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

IA-2: Man-in-the-Middle (MITM) Attacks on NONET: A Decentralized Mesh Network Protocol for Offline Blockchain Transactions

Abstract

NONET is an innovative decentralized mesh network protocol designed to enable blockchain transactions in offline environments through Bluetooth Low Energy (BLE) communication. It employs a sophisticated packet fragmentation and reassembly system, allowing cryptocurrency transactions to propagate via peer-to-peer relay until reaching a gateway node with internet access, which then broadcasts the transaction to the blockchain. The system's architecture supports multi-chain compatibility, offline-first operation, and integration with meta-transaction standards like EIP-3009.

However, despite its promising design, NONET's reliance on BLE mesh technology introduces potential security vulnerabilities, notably susceptibility to man-in-the-middle (MITM) attacks. Such attacks can intercept, alter, or replay transaction packets during relaying, threatening transaction integrity, user privacy, and overall network security. This report explores the system's architecture, identifies the inherent security flaws, and recommends mitigation strategies to safeguard against MITM threats in decentralized offline blockchain networks.

1. Introduction

NONET is an innovative mesh networking protocol aimed at enabling blockchain transactions in environments without reliable internet access, utilizing BLE to relay transaction packets across devices until a gateway node submits them to the blockchain. While the design offers distinct advantages for financial inclusion and emergency use cases, the protocol’s reliance on BLE and mesh topology opens new cybersecurity challenges, notably man-in-the-middle (MITM) attacks.

Man-in-the-middle attacks threaten the confidentiality, integrity, and authenticity of transaction data by intercepting, modifying, or replaying transaction messages as they traverse the mesh. This report undertakes a thorough analysis of such threats to inform secure protocol deployment and operational posture.

2. Timeline of Events and Actor Roles in MITM Attacks

2.1 Actor Roles

- Originator: The user device initiating a new blockchain transaction.
- Relay Nodes: Intermediate devices forwarding fragmented transaction packets.
- Gateway Nodes: Internet-connected nodes that submit transactions to the blockchain network.
- Attacker (MITM Actor): Malicious entity who gains interception capabilities within the BLE mesh transmission range.

2.2 Attack Timeline

Stage	Description	Actors Involved	Attack Vector
1. Device Discovery	Attacker scans for active BLE devices participating in NONET.	Attacker, Relay Nodes	Passive reconnaissance.
2. Pairing/Connection	Establishes BLE connections, sometimes exploiting weak pairing.	Attacker, Victim Node	Exploiting unauthenticated pairing protocols.
3. Interception	Captures transmitted packet fragments in real-time.	Attacker	Packet sniffing and proxying.
4.Modification/Replay	Alters or replays packet fragments undetected.	Attacker	Packet injection or delay manipulation.

5. Transaction Forwarding	Forwards manipulated packets downstream toward the gateway.	Attacker, Gateway Node	Transparent proxy or attack relay.
6. Blockchain Submission	Gateway submits potentially tampered transactions on-chain.	Gateway Node, Blockchain	Final step, possible fraudulent transaction.

2.3 Summary

The MITM attacker leverages proximity and weak BLE security during initial pairing and uses the mesh's multi-hop architecture to intercept and relay message fragments, posing a significant ongoing threat throughout the lifecycle of a transaction.

3. Technical Mechanism of Interception

3.1 BLE Vulnerabilities

Bluetooth Low Energy (BLE) communications operate at 2.4 GHz with a constrained 31-byte payload necessitating message fragmentation. The fundamental BLE security challenges that expose NONET include:

- Weak or legacy pairing modes: Without authenticated pairing (e.g., using Just Works mode), attackers can impersonate devices and intercept keys.
- Lack of end-to-end encryption at application layer: Fragmented packets may be exposed to sniffing and tampering during transmission.
- Proximity Requirement: BLE range (~100 meters open space) confines attacks to nearby malicious actors, facilitating hands-on MITM capabilities.

3.2 Fragmentation Impact

NONET fragments messages into up to 127 packets of 11-byte payload. This fragmentation increases the number of opportunities for packet loss, delay, or insertion attacks by a MITM adversary.

3.3 Replay and Modification

An attacker can:

- Capture fragments of the transaction and replay them later, attempting to confuse nodes or cause transaction duplication.
- Modify packet payloads before forwarding, leading to altered transaction values, destinations, or signatures.

3.4 Exploiting Protocol Stack Weaknesses

MITM exploits can occur at:

- Physical/Transport Layers: Packet sniffing and signal jamming.
- Protocol Layer: Forging packet headers (ID, chunk index) to disrupt reassembly.
- Application Layer: Injecting malicious payloads or fake acknowledgement packets to confuse network state management.

4. Impact of MITM Attacks

4.1 Financial Impact

- Unauthorized manipulation or theft of cryptocurrency funds.
- Transaction rollbacks or double spends through replay attacks.
- Loss of user trust, dampening cryptocurrency adoption in offline scenarios.

4.2 Privacy Implications

- Exposure of transaction metadata, such as sender/receiver addresses and values.
- Potential deanonymization or correlation attacks linking blockchain identities to physical devices.
- Loss of transaction-level pseudonymity.

4.3 Legal and Regulatory Risks

- Liability risks for intermediaries or gateway nodes failing to prevent fraud.
- Increased scrutiny under AML/KYC and transaction monitoring frameworks.
- Potential regulatory penalties in jurisdictions with strict financial compliance.

4.4 National Security Concerns

- Exploitation of mesh networks for disrupting critical financial flows during disasters or conflict.
- Potential for adversarial actors to undermine humanitarian aid distribution reliant on NONET.
- Introduction of systemic risks in decentralized financial infrastructures.

4.5 Case Studies Referenced

- BLE impersonation attacks exploited in consumer devices (2021) illustrate the ease of MITM interception in uncontrolled environments.
- Blockchain-based attacks involving transaction interception underscore the necessity of strong cryptographic assurances.

5. Detection and Response

5.1 Detection Methods

- Anomaly Detection: Monitoring for unusual packet delays, duplicated fragments, or inconsistent acknowledgments.
- Signature Verification: Leveraging ECDSA signature validation to reject tampered packets.
- Consensus Checks: Cross-verifying transactions across multiple relay nodes.
- Transaction Monitoring: Gateway nodes logging suspicious submission patterns for forensic analysis.

5.2 Response Strategies

- Strengthening BLE Pairing: Enforce Secure Connections with authenticated key exchange.
- Firmware Updates: Patch known BLE vulnerabilities such as BIAS attacks.
- End-to-End Payload Encryption: Augment NONET protocol with encrypted payload data and MACs to ensure integrity.
- Multi-Path Validation: Implement systems where multiple independent transmissions confirm a transaction before acceptance.
- User Alerts: Notify users of suspicious or failed transaction attempts.

- Fallback on Internet: Where available, cross-check transactions with internet-connected nodes for validation.

5.3 Incident Case Handling

- Quarantine of suspicious nodes.
- Logging and reporting detected MITM attempts.
- Coordinated network-wide state resets or re-authentication after detected compromise.

6. Lessons and Defenses

6.1 Practical Security Recommendations

1. Use of Secure BLE Pairing Modes
    - Prefer Numeric Comparison or Passkey Entry over “Just Works”.
    - These methods involve user confirmation, blocking silent MITM (Man-in-the-Middle) attacks.
    - Ensure both devices verify the same numeric code or passkey before completing pairing.
2. End-to-End Encryption and Signing
    - Add an extra cryptographic layer on top of BLE’s built-in encryption.
    - Use application-level encryption to maintain data privacy even if BLE encryption is compromised.
    - Sign all critical messages digitally to validate authenticity and integrity.
3. Strong Nonce Management
    - Generate nonces using cryptographically secure random number generators.
    - Assign short validity windows to prevent reuse in replay attacks.
    - Implement nonce tracking to reject duplicates instantly.
4. Mesh Network Hardening
    - Limit the number of communication hops to reduce potential attack points.
    - Use reputation scoring to classify and trust relay nodes based on consistent and correct forwarding.
    - Introduce path diversification so data doesn’t always follow the same route through the mesh.
5. Gateway Node Security

    - Secure BLE–Blockchain or BLE–Internet gateways using layered protections:
        - Use TLS with certificate pinning to verify server identities.
        - Apply RPKI to validate routing paths and prevent BGP hijacking.
        - Implement DNSSEC to secure DNS queries from spoofing.
        - Enforce HSTS to block insecure HTTP downgrade attempts.
    - Regularly audit gateway APIs linked to blockchain nodes.
6. Certificate Transparency
    - Monitor certificate transparency logs to detect suspicious or fraudulent certificates issued for gateways.
    - Enable automated alerts for unauthorized certificate issuance.
    - Revoke compromised certificates immediately to prevent network impersonation.
7. Avoiding Legacy Protocols
    - Phase out outdated cryptographic protocols with known vulnerabilities.
    - Regularly review and update to newer secure versions of BLE and cryptographic libraries.
    - Test backward compatibility only in controlled, isolated environments.
8. User Education
    - Train users to understand secure pairing practices.
    - Warn against pairing with unknown or untrusted devices.
    - Educate users to verify device identities and accept only legitimate connection requests.

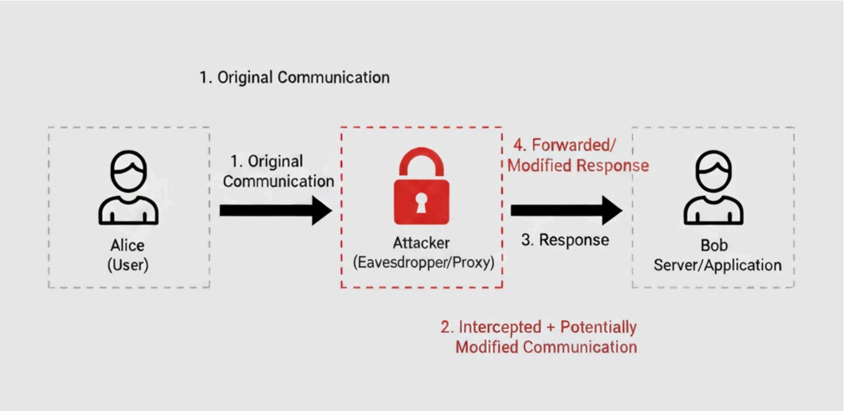
6.2 References to Standards and Technologies

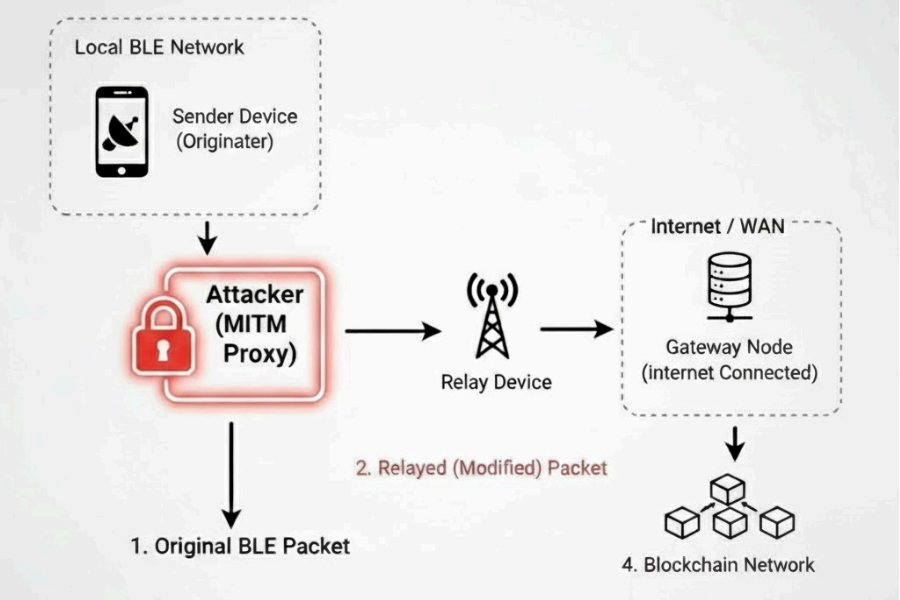
1. Bluetooth Core Specification v5.1 — Defines secure BLE pairing, authentication, and encryption mechanisms.
2. EIP-3009 — Standard for secure meta-transactions in blockchain systems, providing built-in replay protection.
3. RPKI (Resource Public Key Infrastructure) — Ensures routing origin validation to prevent BGP prefix hijacks.
4. DNSSEC (Domain Name System Security Extensions) — Adds cryptographic signatures to verify DNS responses.
5. HSTS (HTTP Strict Transport Security) — Forces browsers and APIs to use HTTPS, eliminating downgrade risks.
6. Secure SIM Provisioning — Enhances device identity binding through authenticated SIM credentials.

7. Multi-Path Validation Mechanisms — Diversify and verify network routes to strengthen trust and prevent single-point failures.

7. Diagrams and Threat Model

7.1 Basic MITM Attack Diagram





7.2 Threat Model Summary

- Adversary Model: Local, active MITM attacker with proximity to BLE mesh devices, capable of packet interception, replay, and injection.
- Assets at Risk: Transaction authenticity, confidentiality, and timely receipt.
- Attack Surface: BLE pairing mechanisms, packet fragmentation protocols, relay nodes, gateway API communications.
- Defenses: Authentication at pairing, encryption/signing, nonce validation, multi-path consensus.

8.Conclusion

The NONET protocol transforms blockchain transaction capabilities by enabling offline operations over a BLE mesh network, fostering financial inclusion and emergency resilience. However, to realize this potential securely, rigorous defenses against man-in-the-middle attacks are imperative. By combining strong BLE pairing security, cryptographically verified transaction messaging, multi-path validation, and robust gateway protections, NONET can mitigate MITM risks effectively, preserving trust in offline decentralized finance.

9. Bibliography

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
3. EIP-3009: Transfer With Authorization, Ethereum Improvement Proposals (2020).
4. Bluetooth SIG (2019). Bluetooth Core Specification Version 5.1.
5. RFC 6550 (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.
6. Carnegie Mellon University CERT Advisory (2021). Bluetooth Impersonation and BIAS Attacks.
7. EC-Council (2025). Man-in-the-Middle Attack Awareness and Defense.
8. Kaspersky Resource Center (2017). Defending Yourself from Man-in-the-Middle Attacks.
9. Punchthrough (2025). BLE Security: Where to Begin.
10. GoodAccess Blog (2025). Defending Against Man-in-the-Middle Attacks.