AC-IA

SECURING OFFLINE BLOCKCHAIN: MITIGATING MITM ATTACK ON NONET

16010123019: Aditi Kanagala
16010123064: Sofian Chicktay
16010123256: Rishi Shanbhag
16010123268: Viraj Bhartiya
16010123325: Shreyans Tatiya

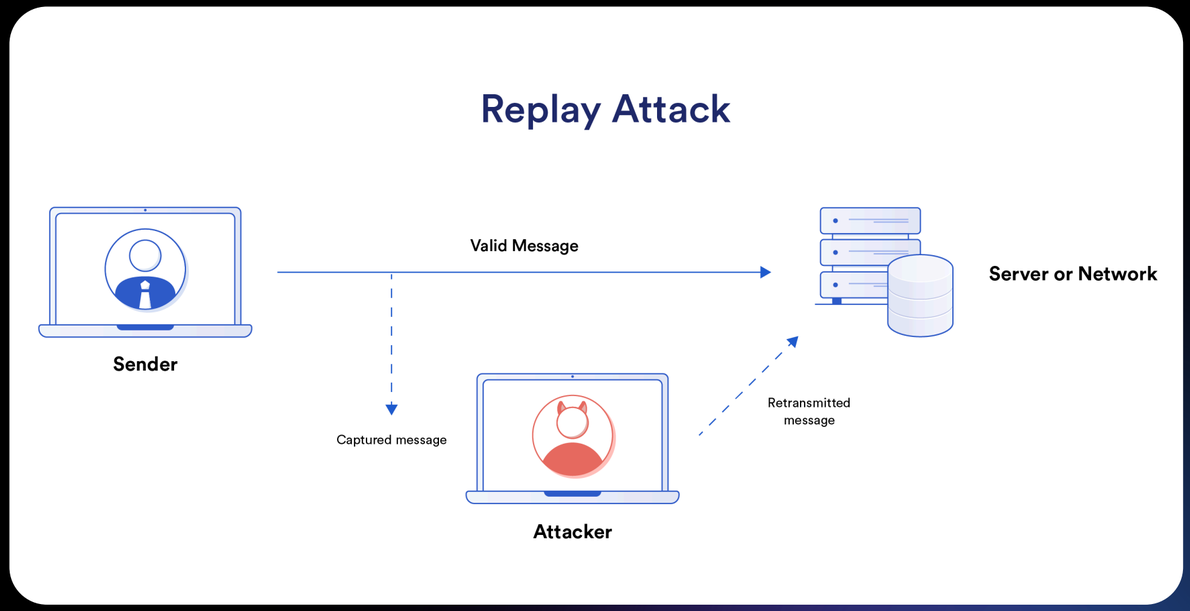
AC-IA

INTRODUCTION

NONET PROTOCOL AND THE MITM THREAT

NONET is an innovative, decentralized mesh network protocol enabling cryptocurrency transactions in environments without reliable internet access. It leverages Bluetooth Low Energy (BLE) to relay fragmented transaction packets until they reach a gateway node connected to the blockchain.

- Architecture: Peer-to-peer relay using BLE mesh.
- Function: Offline-first blockchain transactions.
- Benefit: Enhances financial inclusion and emergency resilience.



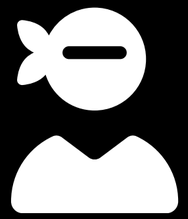
However, this reliance on BLE mesh makes the protocol uniquely susceptible to Man-in-the-Middle (MITM) attacks, compromising transaction integrity and user privacy.

AC-IA

MITM ATTACK TIMELINE

A successful MITM attack exploits the protocol's multi-hop nature, initiating from device discovery and culminating in the submission of a fraudulent transaction.

Originator / Relay Nodes
Initiate and forward fragmented transaction packets.



Attacker (MITM Actor)
A malicious entity in BLE range capable of interception and data modification.

Gateway Nodes
Internet-connected nodes that submit the transaction to the public blockchain network.

Device Discovery & Pairing

Interception & Modification

Forwarding & Submission

AC-IA

TECHNICAL VULNERABILITIES

NONET’s design, while innovative, faces challenges due to the underlying Bluetooth Low Energy (BLE) constraints and its packet fragmentation system.

BLE Vulnerabilities

BLE communications operate at 2.4 GHz, typically within a 100-meter range. Weak or legacy pairing modes (like "Just Works") allow attackers to impersonate devices and intercept cryptographic keys, compromising the transmission.

Packet Fragmentation Impact

This fragmentation exponentially increases the attack surface for a MITM adversary, creating multiple opportunities for:

- Packet sniffing and interception.
- Delay or loss attacks.
- Insertion of malicious fragments.

Lack of E2E Encryption

Crucially, without an application-layer, end-to-end encryption layer, fragmented packets are exposed to tampering during relaying, threatening data integrity across the multi-hop network.

AC-IA

IMPACT OF MITM ATTACKS

Financial Theft

The consequences of successful MITM attacks extend beyond immediate financial loss, threatening the viability of offline decentralized finance.

Privacy Exposure

Exposure of sensitive transaction metadata, leading to potential deanonymization and linking of physical devices to blockchain identities.

Legal & Regulatory Risks

Increased liability for gateway nodes; potential regulatory penalties under AML/KYC frameworks due to unverified transactions.

Systemic Risk

Exploitation of mesh networks to disrupt critical financial flows during conflict or disasters, introducing systemic instability.

AC-IA

DETECTION & RESPONSE

Detection Methods

- Anomaly Detection: Monitor unusual packet delays, duplicates, or ACK inconsistencies.
- Signature Verification: Use ECDSA validation to reject tampered packets.
- Consensus Checks: Cross-verify transactions across multiple relay nodes.
- Transaction Monitoring: Log suspicious submission patterns for forensic analysis.

Response Strategies

- Enforce Secure BLE Pairing with authenticated key exchange.
- Patch Firmware to fix known BLE issues (e.g., BIAS attacks).
- Add End-to-End Payload Encryption with MACs for data integrity.
- Use Multi-Path Validation to confirm transactions via multiple routes.
- Alert Users on suspicious or failed attempts.
- Fallback to Internet nodes for extra validation where possible.

Incident Handling

- Quarantine suspicious nodes.
- Log & Report detected MITM attempts.
- Reset/Re-authenticate network after compromise.

AC-IA

LESSONS & DEFENSES

Secure Pairing & Encryption

Use Numeric Comparison / Passkey pairing to block silent MITM.
Add App-level Encryption & Digital Signatures for end-to-end security.
Manage Nonces Securely — cryptographic RNG, short validity, duplicate rejection.

Network Hardening

Mesh Security: Limit hops, use reputation scoring, diversify paths.
Gateway Protection: TLS + pinning, RPKI, DNSSEC, HSTS, API audits.
Certificate Transparency: Monitor logs, auto-alert, revoke compromised certs

Avoid Weak Links

Phase out legacy protocols with known flaws.
Regularly update BLE & crypto libraries.
Test backward compatibility only in isolated setups.

User Awareness

Train users on secure pairing & identity verification.
Warn against untrusted devices & fake requests.

AC-IA

CONCLUSION

The NONET protocol holds immense potential for expanding financial access, but its security relies on proactive mitigation of BLE-based MITM threats.

CRYPTOGRAPHIC INTEGRITY

Application-level encryption and digital signatures.

ENHANCED AUTHENTICATION

Enforcing secure BLE pairing modes (Passkey/Numeric Comparison).

GATEWAY PROTECTION

Using RPKI, DNSSEC, and TLS for secure internet submission.

RESILIENT ARCHITECTURE

Multi-path validation and reputation scoring for relay nodes.