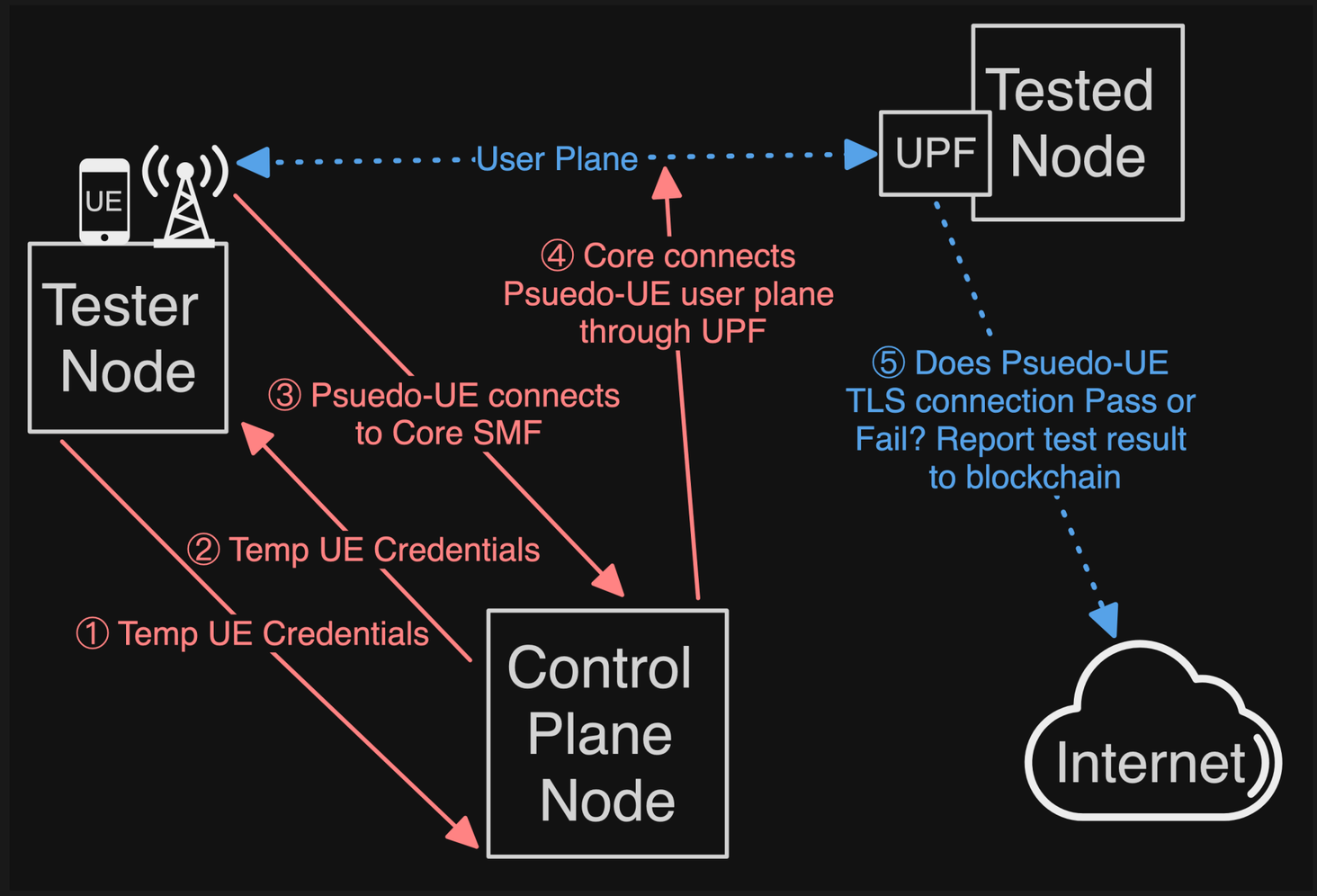
DNEXTG: ENFORCING GOOD BEHAVIOR

- All decentralized nodes run a **network-wide reputation system** via blockchain
  - Node monitor each other to verify correct UPF operation via **reputation tests**
    - node psuedo-UEs try to connect through another node's UPF to the internet
  - Test results shared via BFT blockchain, form average reputation for each node
    - Past reputation test results cannot be edited (immutability) and up to 1/3 of nodes can be malicious to blockchain and reputation network will stay up
  - Improperly handling user data/breaking reporting rules lowers reputation
- Incentive to maintain reputation:
  - Low-reputation nodes (i.e. malicious/malfunction) can be excluded, acted upon
  - High-reputation nodes (i.e. reliable) may be preferred by users, increasing profits

DNEXTG: THREAT MODEL (PROTECTS AGAINST 6 THREATS)

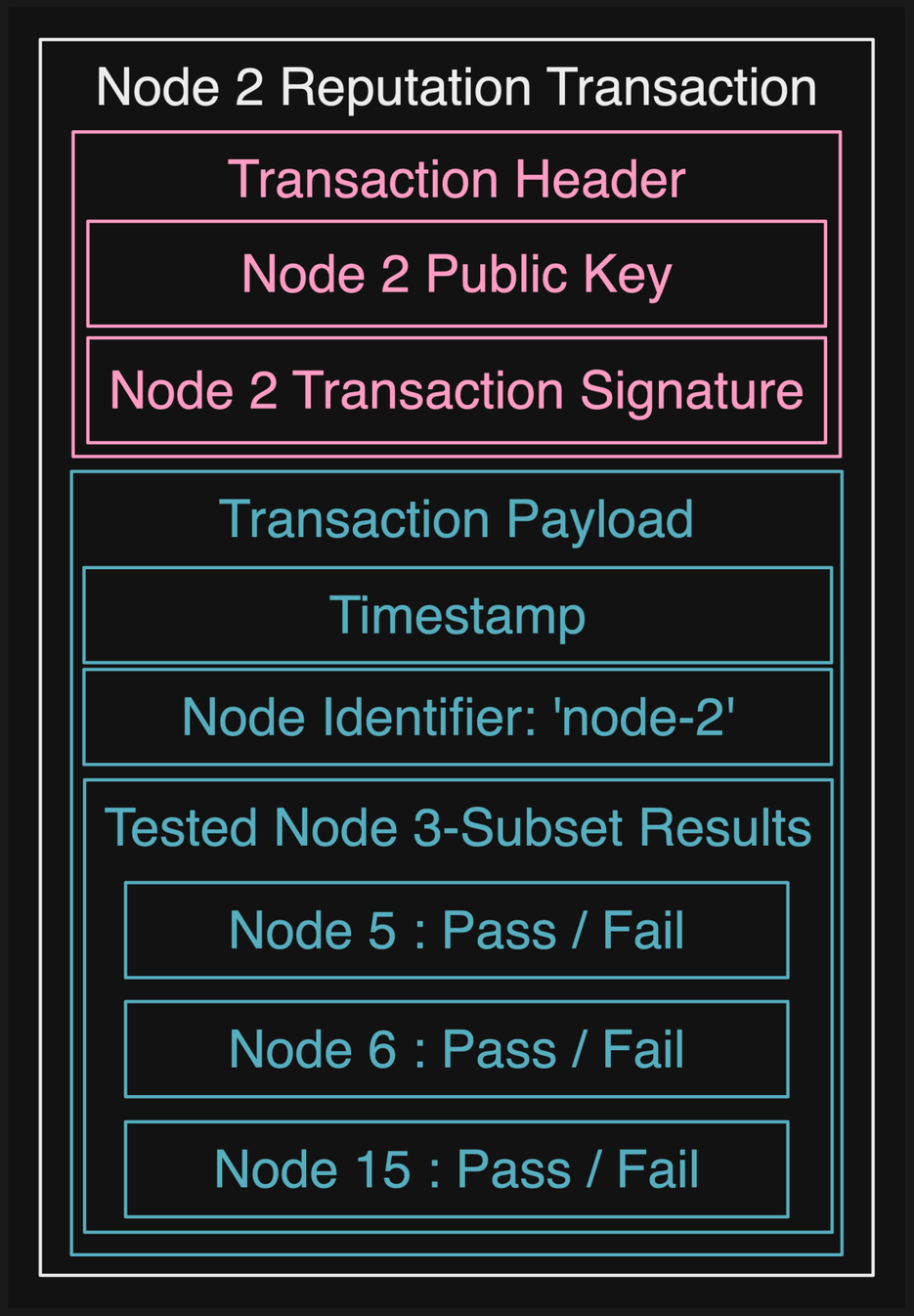
1. Dropping or modifying network traffic
2. False reputation reports (lying about results/who was testing or being tested)
3. Node collusion (nodes pass other nodes' tests to boost reputation)
4. Failing to report reputation / reporting too frequently
5. Abusing reputation-testing credentials (for free data connectivity)
6. Identifying and allowing reputation-test traffic, but not regular traffic

DNEXTG DESIGN: REPUTATION TEST PROCESS



Tester node picks verifiably random node subset, tests if each node UPF is functioning

DNEXTG DESIGN: REPUTATION REPORT GENERATION



- Tester node submits a Reputation Report Transaction to blockchain
- All node Validators collectively accept/reject the transaction
  - If accept, recalculate each node's average reputation from 0-10
  - Example rejection: Node 2 cannot submit a transaction that claims to be published by Node 3 (via Signature)

DNEXTG DESIGN: VERIFIABLY RANDOM NODE SUBSETS

HOW?

- Tester node must test a random 3-subset of peer nodes using seed: recent block hash || node ID
- All node Validators recalculate hash to ensure transaction subset is genuine

DNEXTG DESIGN: VERIFIABLY RANDOM NODE SUBSETS

HOW?

- Tester node must test a random 3-subset of peer nodes using seed: recent block hash || node ID
- All node Validators recalculate hash to ensure transaction subset is genuine

WHY?

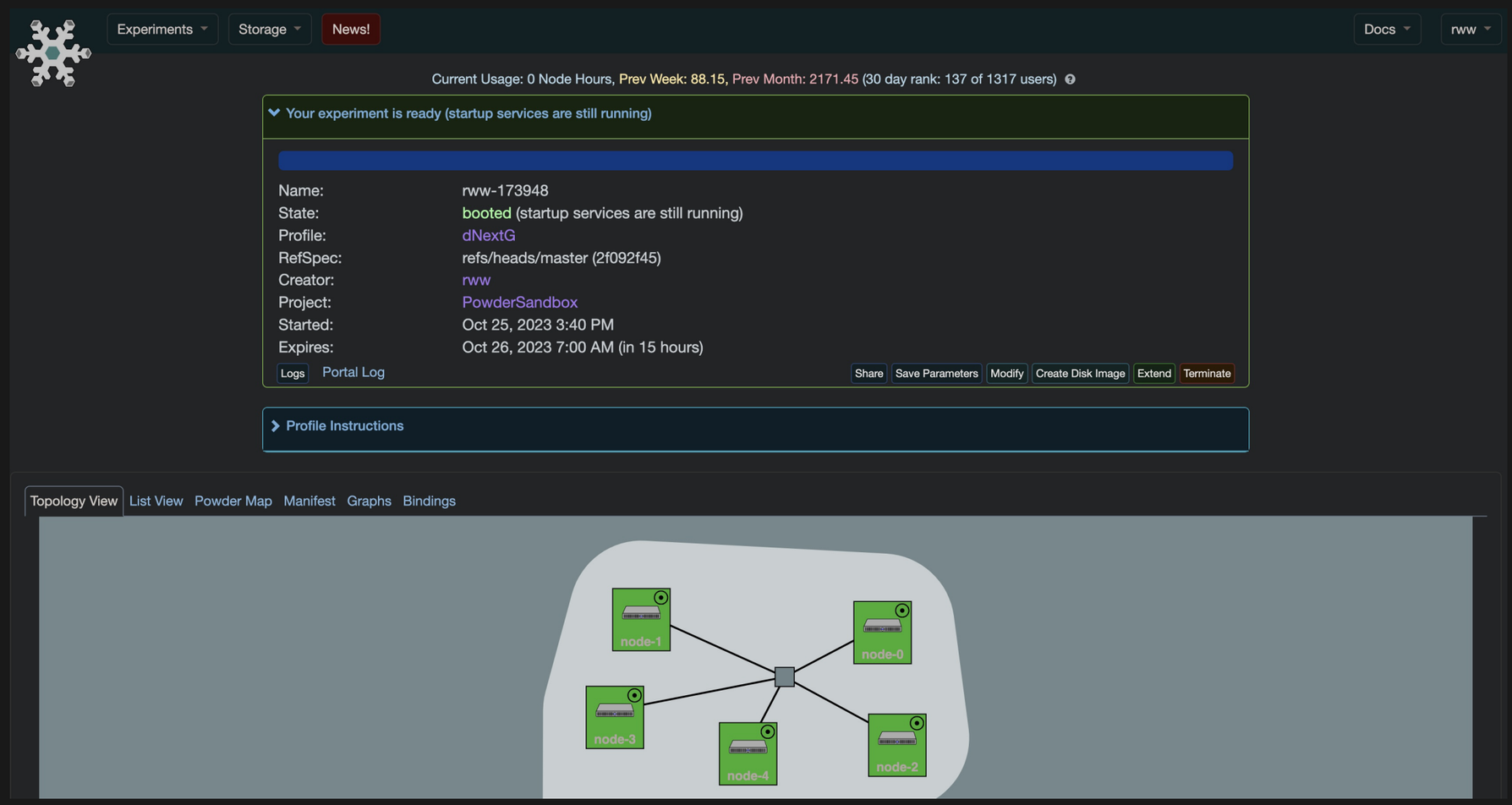
1. Reputation system scales linearly
2. Inhibits node collusion and targeting nodes with fake results
    - All nodes are tested ~equally
3. Consistent reporting → accurate rep.
4. Unpredictable test frequency → hard to distinguish if traffic belongs to a test

DNEXTG DESIGN: USING REPUTATION

- Average Node Reputation of 0-10 formed from last 100 applicable blockchain reports
  - Reputation is halved for nodes that report too frequently/infrequently
- UEs judge which node UPFs are most suitable/reliable using average reputation
  - Core Control Plane node enforces UEs' UPF route requests
- Consortium blockchains typically require a node majority vote to add new nodes
  - Joining should be made difficult (e.g., prove identity) to minimize adding malicious nodes. Nodes can also vote for a new Control Plane node

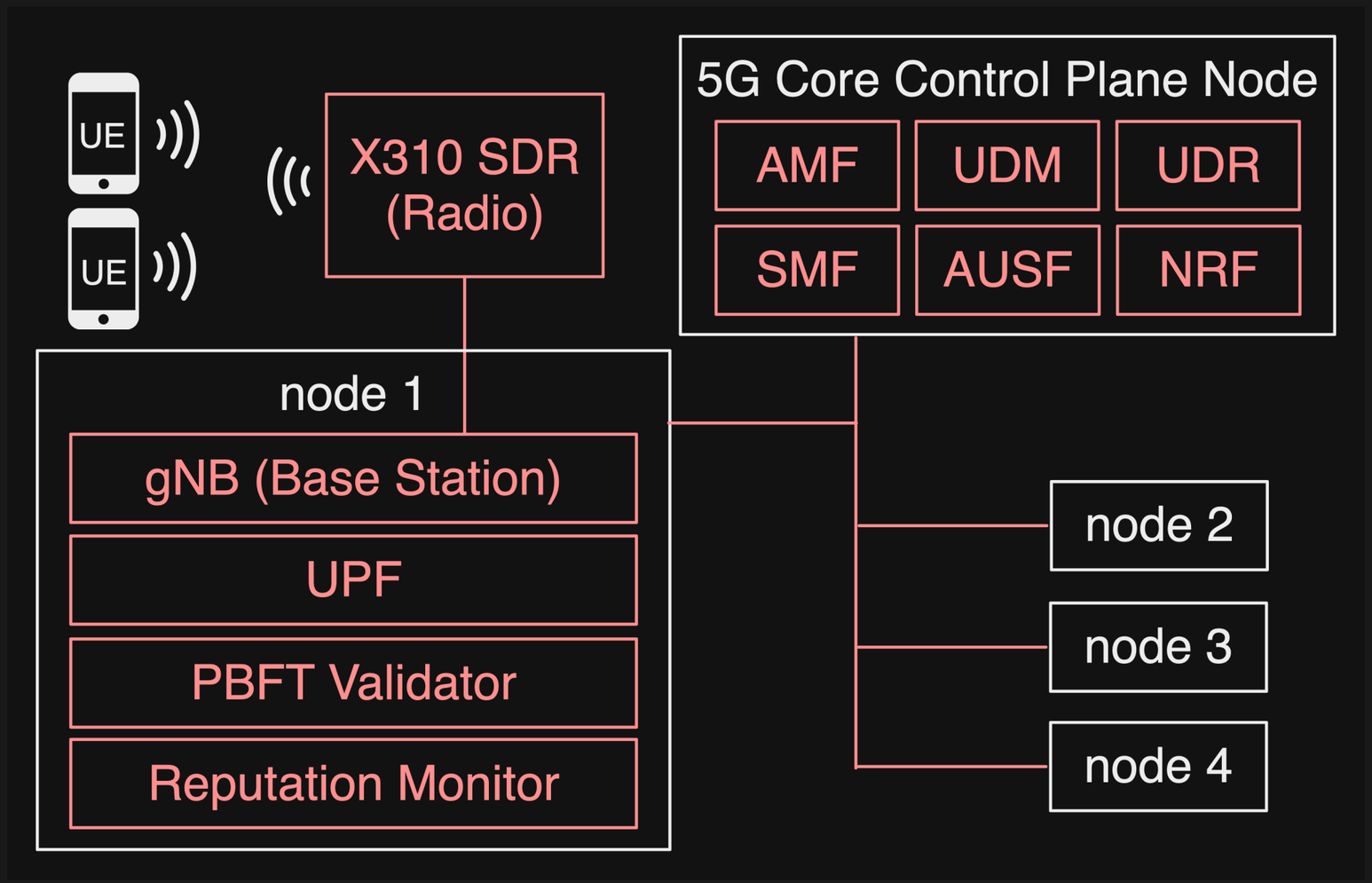
DNEXTG: IMPLEMENTATION (ON POWDER)

- Prototype implemented/evaluated on POWDER (Platform for Open Wireless Data-driven Experimental Research) at the University of Utah, USA
- Runs OpenAirInterface 5G Core + RAN , Hyperledger Sawtooth blockchain with PBFT (Practical Byzantine Fault Tolerance) tested virtually and over-the-air at 3550-3600MHz



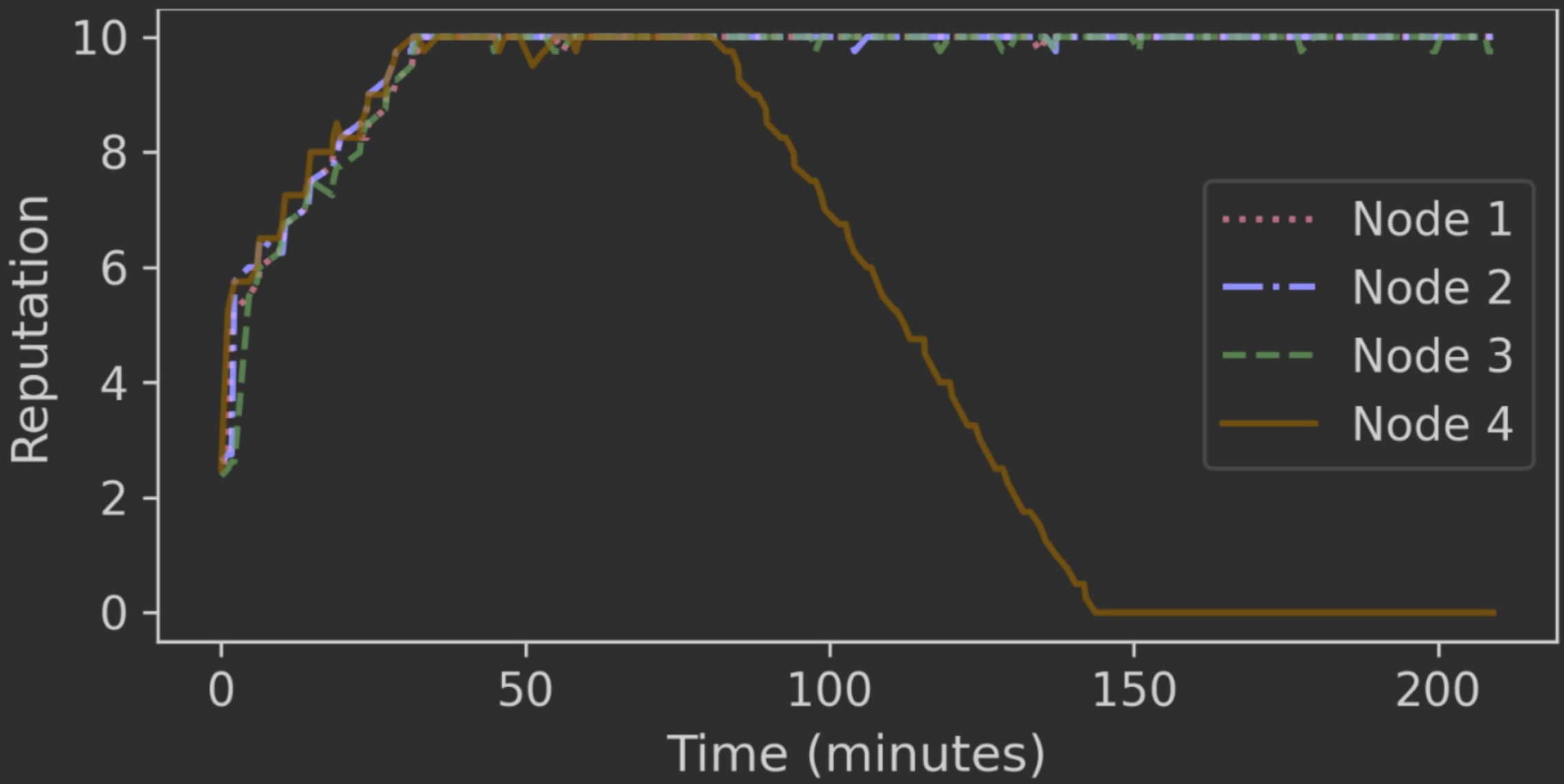
Instantly reproducible with https://github.com/ryanwwest/dNextG at powderwireless.net

DNEXTG: IMPLEMENTATION



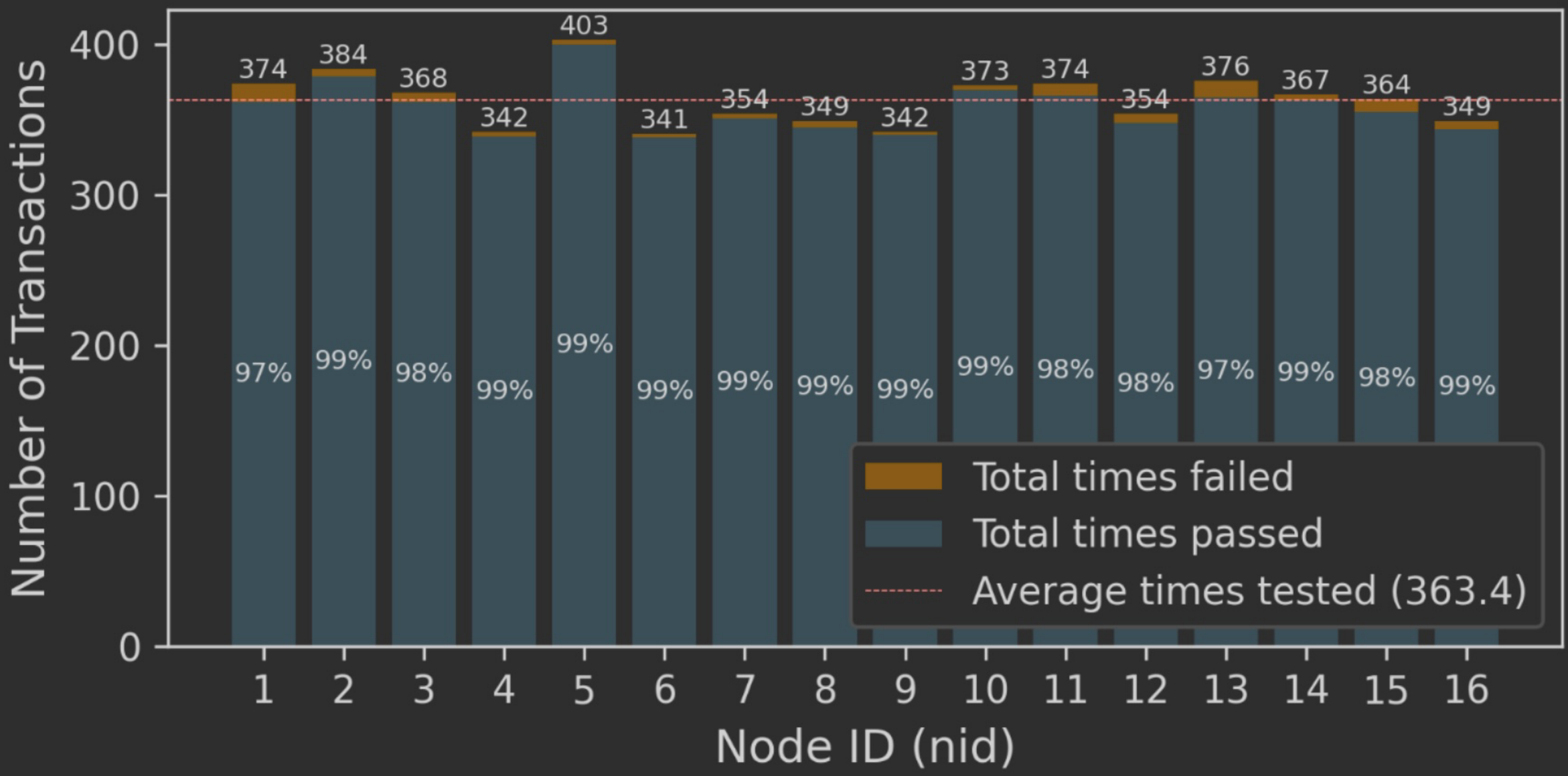
- Reputation Monitor program waits 3 minutes between testing UPFs
- UEs choose the highest-reputation available UPF for user plane routing

DNEXTG EVALUATION: STOPPING A NODE'S UPF



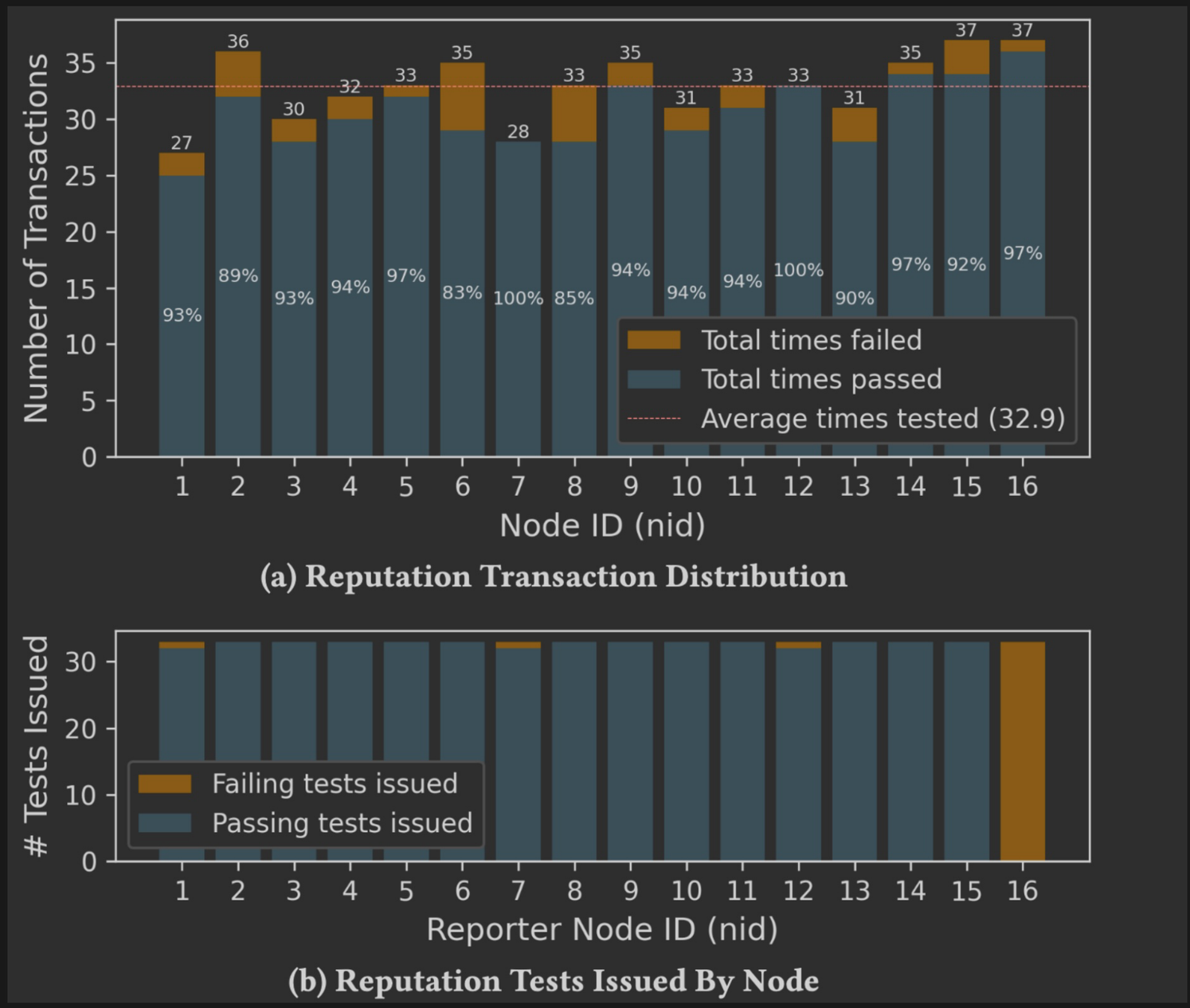
- Normally, UPFs pass other's reputation tests ~98% of the time
- If we stop Node 4's UPF, its reputation drops due to failed tests

DNEXTG EVALUATION: EVEN TESTING DISTRIBUTION



- Over 12 hours, 16 nodes have an even test distribution; random test intervals makes discerning test traffic from user traffic hard

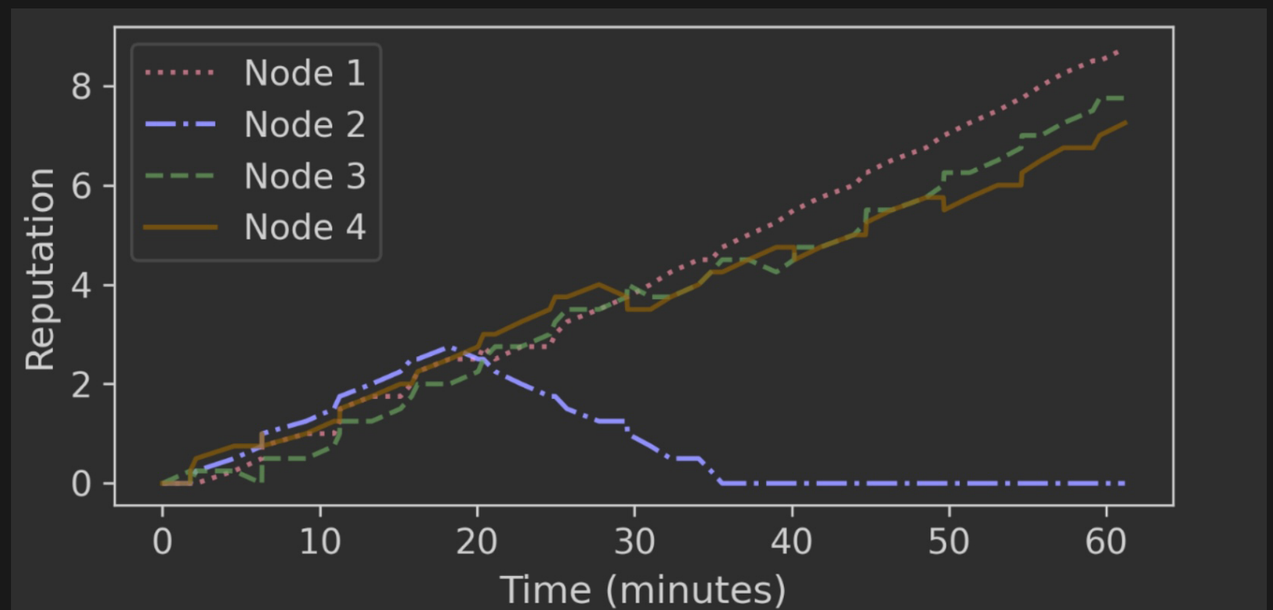
DNEXTG EVALUATION: NODE LYING ABOUT REPUTATION RESULTS



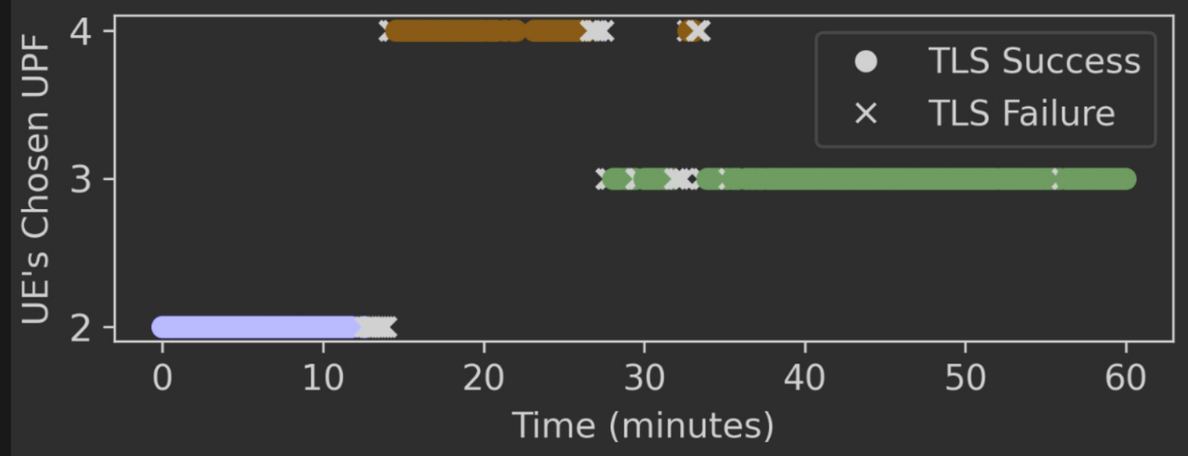
- Assume Node 16 always fails all other nodes. This affects overall reputations slightly but is easily seen as an anomaly and can be acted upon to fix/remove Node 16

DNEXTG EVALUATION: UE REACTIVITY TO REPUTATION CHANGES

- UE connects through Node 1's gNB to Node 2, whose UPF stops after 13 min
  - UE loses internet connection and switches to next-best reputation UPF (Node 4, lower pic).
  - Node 2's reputation drops
- At minute 27 Node 4 loses connectivity so UE connects through Node 3 which thereafter maintains the highest reputation



(a) Average reputations when node 2 stops processing traffic



(b) UE TLS Results Through Chosen UPF and node 1's gNB

DNEXTG: THREAT MODEL (PROTECTS AGAINST 6 THREATS)

1. Dropping or modifying network traffic
2. False reputation reports (lying about results/who was testing or being tested)
3. Node collusion (nodes pass other nodes' tests to boost reputation)
4. Failing to report reputation / reporting too frequently
5. Abusing reputation-testing credentials (for free data connectivity)
6. Identifying and allowing reputation-test traffic, but not regular traffic

CONCLUSION

- Recent changes in 5G/NextG networks allow for new decentralized use cases (military coalition networks, crowdsourced 5G communities)
- dNextG offers zero-trust security and reliable QoS for the Core Network User Plane
  - Replicable on the POWDER platform (powderwireless.net)
- Future work: decentralize the Core control plane

Full Paper Link

Contact: ryan@ryanwwest.com, linkedin.com/in/ryanwwest