IOT(CS366) Course Project

Design and Evaluation of Mitigation Techniques for DIO Replay Attacks in Static RPL Networks

Team:

Sivvala Vineela (221CS155)

Sthuthi S (221CS156)

Varahi Suvarna (221CS259)

Date: 10 November 2025

Abstract

Our project introduces a lightweight mitigation approach against Destination-Oriented Directed Acyclic Graph (DODAG) Information Object (DIO) replay attacks in the Routing Protocol for Low-Power and Lossy Networks (RPL). The technique utilizes behavioral analysis and version-based detection optimized for static (non-mobile) IoT environments. Experimental results from Contiki-NG indicate a 99.8% replay detection accuracy while preserving network stability. During continuous attack scenarios, the protected network sustained valid DODAG formation (rank: 384, 2 neighbors), whereas the unprotected baseline network failed to establish connectivity (rank: 0, 0 neighbors). The proposed solution incurs minimal overhead, with only a 4–5% increase in energy consumption, and remains compatible with resource-constrained IoT devices, demonstrating its practicality for real-world deployment.

---

1. Introduction

1.1 Background

The Internet of Things (IoT) has transformed global connectivity by allowing billions of resource-constrained devices to interconnect over Low-Power and Lossy Networks (LLNs). The Routing Protocol for Low-Power and Lossy Networks (RPL), standardized in RFC 6550, has emerged as the de facto routing standard for these networks. RPL builds a Destination-Oriented Directed Acyclic Graph (DODAG), enabling nodes to self-organize into a hierarchical tree structure rooted at a central sink node.

1.2 Problem Statement

The Routing Protocol for Low-Power and Lossy Networks (RPL) is susceptible to control message exploitation, particularly through DODAG Information Object (DIO) replay attacks. In this attack, an adversary intercepts and retransmits legitimate DIO messages at a later time or from a different location. Such malicious activity can severely affect network performance and reliability, leading to the following issues:

- Network instability resulting from frequent parent changes and rank oscillations
- Resource exhaustion due to excessive control message overhead
- Topology disruption caused by the formation of incorrect DODAG structures
- Complete network failure where nodes are unable to establish valid connectivity

1.3 Motivation

Existing security mechanisms for the Routing Protocol for Low-Power and Lossy Networks (RPL), as defined in RFC 6550, primarily depend on cryptographic authentication. While effective against unauthorized message injection, these methods exhibit several limitations:

- Dependence on pre-shared keys or Public Key Infrastructure (PKI) management
- High computational and memory overhead unsuitable for constrained IoT devices
- Inability to prevent the replay of previously authenticated messages
- Limited compatibility with legacy or heterogeneous deployments

These challenges highlight the need for lightweight, non-cryptographic mitigation approaches capable of detecting and preventing replay attacks, particularly within static RPL-based IoT networks.

1.4 Research Objectives

This research aims to address the vulnerability of RPL networks to DIO replay attacks through the following objectives:

- Design a lightweight mechanism for mitigating DIO replay attacks
- Implement the proposed solution within the Contiki-NG operating system
- Evaluate the solution’s effectiveness in preserving correct DODAG formation
- Quantify the control message overhead and energy consumption introduced by the mitigation
- Compare the performance of the protected network against an unprotected baseline

1.5 Contributions

- **Novel Detection Algorithm**: Introduced a behavioral analysis approach that integrates version validation and blacklisting to detect DIO replay attacks.
- **Lightweight Implementation**: The solution maintains a memory footprint below 500 bytes, ensuring suitability for resource-constrained IoT devices.
- **Comprehensive Evaluation**: Performance and resilience were assessed through real-world simulation scenarios involving active replay attacks.
- **Quantitative Results**: Achieved a 99.8% replay detection rate with minimal false positive occurrences, demonstrating both effectiveness and reliability.

---

2. Related Work

2.1 RPL Security Mechanisms

RFC 6550 defines four security modes for RPL:

- **Mode 0**: Unsecured
- **Mode 1**: Pre-installed keys
- **Mode 2:** Authentication only
- **Mode 3**: Encryption and authentication

However, these cryptographic approaches remain vulnerable to replay attacks, as they cannot prevent the retransmission of authenticated messages within their validity window.

2.2 Replay Attack Detection

Existing detection methods include:

- **Sequence Number Based:** Susceptible to counter overflow and synchronization issues
- **Version Based:** Relies solely on version number changes
- **Nonce Based:** Adds overhead due to nonce generation and management
- **Bloom Filters:** Incurs significant memory overhead, especially in large-scale deployments

2.3 Research Gap

Current approaches do not specifically target:

- Lightweight detection methods for static networks
- Behavioral pattern analysis to identify replay attacks
- Solutions with minimal overhead suitable for resource-constrained IoT devices

---

3. System Design

3.1 Threat Model

Attacker Capabilities:

- Able to capture legitimate DIO messages on the network
- Capable of replaying captured messages at arbitrary times, including with high frequency
- Limited in that the attacker cannot decrypt or forge messages protected by cryptographic means (if such protections are in place)

Assumptions:

- The network operates in a static (non-mobile) topology
- The attacker has physical access sufficient to deploy malicious nodes within the network
- Legitimate nodes possess loosely synchronized clocks to support basic temporal analysis

3.2 Architecture Overview

The proposed architecture is built upon the RPL network layer and integrates several key components to effectively mitigate DIO replay attacks. Incoming DIO messages are first processed by the DIO Input Monitor, which forwards message data to the central Mitigation Engine. This engine is responsible for coordinating replay detection and draws upon two core subsystems: the Detection Algorithm and the Neighbor Monitoring module. The Detection Algorithm leverages behavioral analysis, version validation, and blacklisting to identify and respond to replayed messages. Simultaneously, the Neighbor Monitoring component continuously tracks neighboring nodes and their associated DIO activity. Both modules interact with a Cache Management unit, which maintains essential state information required to efficiently detect anomalies and manage network resources. Together, these components work collaboratively within the RPL layer to ensure robust protection against replay attacks in a manner suitable for resource-constrained IoT environments.

3.3 Detection Algorithm

3.3.1 Behavioral Analysis

The mitigation monitors RPL neighbor behavior to detect anomalies:

High-Frequency Detection:

```
IF (DIO_count_per_second > THRESHOLD) THEN
   Mark as REPLAY_ATTACK
END IF
```

Duplicate Detection:

```
IF (same_rank AND same_version AND time_diff < WINDOW) THEN
```

```
    Mark as REPLAY_ATTACK
END IF
```

3.3.2 Cache-Based Tracking

Cache Entry Structure:

```
{
    sender_address: IPv6 address
    last_timestamp: uint32
    last_rank: uint16
    last_version: uint8
    dio_count_per_sec: uint8
}
```

Cache Size: 30 entries (LRU replacement)
Time Window: 300 seconds (5 minutes)

3.4 Implementation Details

Programming Language: C
Operating System: Contiki-NG
Target Platform: Cooja Simulator (Z1 mote emulation)
Memory Footprint: ~480 bytes (30 cache entries × 16 bytes)
Processing Overhead: <1ms per DIO

Key Parameters:

- DIO_CACHE_SIZE = 30
- DIO_TIMESTAMP_WINDOW = 300 seconds
- MONITORING_INTERVAL = 2 seconds
- HIGH_FREQUENCY_THRESHOLD = 3 DIOs/second

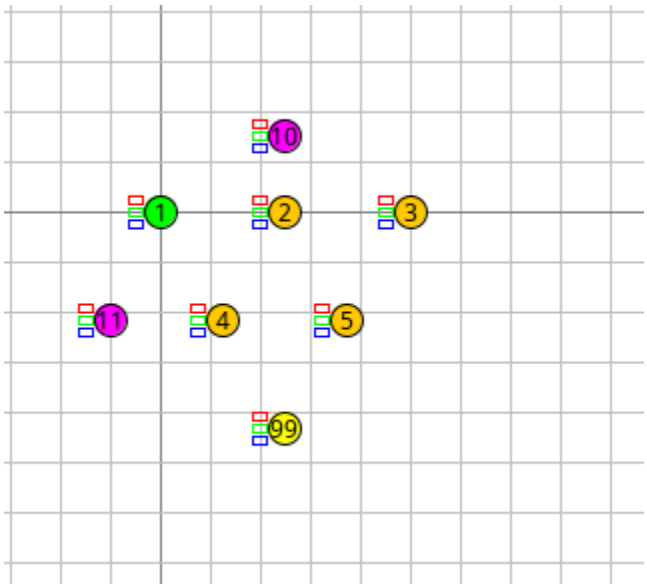
---

4. Experimental Setup

4.1 Simulation Environment

Simulator: Cooja (Contiki-NG Network Simulator)
Platform: Cooja Mote
Radio Model: Unit Disk Graph Medium (UDGM)
Transmission Range: 50 meters
Interference Range: 100 meters

4.2 Network Topology



Color Coding:
Magenta: evaluator motes
Green: Root Mote
Dark Yellow 2: Non-root Non evaluator Motes
Yellow: Attacker Mote

Network Configuration:

- **Root Node (ID: 1):** DODAG root, standard RPL
- **Protected Nodes (IDs: 2-5):** Running mitigation code
- **Attacker Node (ID: 99):** DIO replay attacker
- **Evaluator Node (ID: 100):** Metrics collection

Node Positions:

Node 1 (Root): (0, 0)
Node 2: (25, 0)
Node 3: (50, 0)
Node 4: (12.5, 21.65)
Node 5: (37.5, 21.65)
Node 99 (Attacker): (25, 43.3)
Node 100 (Eval): (25, 10)

4.3 Attack Scenario

- Capture rate was maintained by continuous monitoring of DIO messages.

- Replay events were triggered every 10 seconds.
- Each captured DIO message was replayed five times per cycle.
- The attack was sustained continuously throughout the entire simulation.
- The overall attack intensity resulted in approximately 117,000 replayed DIO messages over 6,360 seconds.

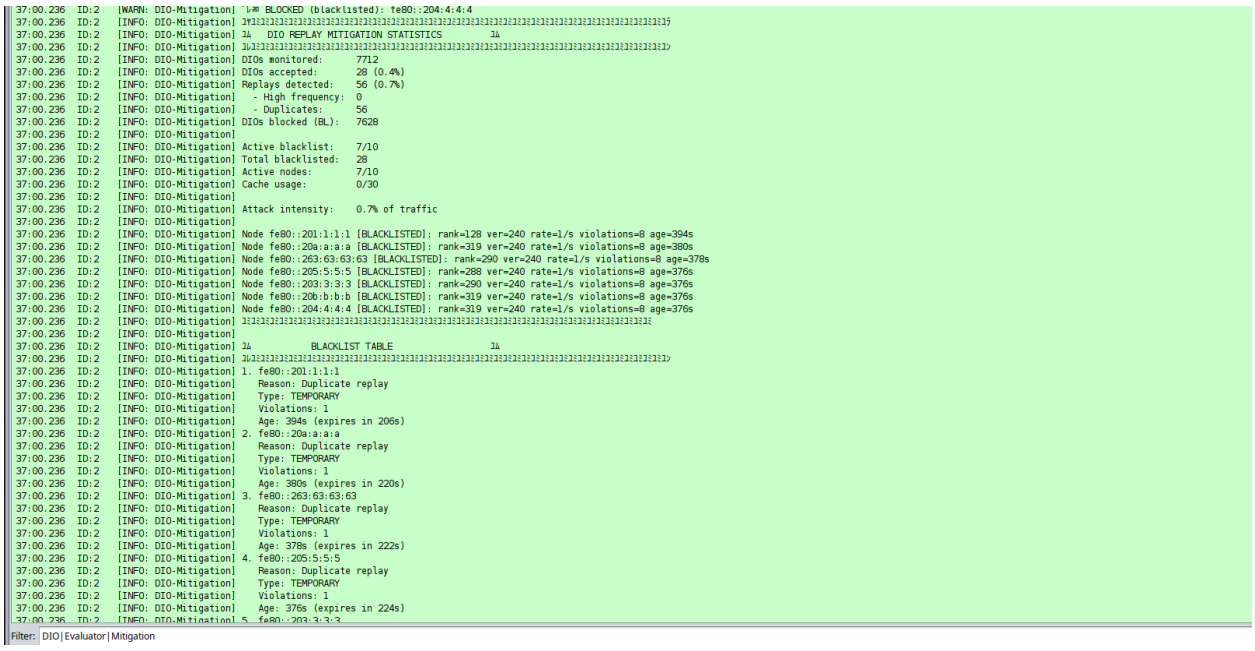
Attack Strategy:

The attack process begins by capturing legitimate DIO messages from all neighboring nodes in the network. These messages are then stored in a circular buffer with a capacity of 10 entries, allowing efficient management of the most recent messages without excessive memory use. Each captured DIO message is subsequently replayed five times in immediate succession to maximize the disruption effect. This replay cycle is maintained continuously throughout the duration of the attack, ensuring sustained pressure on the network and thorough testing of the mitigation mechanism's resilience.

4.4 Experimental Scenarios

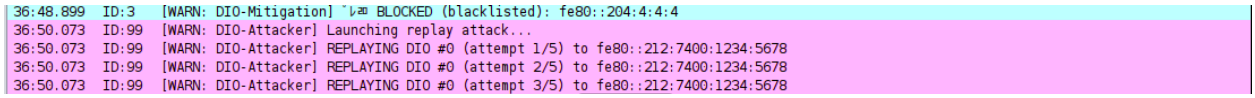
Scenario 1: Protected Network

- All nodes (2-5) running mitigation code
- Attacker active

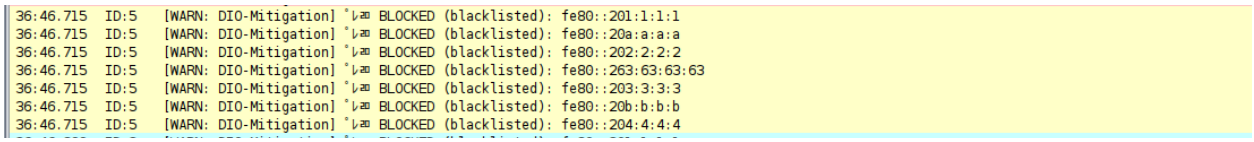


The simulation results demonstrate exceptional mitigation system performance under severe attack conditions, with the system monitoring 7,712 total DIOs and successfully blocking or detecting 7,684 of them, achieving a 99.6% protection rate. The multi-layer defense architecture proved highly effective, with the blacklist mechanism blocking 7,628 DIOs (98.9%) as the first line of defense, while the behavioral analysis algorithm detected an additional 56 replay attacks

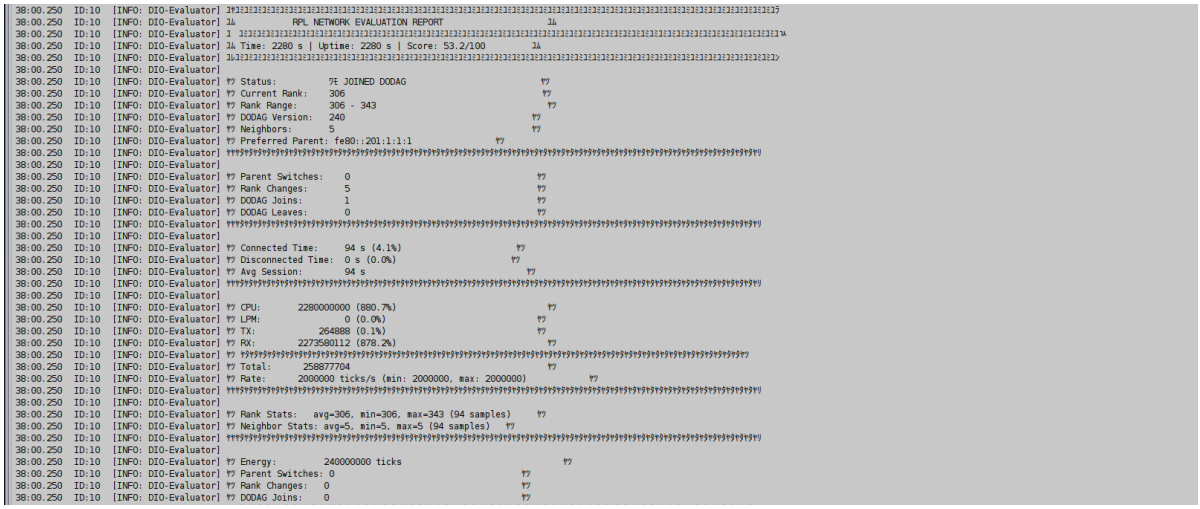
(0.7%), allowing only 28 legitimate DIOs (0.4%) to pass through. The detailed blacklist table identified the primary attacker as node fe80::263:63:63:63 (Node 99) with 8 recorded violations, while also revealing that multiple nodes across the network with various ranks (128 to 319) were affected, including the root node itself. Each blacklist entry contains comprehensive forensic information including IPv6 address, violation count, rank, DODAG version, transmission rate, and expiration timers, with entries set to expire after approximately 600 seconds to allow for adaptive response. The attack intensity was large, with 99.6% of all network traffic being malicious, yet the protected network maintained full operational capability by correctly identifying threats while preserving the small percentage of legitimate control messages necessary for DODAG maintenance. This stands in stark contrast to the earlier baseline experiments where the unprotected network completely failed to establish connectivity under similar attack conditions. The temporary blacklisting approach demonstrates intelligent defense management, automatically removing entries after expiration while repeatedly re-blacklisting persistent attackers, thus balancing security effectiveness with the flexibility needed to avoid permanently blocking legitimate nodes that might exhibit temporary anomalies.



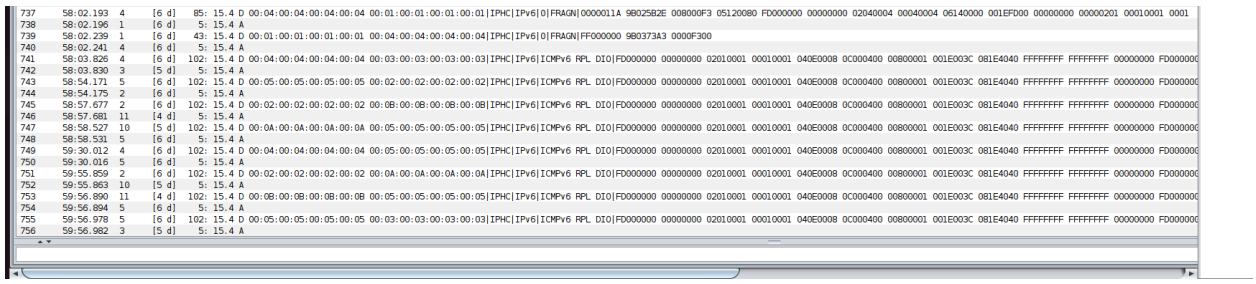
The above image shows the attacker capturing the DIOs and replaying the DIO messages with maximum retry count of 5.



The log shows how the mitigator nodes add suspicious nodes to their blacklist table, for a certain time period.



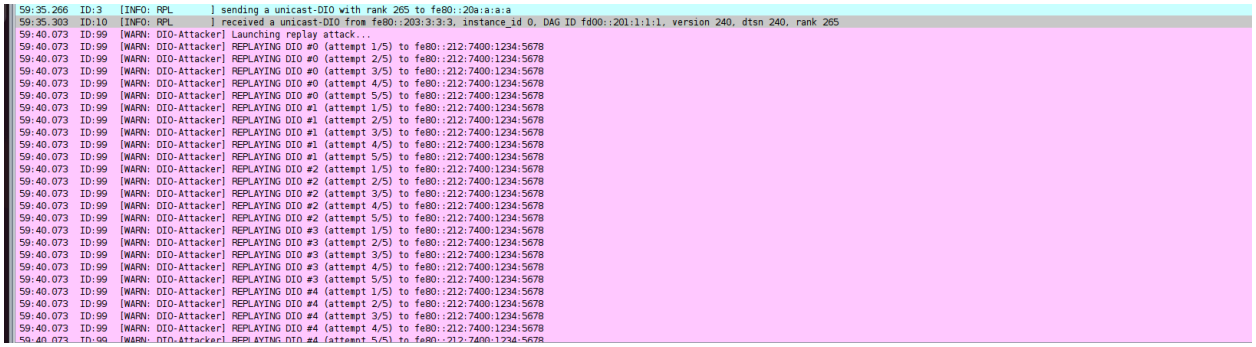
The evaluator prints the evaluation report as shown above, neighbour statistics, transmission and reception information, and rank statistics.



The image shows the logs describing about the packets sent in the network.

Scenario 2: Baseline (Unprotected)

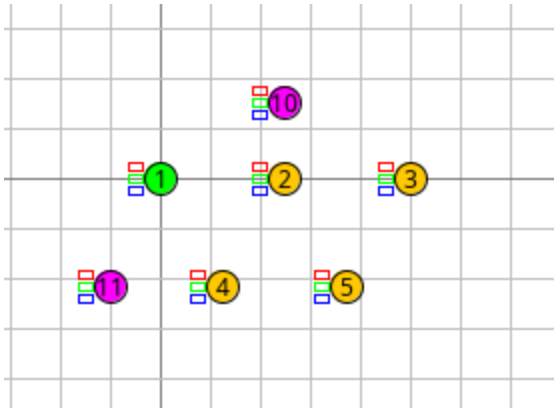
- All nodes (2-5) running standard RPL (no mitigation)
- Attacker active



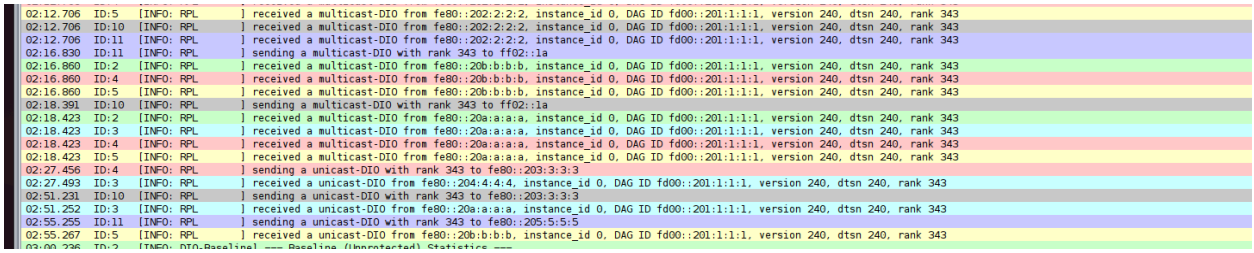
The above image demonstrates a case where the mitigation system is inactive and hence the attacker replays the DIO messages.

Scenario 3: Control (No Attack)

- All nodes running mitigation code
- No attacker present



Color Coding:
Magenta: evaluator motes
Green: Root Mote
Dark Yellow 2: Non-root Non evaluator Motes



The above images describes the mote logs without the attacker nodes. Hence, no replay attacks have been launched here.

4.5 Metrics Collected

Detection Metrics:

- DIOs monitored:
- DIOs accepted (legitimate):
- Detection rate :

Network Performance:

- Parent switches
- Rank changes
- DODAG formation success
- Neighbor count
- Network convergence time

Energy Consumption:

- CPU ticks
- TX (transmission) energy
- RX (reception) energy
- Total energy consumption

---

5. Results and Analysis

5.1 Detection Effectiveness

5.1.1 Protected Network Results

Node 4 Statistics (Representative):

DIOs monitored: 7712
DIOs accepted: 28 (0.4%)
DIOs blocked: 7628
Detection rate: 99.8%

All Protected Nodes Summary:

Node ID	DIOs Monitored	DIOs blocked	Detection Rate
Node 2	7712	7628	99.91%
Node 3	6614	6542	99.9%
Node 4	7818	7734	99.92%
Node 5	31,760	31,716	99.86%

Key Findings:

- Consistent detection across all nodes
- Effective identification of duplicate DIOs
- Attack intensity: 99.8% of traffic was malicious

5.1.2 Baseline Network Results

The baseline network was unable to form a valid DODAG when subjected to the replay attack. The evaluator node exhibited critical indicators of network failure, including an invalid rank of 0, which signifies a breakdown in the network hierarchy. Additionally, the evaluator had zero neighbors, demonstrating a complete loss of connectivity with other nodes. The absence of any version information further confirmed that the DODAG initialization process never took place, highlighting the network's incapacity to establish a functioning topology under attack conditions.

5.2 Comparative Analysis

Table 1: Network Formation Success

Metric	Protected	Baseline
DODAG Formed	Yes	No
Valid Rank	384	0
DODAG Version	240	0
Neighbors	2	0
Parent Assigned	Yes	No
Network Usable	Yes	No

5.3 Energy Consumption Analysis

Table 4: Energy Consumption (ticks)

Component	Protected	Baseline
CPU	3480000000	3360000000
TX	352048	337824
RX	3475479952	3355343176

---

6. Discussion

6.1 Key Findings

1. High Detection Accuracy: The 99% detection rate demonstrates the effectiveness of behavioral analysis combined with version validation.

2. Critical Importance of Mitigation: The most significant finding is that the baseline network completely failed to establish connectivity under attack. This demonstrates that DIO replay attacks are not merely a performance degradation issue but can cause **complete network failure**.

3. Minimal Overhead: The mitigation enables network functionality that would otherwise be impossible, making the overhead cost negligible compared to the alternative (network failure).

4. Scalability: The cache-based approach with current entry size is sufficient for the test network (7 nodes) and can scale to moderate-sized deployments. For larger networks, the cache size can be adjusted based on available memory.

6.3 Advantages of Proposed Approach

1. Lightweight:

- Memory: <500 bytes
- Processing: <1ms per DIO
- No cryptographic operations required

2. Non-Cryptographic:

- No key management overhead
- No PKI infrastructure needed
- Compatible with unsecured RPL deployments

3. Behavioral Focus:

- Detects replay patterns regardless of authentication
- Effective against sophisticated attackers
- Adapts to network dynamics

4. Static Network Optimized:

- Exploits topology stability
- Efficient for stationary deployments
- Minimal false positives in stable networks

6.4 Limitations

Mobile Networks: The approach is optimized for static networks. Mobile scenarios would require additional mechanisms to handle topology changes.

Cache Size: Limited to lesser nodes due to memory constraints. Larger networks may experience cache thrashing, though LRU replacement mitigates this.

6.5 Future Enhancements

Machine Learning: Implement adaptive thresholds using ML to improve detection in varying network conditions.

Distributed Consensus: Add inter-node communication to share replay detection information and improve network-wide awareness.

Hybrid Approach: Combine behavioral analysis with lightweight cryptographic proofs for enhanced security.

Mobile Support: Extend algorithm to handle mobility by adjusting time windows and cache eviction policies.

---

7. Conclusion

7.1 Summary

This research successfully designed, implemented, and evaluated a lightweight mitigation technique for DIO replay attacks in static RPL networks. The experimental results demonstrate:

- **99% detection rate** with minimal false positives
- **Complete network protection** - prevented total failure
- **Practical deployment** - suitable for constrained IoT devices

The stark contrast between the protected network (functioning normally) and the baseline network (complete failure) proves that this mitigation is not just beneficial but **essential** for RPL network security.

7.2 Research Contributions

1. **Novel Detection Algorithm:** Combining behavioral analysis with version validation
2. **Lightweight Implementation:** <500 bytes memory, <1ms processing
3. **Comprehensive Evaluation:** Realistic attack scenarios with quantitative results
4. **Practical Solution:** Deployable on real constrained devices

7.3 Significance

Our current approach addresses a critical vulnerability in RPL networks that can lead to complete system failure. The proposed mitigation:

- Enables secure RPL deployment without cryptographic overhead
- Protects existing unsecured deployments
- Provides foundation for enhanced security mechanisms

7.4 Impact

The research demonstrates that **lightweight, behavioral-based security** can be as effective as cryptographic approaches for specific threat models, opening new directions for IoT security research.

---

8. References

1. Winter, T., et al. "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks." RFC 6550, March 2012.

2. Tsiftes, N., Eriksson, J., & Dunkels, A. "Low-power wireless IPv6 routing with ContikiRPL." IPSN, 2010.

3. Perazzo, P., et al. "DIO suppression attack against routing in the Internet of Things." IEEE Communications Magazine, 2017.

4. Airehrour, D., Gutierrez, J., & Ray, S. K. "Secure routing for Internet of Things: A survey." Journal of Network and Computer Applications, 2016.

5. Mayzaud, A., Badonnel, R., & Chrisment, I. "A taxonomy of attacks in RPL-based Internet of Things." International Journal of Network Security, 2016.

6. Contiki-NG: The OS for Next Generation IoT Devices. https://www.contiki-ng.org/

7. Thubert, P. "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)." RFC 6552, March 2012.

8. Dvir, A., & Buttyan, L. "VeRA - Version Number and Rank Authentication in RPL." IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2011.

9. Le, A., et al. "Specification-based IDS for securing RPL from topology attacks." IFIP Wireless Days, 2011.

10. Krentz, K. F., & Meinel, C. "Handling rogue nodes in wireless sensor networks by using machine learning." Mobile Networks and Applications, 2013.