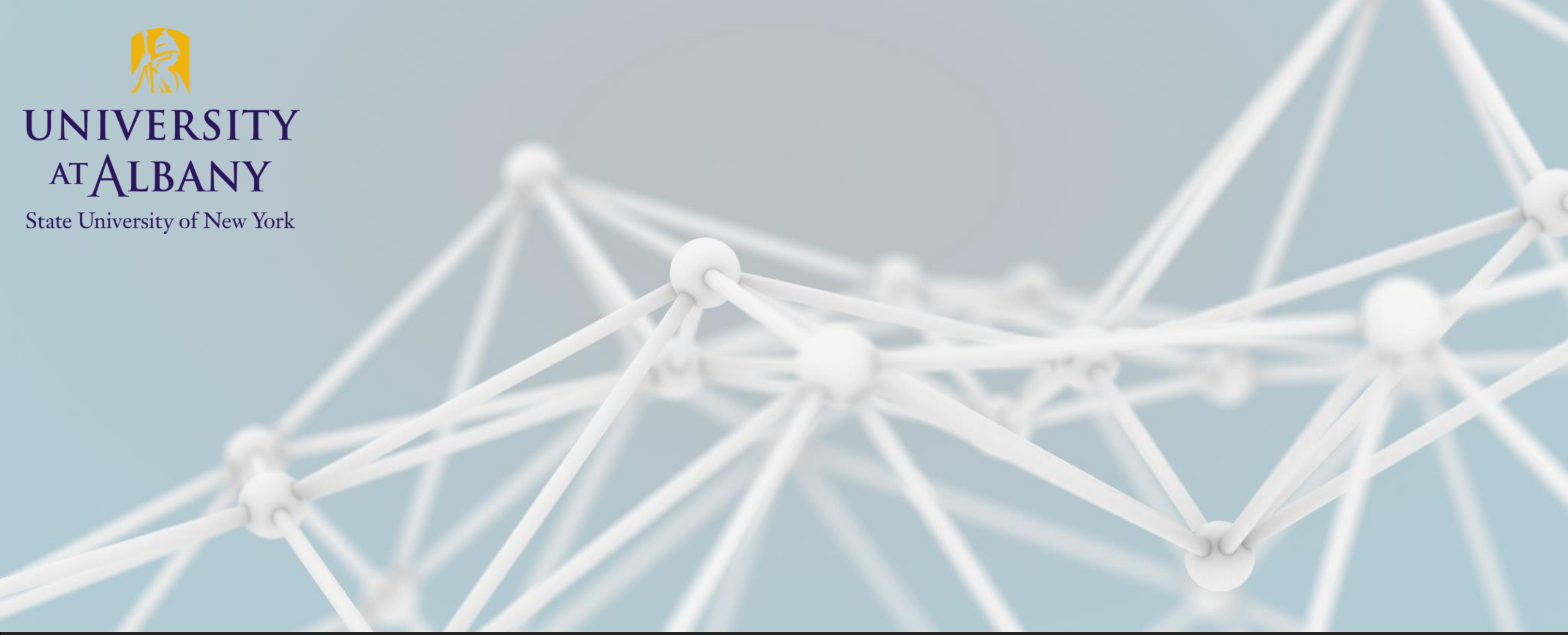


UNIVERSITY AT ALBANY
State University of New York

Reputation Based Routing in MANET using Blockchain

MAQSOOD CAREEM AND AVEEK DUTTA

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

UNIVERSITY AT ALBANY, SUNY

Motivation

Core Issue in routing in MANETs is the lack of trust → Unreliable packet delivery.

- Potential Solution:
  - Assess behavior and accrue the Reputation of Nodes
  - Determine Reputed route for packets

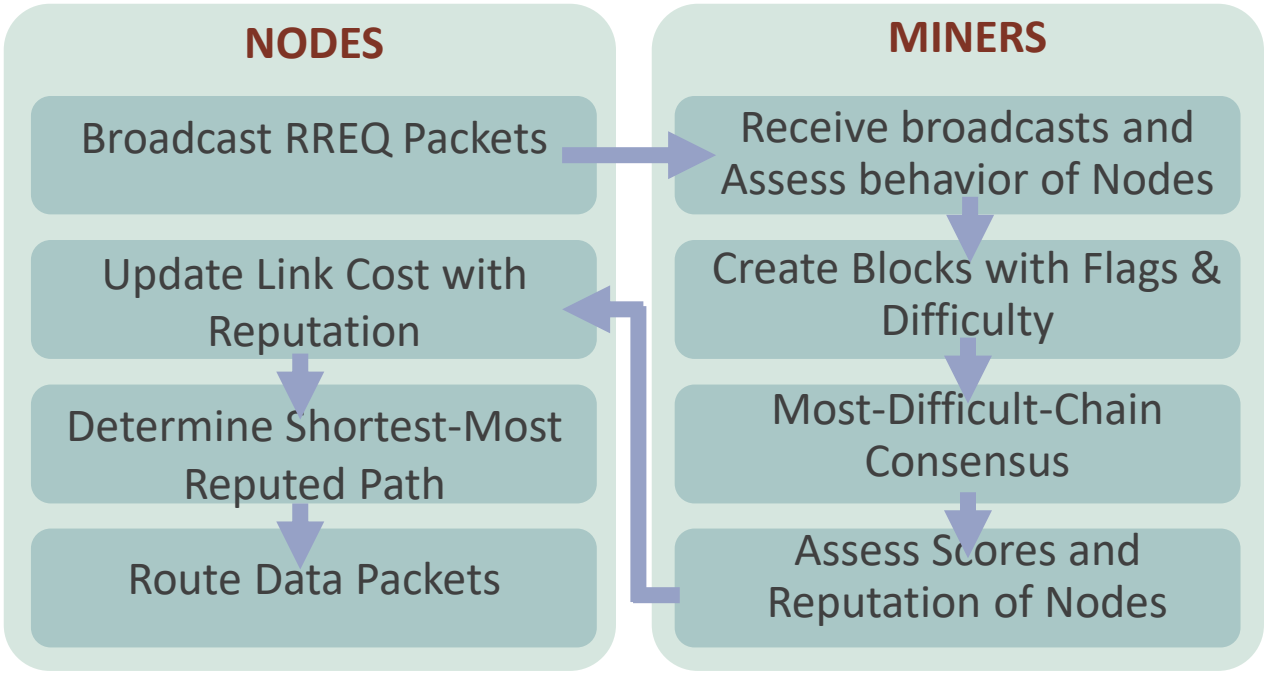
Blockchain based Reputed Routing in MANETs

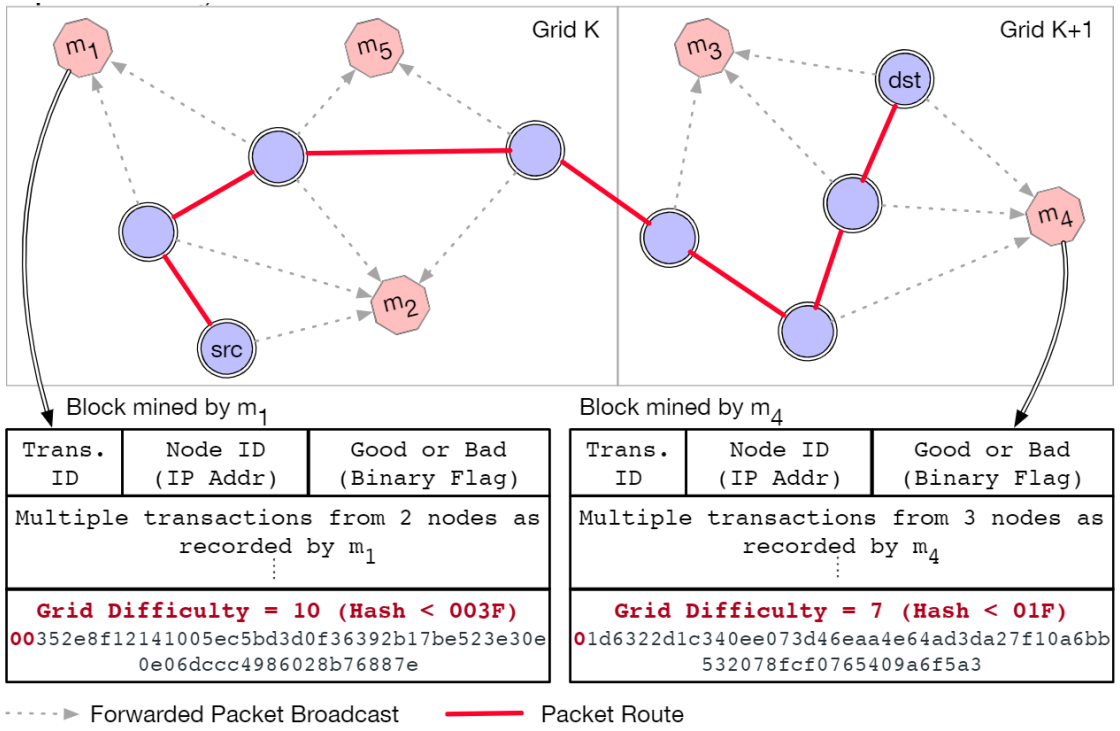
Determines the Shortest-Most Reputed path for routing.

System Model

- **Network & Routing Model**
  - Nodes are Distributed & Mobile. Fraction of Nodes serve as Miners
  - Routing: Any Reactive Routing Protocol (AODV is used as an example)
- **Blockchain Model**
  - Miners assess the Routing behavior of nodes
  - Record and disseminate information via Blockchain with heterogeneous Difficulty
- **Threat Model**
  - **Malicious Node (Routing Threat):** Black hole attack, Grey hole attack, Misrouting attack
  - **Malicious Miner (Blockchain Threat):** 51% attack, Forging blocks

Mechanism


NODES
Broadcast RREQ Packets
Update Link Cost with Reputation
Determine Shortest-Most Reputed Path
Route Data Packets
MINERS
Receive broadcasts and Assess behavior of Nodes
Create Blocks with Flags & Difficulty
Most-Difficult-Chain Consensus
Assess Scores and Reputation of Nodes


Grid K
Grid K+1
m1
m5
m2
src
m3
dst
m4
Block mined by m1
Trans. ID
Node ID (IP Addr)
Good or Bad (Binary Flag)
Multiple transactions from 2 nodes as recorded by m1
Grid Difficulty = 10 (Hash < 003F)
00352e8f12141005ec5bd3d0f36392b17be523e30e0e06dccc4986028b76887e
Block mined by m4
Trans. ID
Node ID (IP Addr)
Good or Bad (Binary Flag)
Multiple transactions from 3 nodes as recorded by m4
Grid Difficulty = 7 (Hash < 01F)
01d6322d1c340ee073d46eaa4e64ad3da27f10a6bb532078fcf0765409a6f5a3
Forwarded Packet Broadcast
Packet Route

Contributions

- **Novel Blockchain Design:** Records routing actions of nodes
  - Difficulty of mining ∝ Number of miners in a grid. (credibility of validation)
- **Nonlinear Reputation Metric:**
  - Combination of Credibility of Routing & Credibility of Validation
- **Novel Routing Protocol:**
  - Shortest, most reputed path routing
- **Evaluation on Novel Simulator:**
  - Integrated Blockchain based reputation management & MANET routing simulator

I. Routing Anomaly Detection

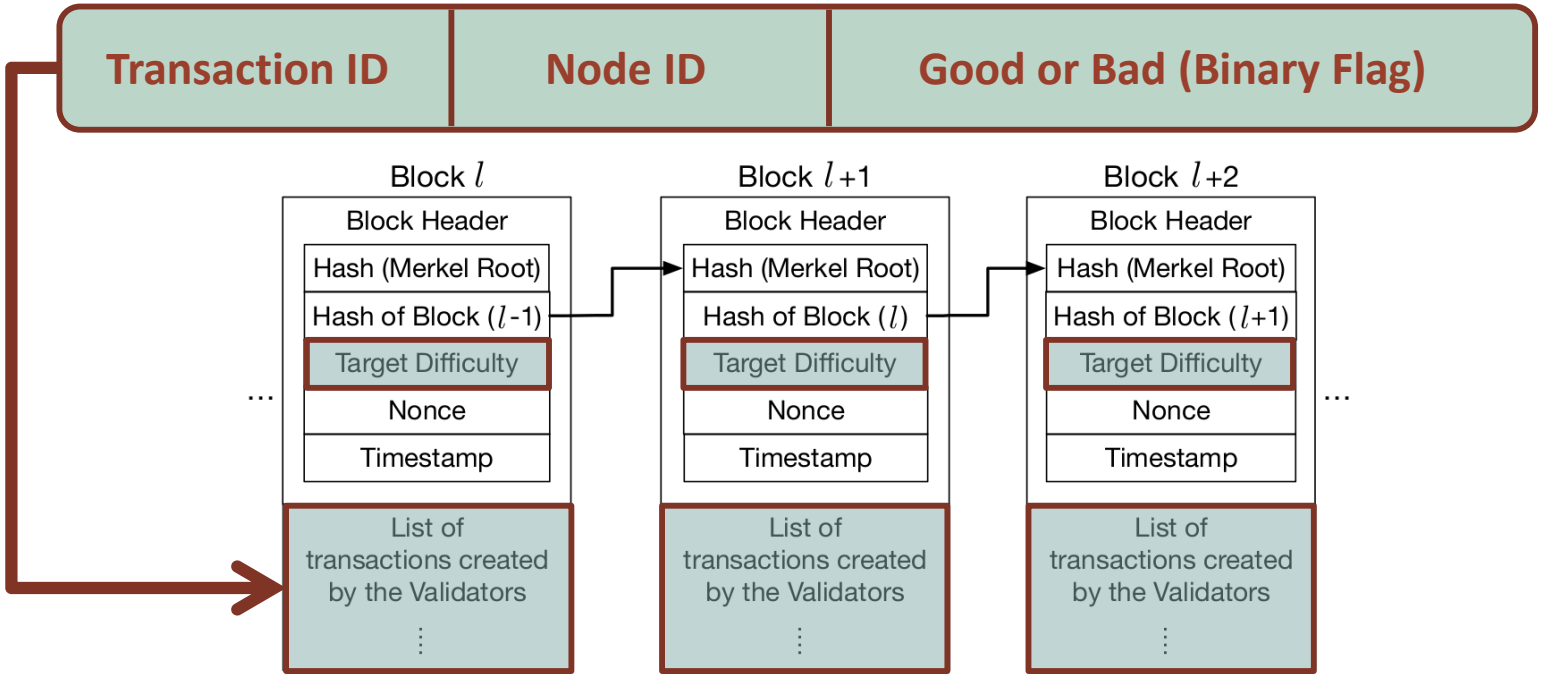
- **Anomaly Detection Module at Miner:**
  - Receive broadcast packets from nodes within grid
  - Detect whether forwarding action of node is Good or Bad: ***WatchDog Module [1]***
- **Outputs:**
  - Node ID (IP address)
  - Binary Flag

$$flag = \begin{cases} 1, & if \quad \text{Good Action} \\ 0, & if \quad \text{Bad Action} \end{cases}$$

[1] S. Marti et. al, "Mitigating routing misbehavior in mobile ad hoc networks," MobiCom '00

II. Blockchain-based Reputation

- Miner creates a transaction for each packet received
- Transactions are aggregated to create a Block with a Difficulty target



A. Difficulty of Mining

- Difficulty: Hardness to find a hash below a target T

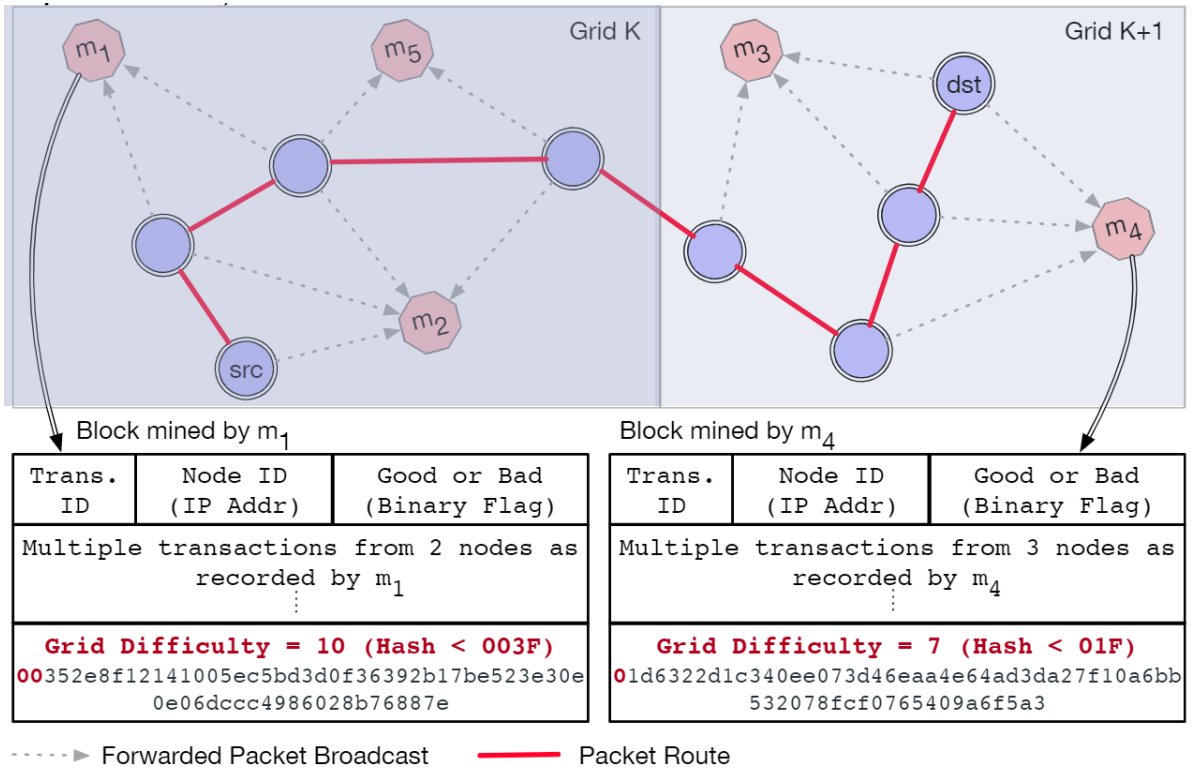
Difficulty

$$D_k = \left\lceil D_{max} \times \frac{|\mathcal{M}_k|}{M} \right\rceil$$

$|\mathcal{M}_k|$ # Sensors in Reception zone of validator

M Total Number of sensors

[Immutability] vs [Low Power & Fast Convergence]

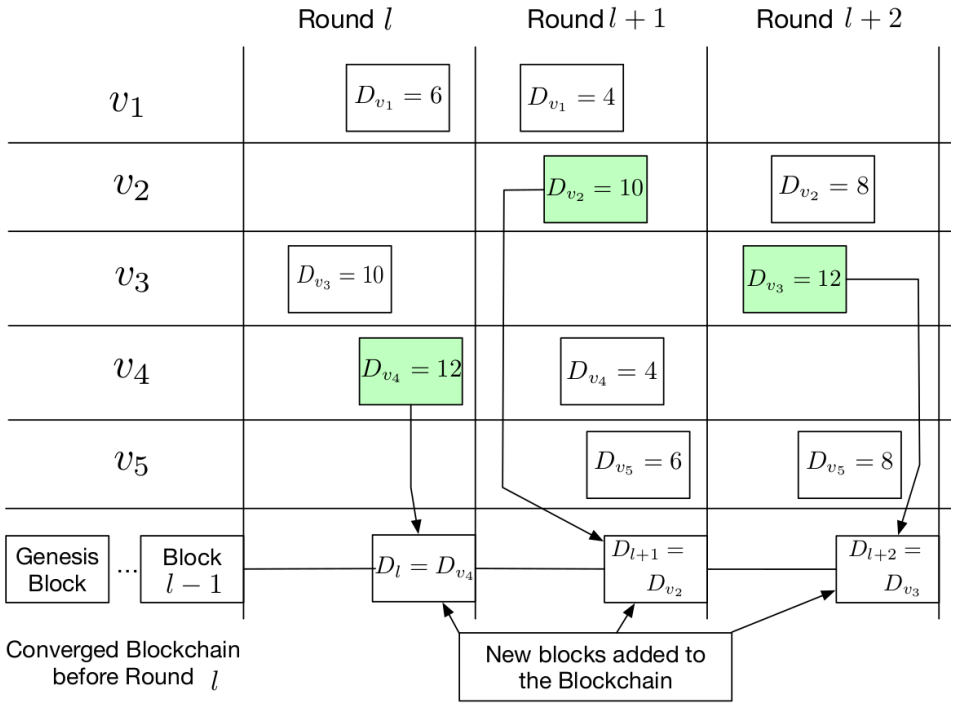


Difficulty ∝ Validation Credibility (Power of the Crowd)

B. Most-Difficult-Chain consensus

- Miners arrive at Consensus on Most-Difficult-Chain
- Miners broadcast this chain to Nodes within its grid

- **Most-Difficult-Chain Consensus [2]:**
  - At each round, the most difficult mined block is added to Blockchain.

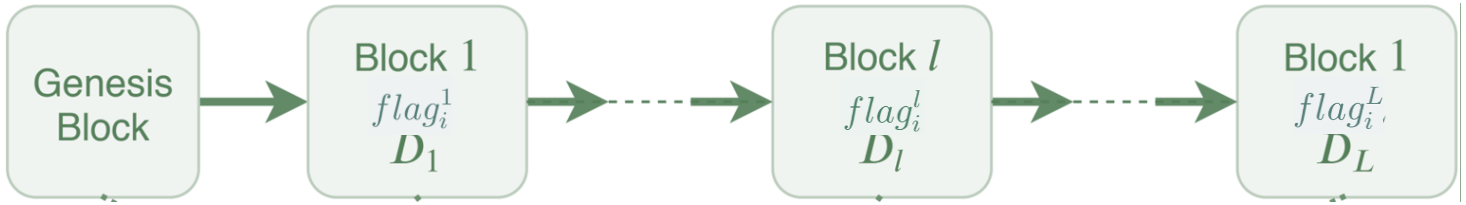


Miners and Nodes get the most credible chain of assessed information

[2] Maqsood and A. Dutta, "SenseChain: Blockchain based Reputation System for Distributed Spectrum Enforcement," IEEE DYSPAN 2019

C. Forwarding Score of a Node

- Miners evaluate the Forwarding Score for each node using Most-Difficult-Chain



$$S_i^l = \frac{|good\ actions|_i^l - |bad\ actions|_i^l}{|good\ actions|_i^l + |bad\ actions|_i^l}$$

$|\cdot|_i^l$ - Count of the type of Action by Node i in Block l

Forwarding Score: Net-Goodness of Routing Behavior of each Node Credibility of Routing

D. Historical Reputation & Provenance

- Miners assess the Reputation for each node using Most-Difficult-Chain and the Scores

$$\eta_i = \frac{\beta}{L.D_{max}} \left(\sum_{l=1}^{L} D^l S_i^l \right)$$

Score of Node i
(Credibility of Routing)

Difficulty of Block l

(Credibility of Validation)

Length of Chain

$$\mathcal{R}_i = \frac{1}{1 + e^{-\eta_i}}$$

Most-Difficult-Chain → Most Credible Reputation Assignment

III. Reputed Routing

- The Cost of a Path is modified to include the reputation of nodes

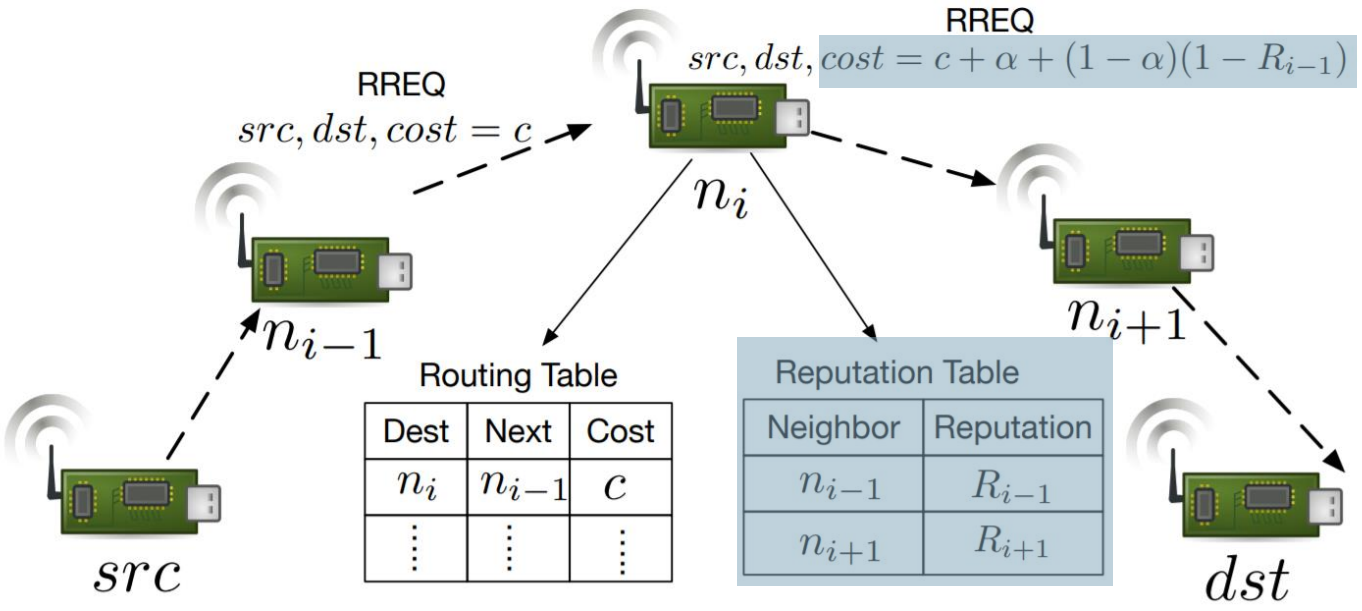
- **Implementation:**
  - RREQ: Route Cost Field, Node List
  - Reputation Table at each Node
  - Each Node allows duplicate pkts

- **Link Cost**
  - Discount the Reputation from Link Cost

$$c(n_i, n_{i+1}) = \alpha + (1-\alpha)(1-\mathcal{R}_i)$$

Hop Count Cost

Reputation Cost



Shortest-Most Reputed Path

- Destination node picks the path with the least Route Cost among all paths

Route Cost

$$c(\mathcal{P}) = \alpha|\mathcal{P}| + (1-\alpha)\left(|\mathcal{P}| - \sum_{n_i \in \mathcal{P}} R_i\right)$$

Number of Nodes in Path

Cumulative Reputation of Path

Shortest-Most Reputed Path

$$\mathcal{P}_{rep} = argmin_{\mathcal{P}}\ c(\mathcal{P})$$

Intrinsic Security: Reputation of node is incorporated by upstream nodes.

IV. Evaluation & Results

Simulation Framework

1) Blockchain Simulator

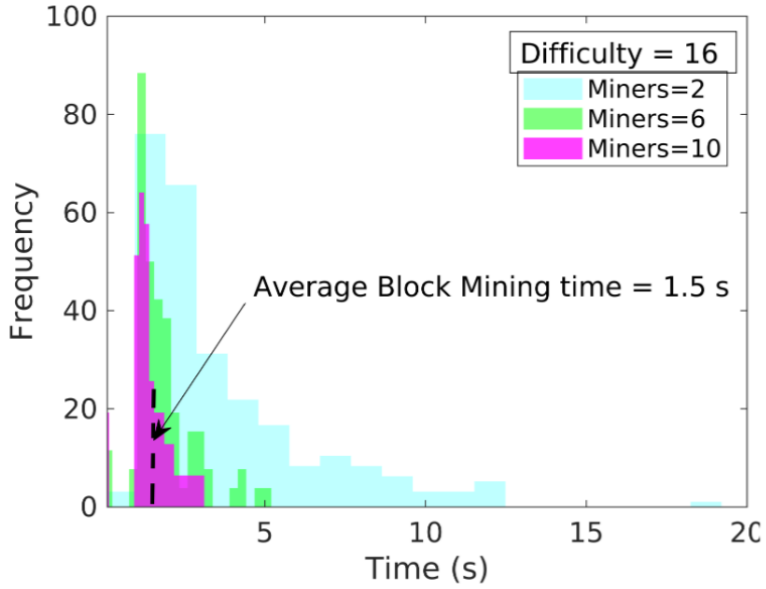
2) MANET Routing Simulator

TABLE I: Simulation Parameters

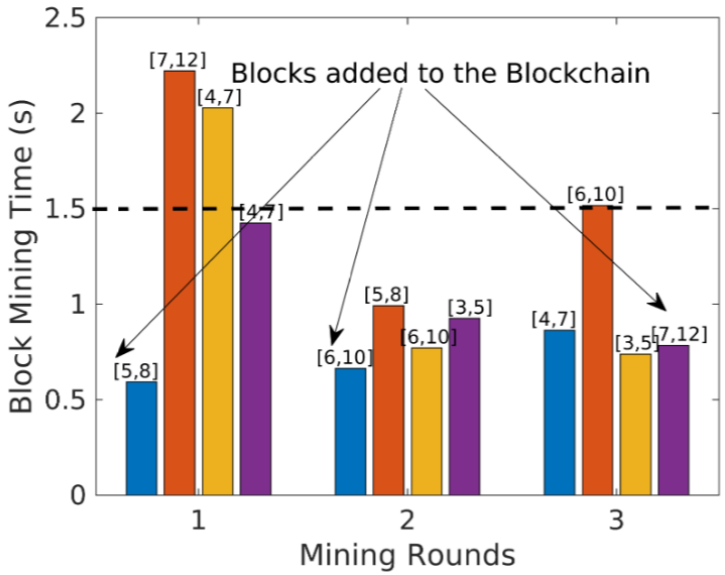
Parameters	Value/Model
Routing Protocol	AODV
Traffic Type	Constant bit rate (CBR)
Transmission Range	30 m
Node Distribution	Uniform Distribution
Mobility Model	Random Waypoint
Area	100m $\times$ 100m
Grid Size	50 m
Number of Nodes (N)	30
Number of Miners (M)	[10, 20]
Cryptographic Hash Function	SHA-256
Maximum Difficulty (D_{max})	16
Tuning parameter (α)	0.5

A. Blockchain Performance

Block mining times of Grids with # Miners



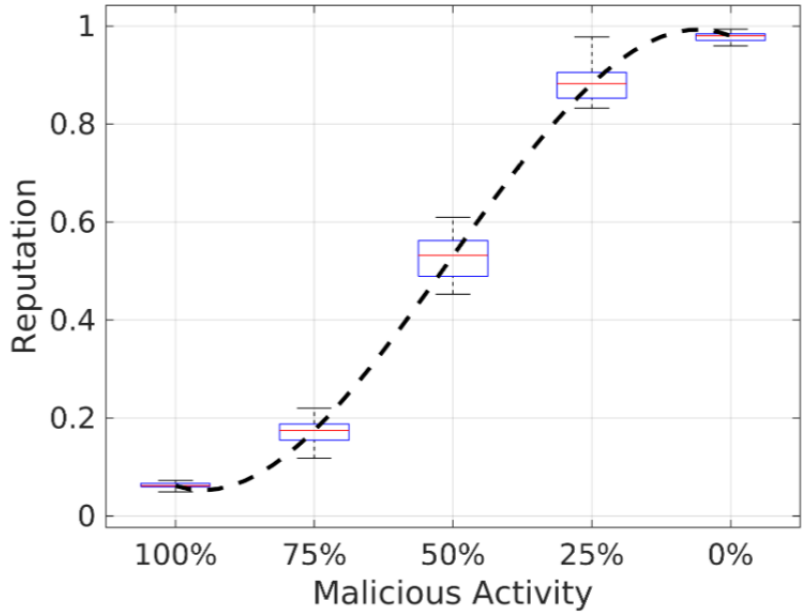
Mining time per Grid & winning block in each round



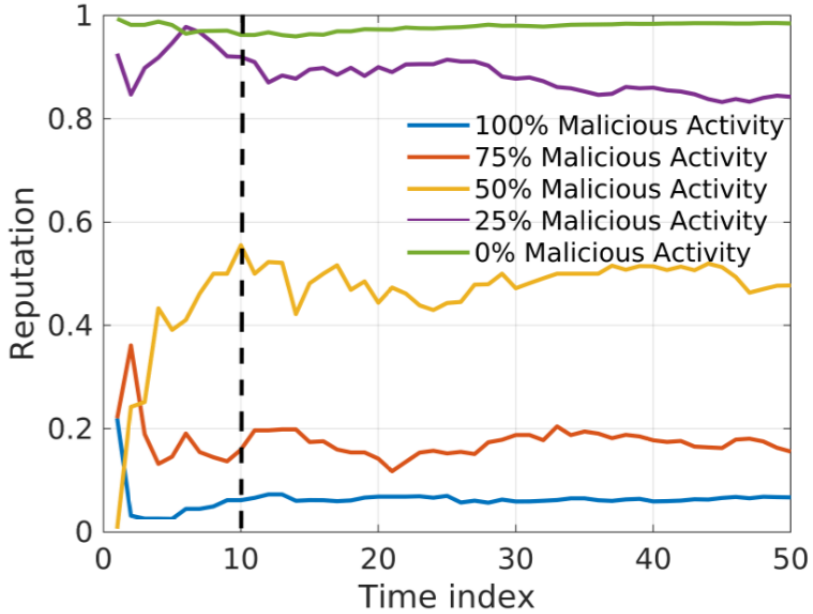
The Most credible Mined Block is added to the Blockchain is each round

B. Reputation Assignment

Reputation with degree of Maliciousness



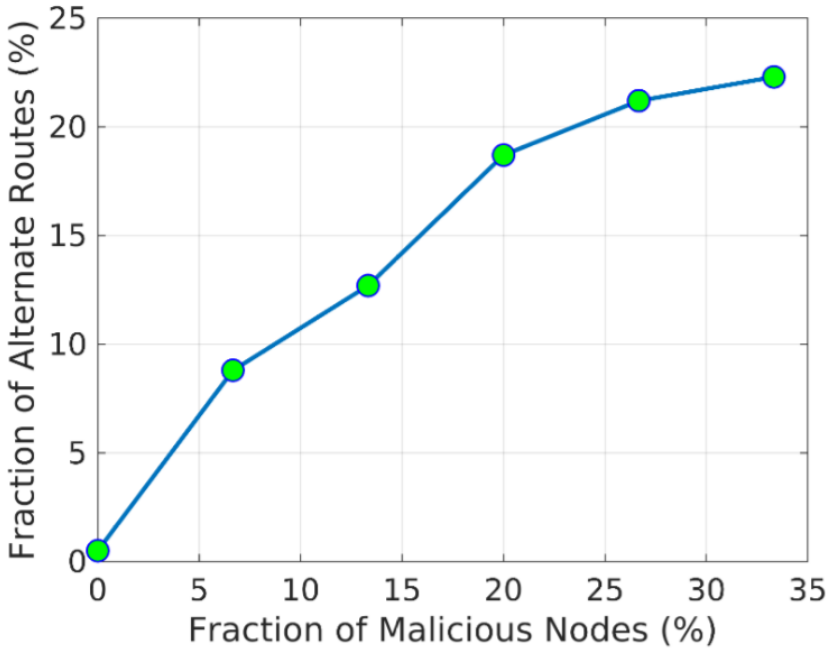
Reputation of Malicious Nodes over time



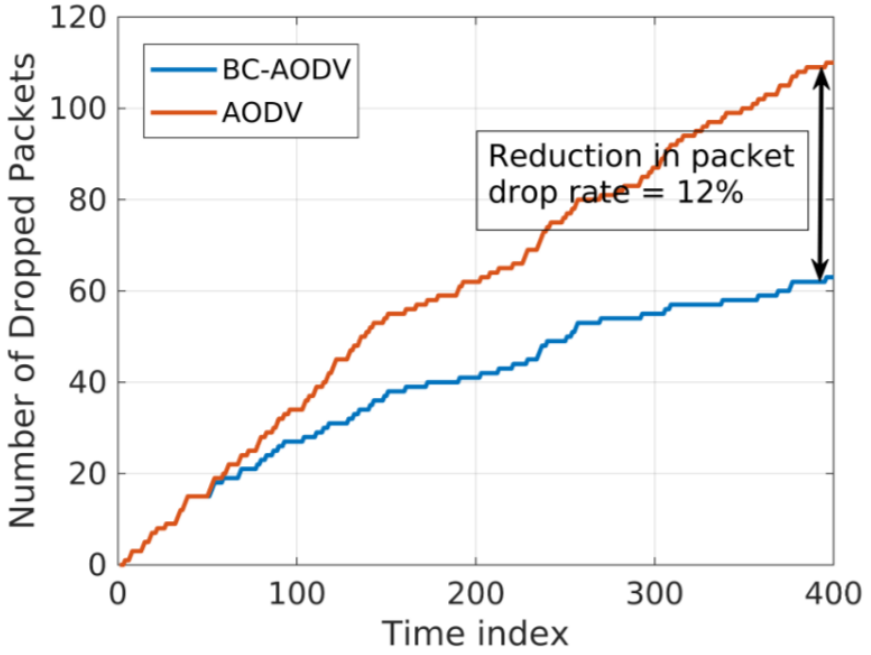
Reputation of Nodes represents the Degree of Maliciousness of Nodes

C. Routing Performance

Fraction of route alterations from AODV



Cumulative sum of packets dropped over time



Shortest-Most Reputed Path Routing Reduces the Packet Drop Rate

Conclusion

1. **Novel Blockchain Design:** Captures Routing Credibility and Validation Credibility

2. **Nonlinear Reputation Metric:** Aggregation of historical Scores and Difficulty

3. **Reputed Routing Scheme:** Shortest, Most Reputed Path Routing

Reputed Routing based on Reputation accrued via a Most-Difficult-Blockchain

Thank You

FEEDBACK & QUESTIONS