AUTHREX SYSTEMS

Simulation User Guide

AUTHREX Distributed Kernel

8-Node Actor Model — Master Pulse TTP Architecture

FIELD	VALUE
Document	Simulation User Guide
Version	1.0 — March 31, 2026
Filename	authrex-distributed-kernel.html
File Size	21 KB
Dependencies	THREE.js r128 (CDN), Web Workers (8), WebCrypto API
Browser	Chrome 90+ / Edge 90+ (WebGL + WebCrypto required)
Author	Burak Oktenli — Georgetown University
ORCID	0009-0001-8573-1667
License	CC BY 4.0 International

1. PREREQUISITES

Before opening this simulation: (1) Use Chrome 90+ or Edge 90+ (recommended). Firefox and Safari may have WebGL differences. (2) Ensure internet connectivity — this simulation loads THREE.js from a CDN. Without internet, the 3D visualization will show a fallback message but the governance engine continues. (3) Open the HTML file directly in the browser (double-click the file or drag into Chrome). No web server is required. (4) Allow the page to fully load before interacting with controls.

2. QUICK START

Open in Chrome. An 8-node distributed system loads with a 3D COP and telemetry display. This simulation uses a Master Pulse Time-Triggered Protocol (TTP) — workers are purely reactive to SYNC_PULSE from the master thread. Click one of the three scenario buttons (CASE RED, CASE AMBER, or CASE BLACK) to begin.

3. STEP-BY-STEP WALKTHROUGH

CASE RED — Byzantine Node

Single node exhibits Byzantine behavior. Tests 8-node PBFT with Master Pulse TTP.

Step 1: Click ▶️ CASE RED: BYZANTINE SPOOF button — Single-click button — no dropdown. Immediately starts the scenario.

Step 2: Click the scenario button — The selected scenario activates immediately. One of 8 nodes receives EW compromise signal via Master Pulse.

- ▶️ **Observe:** One node wireframe turns RED in 3D COP
- ▶️ **Observe:** Trust (tau) begins decaying in telemetry row for that node
- ▶️ **Observe:** ACI drops proportionally
- ▶️ **Observe:** SHA-256 state pin updates in provenance display
- ▶️ **Observe:** Pipeline: SATA → SPIKE, HMAA → ESCALATION

Step 3: Watch PBFT evaluation — Master thread evaluates consensus at 20Hz. With 1/8 nodes compromised, threshold (>2/3) is NOT met.

- ▶️ **Observe:** ESC count: 1/8 — below PBFT threshold
- ▶️ **Observe:** CARA does not auto-fire (1/8 < 2/3)
- ▶️ **Observe:** P(Escalation) rises but stays manageable

Step 4: Watch for PBFT auto-quarantine — If consensus threshold (>2/3) is breached, the system automatically quarantines the node.

- ▶️ **Observe:** Node turns grey/dimmed (QUARANTINED)
- ▶️ **Observe:** Auth = 0, Trust = 0.01
- ▶️ **Observe:** Pipeline: CARA → FTS
- ▶️ **Observe:** SHA-256 hash updates to reflect new state

CASE AMBER — EW Jamming

EW jamming degrades a node without Byzantine compromise. Shows DEGRADED state (amber, distinct from red).

Step 1: Click ▶️ CASE AMBER: THEATER JAMMING button — Single-click button. EW jamming signal sent to target node.

- ▶️ **Observe:** Node wireframe turns AMBER (not red)
- ▶️ **Observe:** State shows DEGRADED (distinct from COMPROMISED)
- ▶️ **Observe:** Trust decays more slowly than Byzantine case
- ▶️ **Observe:** Visual difference: amber = degraded capability, red = hostile intent

Step 2: Compare to CASE RED visually — The DEGRADED state uses amber coloring to show reduced capability without Byzantine hostility.

- ▶️ **Observe:** Amber wireframe = degraded sensors/comms
- ▶️ **Observe:** Red wireframe = active Byzantine behavior
- ▶️ **Observe:** This distinction drives proportional governance response

Step 3: Watch for auto-quarantine or reload to reset — The system may auto-quarantine via PBFT, or reload the page to reset.

- ▶️ **Observe:** Authority revoked. Node isolated from mesh.
- ▶️ **Observe:** Remaining 7 nodes continue with Master Pulse TTP

CASE BLACK — C2 Node Compromise

Highest-authority node compromised. Tests governance response to Tier-3 breach.

Step 1: Click ▶️ CASE BLACK: C2 ATTRITION button — Single-click button. C2-level node receives compromise signal.

- ▶️ **Observe:** High-authority node turns RED
- ▶️ **Observe:** Cascade risk elevated — C2 node has outsized weight in P(esc)
- ▶️ **Observe:** PBFT evaluation intensifies — remaining nodes detect authority gap
- ▶️ **Observe:** Pipeline: HMAA → ESCALATION, FLAME → CRITICAL

Step 2: Watch cascade dynamics — Loss of C2 node disrupts the authority hierarchy across the 8-node mesh.

- ▶️ **Observe:** DDS messages from C2 node contain compromised state data
- ▶️ **Observe:** Peer nodes adjust their own ACI based on C2 compromise
- ▶️ **Observe:** P(Escalation) rises sharply due to C2's high authority weight

Step 3: Watch cascade + auto-quarantine — C2 compromise cascades through the mesh. PBFT may auto-quarantine.

- ▶️ **Observe:** Authority = 0. Node isolated.
- ▶️ **Observe:** Mesh reorganizes under degraded authority structure
- ▶️ **Observe:** Seeded LCG ensures this exact sequence is deterministically reproducible

4. INTERFACE REFERENCE

4.1 Dashboard Metrics

METRIC	RANGE	MEANING
Node trust	0.00 - 1.00	SATA trust score per node
ACI	0.00 - 1.00	Authority Confidence Index per node
State	NOM/COMP/DEGR/ QUAR	Governance state with DEGRADED as distinct from COMPROMISED
SHA-256 pin	Hex string	State hash pinned via WebCrypto SHA-256

4.2 Controls

BUTTON	FUNCTION
▶️ CASE RED: BYZANTINE SPOOF	Single-click: inject Byzantine compromise into one node
▶️ CASE AMBER: THEATER JAMMING	Single-click: deploy EW jamming (DEGRADED state, amber)
▶️ CASE BLACK: C2 ATTRITION	Single-click: compromise highest-authority C2 node
Note: No manual CARA button	CARA triggers automatically via PBFT consensus when threshold (>2/3) is crossed
↺ RESET (page reload)	Reload page to terminate all 8 workers and respawn

4.3 ERAM Pipeline Indicators

The pipeline banner at the top of the screen shows 6 BLADE governance modules. Each indicator changes color based on simulation state:

COLOR	STATE	MODULES	MEANING
Green	NOMINAL	All modules	System operating within normal bounds
Amber	WARNING	MAIVA, ADARA	Anomaly detected, monitoring escalation
Red	CRITICAL	SATA, HMAA, CARA, FLAME	Compromise detected or interlock active

4.4 Node States

STATE	COLOR	MEANING
NOMINAL	Green	Normal operation
COMPROMISED	Red	Byzantine behavior detected
DEGRADED	Amber	EW jamming — reduced capability but not Byzantine
QUARANTINED	Grey	CARA interlock — isolated from mesh

5. WHAT SUCCESS LOOKS LIKE

This simulation demonstrates the most architecturally pure distributed system in the portfolio: 8 independent Workers with NO internal timers — all timing comes from Master Pulse TTP sync signals. This eliminates clock drift between nodes.

Key differentiator: the DEGRADED state (amber) is distinct from COMPROMISED (red). EW jamming reduces capability but does not indicate Byzantine behavior — the governance response is proportional to the threat type. This distinction is unique to this simulation.

The seeded LCG (seed*1664525+1013904223 >>> 0) ensures every run is deterministically reproducible for verification.

6. TROUBLESHOOTING

PROBLEM	SOLUTION
Black screen / no 3D	Requires internet for THREE.js CDN. Use Chrome with WebGL enabled.
Buttons don't respond	Buttons enable in sequence (phase guards). Follow the numbered steps in this guide.
Hash shows N/A	WebCrypto requires HTTPS or localhost. Open via file:// in Chrome.
Pipeline banner missing	Scroll to top. Banner is fixed-position. Check if boot animation is still playing.
Page feels slow	Close DevTools. Reduce browser tabs. Ensure GPU acceleration is enabled in browser settings.

END OF GUIDE