

On the Observability of Selective Forwarding Attacks in RPL/BRPL-based IoT Networks

이건형

Abstract

본 문서는 RPL/BRPL 기반 IoT 네트워크에서 선택적 포워딩(Selective Forwarding) 공격이 언제 성능 지표로 관측 가능 한지를 분석한다. 기존 연구들이 공격 탐지 기법 자체에 집중한 반면, 본 연구는 공격률 증가가 항상 PDR 또는 지연 저하로 이어지지 않는다는 실험적 관찰에서 출발한다. 우리는 공격 노드를 실제로 경유하는 트래픽의 정도를 구조적 노출(Exposure)로 정의하고, Contiki-NG 및 Cooja(headless) 시뮬레이션으로 토플로지 구조와 경로 다양성이 관측 가능성에 미치는 영향을 정량적으로 분석한다. 예비 실험(총 61회 실행) 결과, 공격률보다 노출이 관측 가능성을 지배하는 핵심 요인임을 확인하였다. 또한 본 문서는 재현 가능한 실험 워크플로우(시나리오 정의-실행-로그 수집-분석-리포트)와 RPL-Classic 기반 BRPL 구현 아키텍처를 함께 제시하여, 향후 대규모 실험 확장 기반을 마련한다.

Index Terms

RPL, BRPL (Backpressure RPL), Selective Forwarding Attack, Observability, Structural Exposure, Low-Power and Lossy Networks

I. 서론

선택적 포워딩 공격은 IoT/WSN 환경에서 대표적인 내부 공격이다. 공격 노드는 라우팅 제어는 정상 수행하되 데이터 패킷 일부를 선택적으로 폐기하여 전달률(PDR) 저하 및 지연 증가를 유발한다. 그러나 실험 환경에서 반복적으로 관찰되는 현상은 다음과 같다. 공격률 α 를 증가시켜도 PDR/지연 변화가 미미하거나, 토플로지에 따라 효과가 과도하게 달라지는 사례가 발생한다. 즉, “공격률 증가 \Rightarrow 관측 가능한 성능 저하”라는 단순 가정은 항상 성립하지 않는다.

본 연구는 관측 가능성(observability) 관점에서 문제를 재정의한다. 공격이 존재하더라도, 공격 노드가 실제 트래픽 경로에 포함되지 않거나 경로 다양성(path diversity) 및 parent 전환으로 우회가 발생하면 성능 지표 변화가 희석되어 공격이 보이지 않을 수 있다. 따라서 공격률 자체보다 “트래픽이 공격자를 얼마나 경유하는가”가 관측 가능성을 좌우할 가능성이 높다.

이를 위해 본 문서는 공격 노드 경유 정도를 구조적 노출(Exposure)로 정의하고, 다양한 구조 시나리오(A/B/C/D)에서 공격률을 변화시키며 PDR 중심의 관측 결과를 비교한다.

A. 연구 질문

본 문서는 다음 질문에 답하고자 한다.

- 동일 공격률에서, 왜 어떤 구조에서는 공격이 명확히 관측되고 어떤 구조에서는 관측되지 않는가?
- 노출(Exposure)과 경로 다양성(Path Diversity)이 관측 지표(PDR/지연)와 맷는 관계는 무엇인가?
- 네트워크 규모(노드 수 증가)는 관측 가능성에 어떤 영향을 주는가?

B. 기여(중간보고 범위)

본 문서는 탐지 알고리즘을 제안하지 않는다. 대신 다음을 기여로 제시한다.

- (C1) 선택적 포워딩 공격의 관측 가능성을 노출 개념으로 정식화하고, 예비 실험으로 1차 검증한다.
- (C2) headless Cooja 기반 재현 가능한 실험 파이프라인과 구조화 로그 포맷을 제시한다.
- (C3) RPL-Classic 기반 BRPL 구현 아키텍처(Queue-DIO 확장-QuickTheta/Beta-parent 선택)를 정리하여 후속 실험 확장의 기반을 마련한다.

II. 배경

A. RPL 개요

RPL은 LLN 환경에서 IPv6 라우팅을 제공하는 프로토콜이며, DODAG(Directed Acyclic Graph) 구조를 형성한다. 노드는 루트까지의 경로 비용을 랭크(rank)로 나타내며, DIO/DAO 제어 메시지에 기반해 parent를 선택한다 [1]. 목적 함수로는 OF0 [2]와 MRHOF [3]가 대표적이다.

B. BRPL 개요

BRPL(Backpressure RPL)은 RPL의 경로 비용과 백프레셔(backpressure) 정보를 결합해 트래픽/혼잡 상황에서 라우팅을 적응적으로 조정하는 확장이다 [4]. 본 연구는 RPL-Classic 기반으로 BRPL 구성요소(큐 상태, DIO 큐 옵션, 가중치 기반 parent 선택)를 구현하고, 선택적 포워딩 공격 관측 가능성 실험에 활용한다.

III. 시스템 및 위협 모델

A. 네트워크 모델

본 연구는 단일 루트, 정적 배치(static placement) LLN을 고려한다. 각 송신 노드는 루트로 주기적 UDP 트래픽을 생성한다. 라우팅은 RPL Classic 또는 BRPL로 동작하며, 동일한 시나리오 구성에서 토글된다.

B. 공격 모델

공격자는 내부 노드로 가정하며, 자신을 경유하는 데이터 패킷을 확률 $\alpha \in [0, 1]$ 로 폐기한다. 라우팅 제어(DIO/DAO)는 정상 수행하여, 공격이 제어-plane에서 노출되지 않도록 한다. 즉, 공격은 data-plane에 국한된다.

C. 관측 가능성 정의

공격이 관측 가능하다는 것은, 정상 상태 대비 PDR 또는 지연이 통계적으로 유의미한 수준으로 변화함을 의미한다. 본 중간보고에서는 우선 PDR 중심으로 관측 가능성을 정리하며, 95% 신뢰구간(Confidence Interval) 비중첩, 또는 명확한 효과 크기(예: PDR 감소)가 확인되는 경우를 관측 가능으로 간주한다. 이는 탐지 알고리즘 자체가 아닌 관측 가능성을 다루기 위한 운영상 정의(operational definition)이며, 본 보고서는 공격 탐지 기법 제안이 아니라 이러한 관측 가능성의 1차 정리에 초점을 둔다.

IV. 실험 방법론

본 절은 “시나리오 정의–실행–로그–분석–리포트”로 이어지는 실험 워크플로우를 재현 가능 관점에서 정리한다.

A. 실험 워크플로우(자동화 파이프라인)

Fig. 1은 전체 워크플로우를 요약한다. 시나리오(.csc) 정의 후 펌웨어를 빌드하고, headless Cooja로 반복 실행한다. 각 실행(run)은 COOJA.testlog를 산출하며, 분석 스크립트가 이를 파싱해 요약 CSV 및 그림/표를 생성한다 [5], [6].

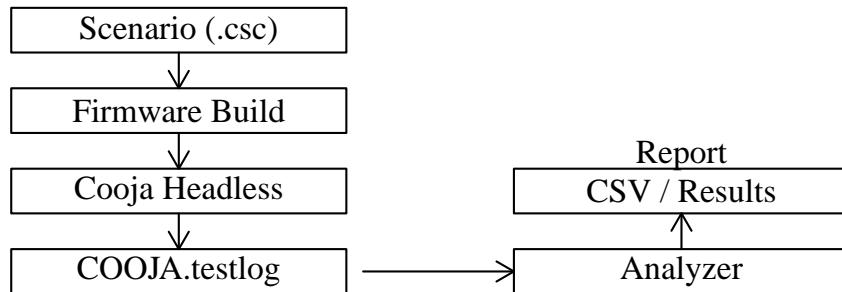


Fig. 1. 실험 워크플로우 개요: 시나리오 정의 → 펌웨어 빌드 → headless Cooja 실행 → 로그 수집 → 분석/리포트

B. 구성요소 및 코드 구조

레포 구성은 아래와 같이 명확히 분리되어 있다.

- 시나리오: simulations/scenarios/*.csc
- 펌웨어: simulations/firmware/rpl-node.c (UDP 트래픽/공격자 모드/OBS 로그)
- 실행기: scripts/run_cooja_headless.py (headless 실행 및 환경변수 주입)
- 실행 래퍼: scripts/run_experiments.sh
- 분석기: scripts/analyze_results.py (PDR*, drop rate, 95% CI 계산)

C. 시나리오 설계(A/B/C/D)

구조적 특성을 제어하기 위해 네 가지 시나리오를 구성하였다. Fig. 2는 시나리오 배치를 요약한다.

- A (Low Exposure): 공격 노드가 경로에 포함되기 어려운 구조
- B (High Exposure): 공격 노드가 필수 중계가 되는 구조 (B(10), B(20))
- C (High Path Diversity): 경로 다양성이 높은 구조
- D (중심성 변화): 평균 경로 길이는 유사하되 중심성 차이를 유도한 구조

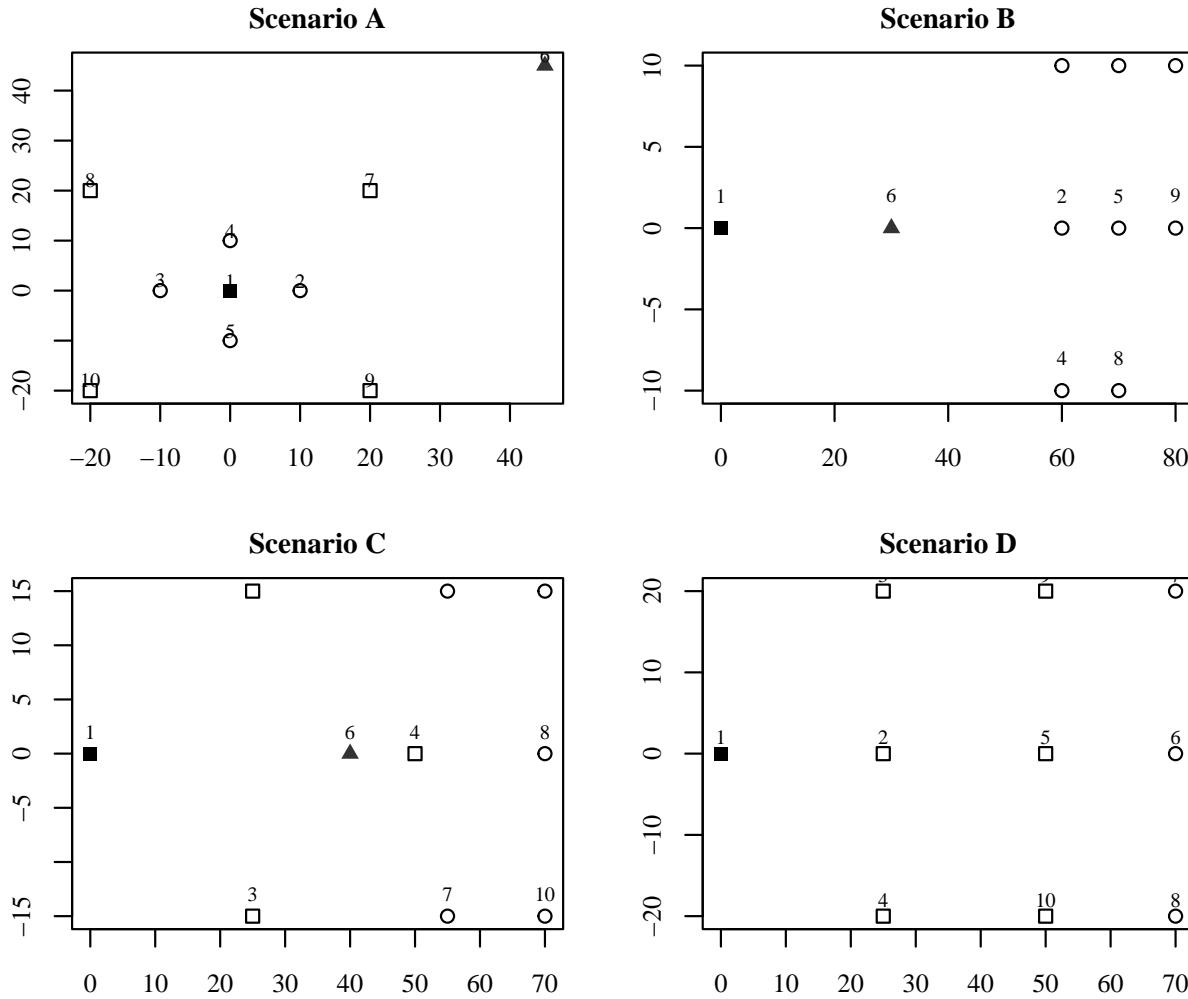


Fig. 2. 시나리오 A/B/C/D 토플로지 요약(루트/공격자/노드 배치).

D. 노출(Exposure) 지표 정의 및 근사

노출은 “공격 노드를 실제로 경유한 트래픽의 비율”로 정의한다. 이 값은 공격률과 독립적으로 토플로지/parent 선택 구조에 의해 결정될 수 있다. 본 중간보고에서는 구현 및 측정 가능성을 고려하여, run별 로그에서 관측된 경유 비율(요약 CSV의 `exposure_e1_prime`)을 노출의 근사치로 사용한다. Fig. 8에서 노출과 PDR 변화의 관계를 시각화한다.

E. 평가지표 및 통계 요약

PDR 정의 및 보정. 일부 로그에서 PDR이 1을 초과하는 현상이 관찰되었다. 이는 TX/RX 카운트 기준 불일치 또는 집계 오차 가능성이 있으므로, 본 보고서는 $PDR^* = \min(PDR, 1.0)$ 로 클리핑하여 보고한다.

신뢰구간. 시나리오 $\times\alpha$ 조합별 반복 실행 결과로 평균 및 95% CI를 산출하여 표로 제시한다.

F. 실험 파라미터

Table I는 실험 파라미터를 요약한다. (테이블 파일은 `tables/table1_sim_params.csv`에서 로드한다.)

TABLE I
실험 파라미터(요약)

"parameter"	"value"
"attack rate α "	"scenario-specific"
"queue size"	"200 packets"
"MAC/RDC"	"CSMA / NULLRDC"
"duration"	"3600s"

V. STRUCTURAL EXPOSURE MODELING

본 절은 선택적 포워딩 공격의 관측 가능성을 설명하기 위한 핵심 구조 변수로서 구조적 노출(*Structural Exposure*)을 정의하고, RPL의 parent 선택(및 switching) 통계를 이용해 노출을 추정하는 모델을 제시한다.

A. Ground-truth Exposure 정의

공격 노드 a , 루트 r , 송신 노드 집합 S 를 고려한다. 관측 구간 T 동안 생성된 모든 데이터 패킷 집합을 \mathcal{P}_T 라 하자. 각 패킷 $p \in \mathcal{P}_T$ 의 실제 전달 경로(중계 노드 시퀀스)를 $\text{Path}(p)$ 라 할 때, **Ground-truth Exposure**는 다음과 같이 정의한다.

$$E_T(a) \triangleq \frac{|\{p \in \mathcal{P}_T : a \in \text{Path}(p)\}|}{|\mathcal{P}_T|}. \quad (1)$$

즉, 전체 송신 트래픽 중 공격 노드를 실제로 경유한 트래픽의 비율이다. 이는 공격률 α 와 독립이며(드랍 확률이 아닌 경유 확률), 토플로지 및 라우팅(parent 선택)에 의해 결정된다.

B. 정적 수렴 구간에서의 트리 기반 *Exposure*

RPL이 수렴하여 관측 구간 동안 parent가 고정된다고 가정하면, 라우팅 구조는 루트로 향하는 트리(또는 유사 트리)로 근사 가능하다. 이때 공격 노드 a 의 자손(서브트리) 집합을 $\text{Desc}(a)$ 라 하면, 각 송신 노드 $i \in S$ 의 트래픽 생성률을 λ_i 로 두었을 때, 트리 기반 노출은 다음과 같이 표현된다.

$$E_{\text{tree}}(a) \triangleq \frac{\sum_{i \in S} \lambda_i \cdot \mathbf{1}[i \in \text{Desc}(a)]}{\sum_{i \in S} \lambda_i}. \quad (2)$$

이는 “공격자 서브트리에 속한 송신자들의 트래픽 비중”에 해당한다.

C. Parent switching을 반영한 시간평균 *Exposure*

현실적으로는 시간에 따라 preferred parent가 변할 수 있다(parent switching). 이를 반영하기 위해, 노드 i 가 이웃 후보 $j \in \mathcal{N}_i$ 를 parent로 선택하는 시간 비율(또는 확률)을 $\pi_{i \rightarrow j}$ 로 정의한다. 이때 “노드 i 에서 생성된 패킷이 최종적으로 공격자 a 를 경유할 확률”을 q_i 로 두면, 다음의 재귀식(흡수 상태 포함)으로 정의할 수 있다.

$$q_i = \sum_{j \in \mathcal{N}_i} \pi_{i \rightarrow j} q_j, \quad \forall i \notin \{a, r\} \quad (3)$$

$$q_a = 1, \quad q_r = 0. \quad (4)$$

그러면 시간평균 노출은 다음과 같이 계산된다.

$$E_{\text{mix}}(a) \triangleq \frac{\sum_{i \in S} \lambda_i q_i}{\sum_{i \in S} \lambda_i}. \quad (5)$$

직관적으로 E_{mix} 는 parent switching 하에서의 경유 확률을 시간평균화한 노출이며, $\pi_{i \rightarrow j}$ 는 로그로부터 “parent가 j 였던 시간 비율”로 추정할 수 있다.

실험에서는 BRPL/RPL 노드가 출력하는 parent 선택/변경 로그(예: PARENT 이벤트)와 구조화된 요약 CSV에서의 parent 구성 비율을 기반으로 $\pi_{i \rightarrow j}$ 를 추정하였다. 구체적으로, 관측 구간 동안 노드 i 가 parent로 j 를 보고한 샘플 수를 노드 i 의 전체 parent 샘플 수로 나누어 row-normalized 확률로 사용한다. 시뮬레이터 로그에는 연속적인 시간 정보가 제한적으로 주어지므로, 본 보고서는 이벤트 발생 횟수 비율을 시간 비율의 근사치로 간주한다. 또한 실제 계산에서는 DODAG가 수렴한 이후의 구간에서만 $\pi_{i \rightarrow j}$ 를 추정하고, 필요 시 각 행이 1이 되도록 row-normalization 및 고립 노드에 대한 연결성 보정을 수행함으로써 식 (3)–(4)가 항상 해를 갖도록 한다.

D. 링크 품질을 포함한 *Effective Exposure*(선택)

무선 링크 손실을 반영하기 위해, 링크 $i \rightarrow j$ 의 데이터 전달 성공 확률을 $s_{i \rightarrow j}$ 로 두면, 공격자 경유 확률 재귀식을 다음과처럼 확장할 수 있다.

$$q_i = \sum_{j \in \mathcal{N}_i} \pi_{i \rightarrow j} s_{i \rightarrow j} q_j. \quad (6)$$

이는 “공격자를 경유할 경로를 선택했더라도 링크 손실로 인해 공격자에 도달하지 못하는” 경우를 반영한다. (본 중간보고에서는 $s_{i \rightarrow j} = 1$ 근사로 시작하고, 후속 연구에서 ETX 기반 추정 등을 포함한다.)

E. Exposure와 공격률의 분리 및 PDR 근사

선택적 포워딩 공격에서 공격률 α 는 “공격자가 자신을 통과한 패킷을 드랍할 확률”이다. 따라서 공격에 의한 기대 손실은 노출과 공격률의 곱으로 근사할 수 있다. 배경 손실을 무시하면,

$$\mathbb{E}[\text{PDR}] \approx 1 - \alpha \cdot E_{\text{mix}}(a). \quad (7)$$

배경 손실플을 L_0 로 두면 다음과 같이 확장 가능하다.

$$\mathbb{E}[\text{PDR}] \approx (1 - L_0) \cdot (1 - \alpha \cdot E_{\text{mix}}(a)). \quad (8)$$

즉, 공격률이 커도 노출이 충분히 작으면(구조적으로 우회되면) PDR 저하가 거의 관측되지 않을 수 있다.

VI. BRPL 구현 아키텍처(RPL-CLASSIC 기반)

본 절은 BRPL 구현이 실험 결과에 대한 신뢰성을 제공하도록, 모듈 구성과 데이터 흐름을 구조적으로 기술한다.

A. 설계 선택: RPL-Classic 기반

BRPL은 parent 선택과 메트릭 계산을 변경하는 확장이므로, 개입 지점이 명확한 RPL-Classic 기반이 구현/분석에 유리하다. 특히 본 연구는 parent 구성 비율 및 경유 경로를 관측해야 하므로, 라우팅 의사결정 과정의 로깅 가능성이 중요한 요구사항이다.

B. 모듈 구성

BRPL은 contiki-ng-brpl의 RPL-Classic 스택에 다음을 추가/확장한다.

- **Queue Manager:** contiki-ng-brpl/os/net/routing/rpl-classic/brpl-queue.c
- **DIO Queue Option:** contiki-ng-brpl/os/net/routing/rpl-classic/rpl-icmp6.c
- **BRPL OF/Rank Facade:** contiki-ng-brpl/os/net/routing/rpl-classic/rpl-brpl.c
- **QuickTheta/QuickBeta:** contiki-ng-brpl/os/net/routing/rpl-classic/rpl-brpl.c
- **RPL DAG/Parent 확장:** contiki-ng-brpl/os/net/routing/rpl-classic/rpl.h

Fig. 3는 데이터 흐름을 요약한다.

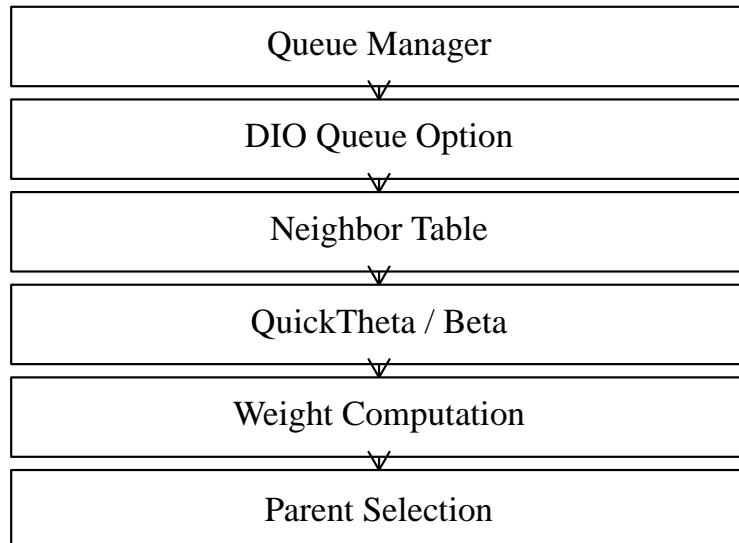


Fig. 3. BRPL 구현 아키텍처: Queue 상태 → DIO 큐 옵션 전파 → 이웃 큐 상태 생성 → QuickTheta/Beta → weight 계산 → parent 선택

C. Queue Manager 및 DIO Queue Option

각 노드는 per-DAG 큐 상태를 유지하며, 스케줄링은 LIFO, 큐 full 시 신규 패킷 drop 정책을 사용한다. 큐 길이는 DIO에 옵션 형태로 포함되어 이웃에게 전파된다. 구현 설정은 다음과 같다.

- Queue max: 200 packets
- Queue scheduling: LIFO
- Queue full: drop new packet
- DIO queue option: code 0xCE, payload 4 bytes, big-endian
- DIO interval: 512–1024ms
- MAC/RDC: CSMA / NULLRDC

D. Parent 선택(가중치) 및 직관

부모 선택은 RPL 비용과 백프레셔 항을 결합한 weight를 최소화한다.

$$w_{x,y} = \theta \cdot \hat{p}_{x,y} - (1 - \theta) \cdot \widehat{\Delta Q}_{x,y} \quad (9)$$

여기서 $\hat{p}_{x,y}$ 는 정규화된 경로 비용(예: ETX 기반), $\widehat{\Delta Q}_{x,y}$ 는 정규화된 큐 차등(backpressure) 항이다. QuickTheta/QuickBeta는 트래픽 및 이웃 변화에 따라 θ 를 업데이트한다. Fig. 4는 θ 변화에 따른 선택 경향을 개념적으로 보여준다.

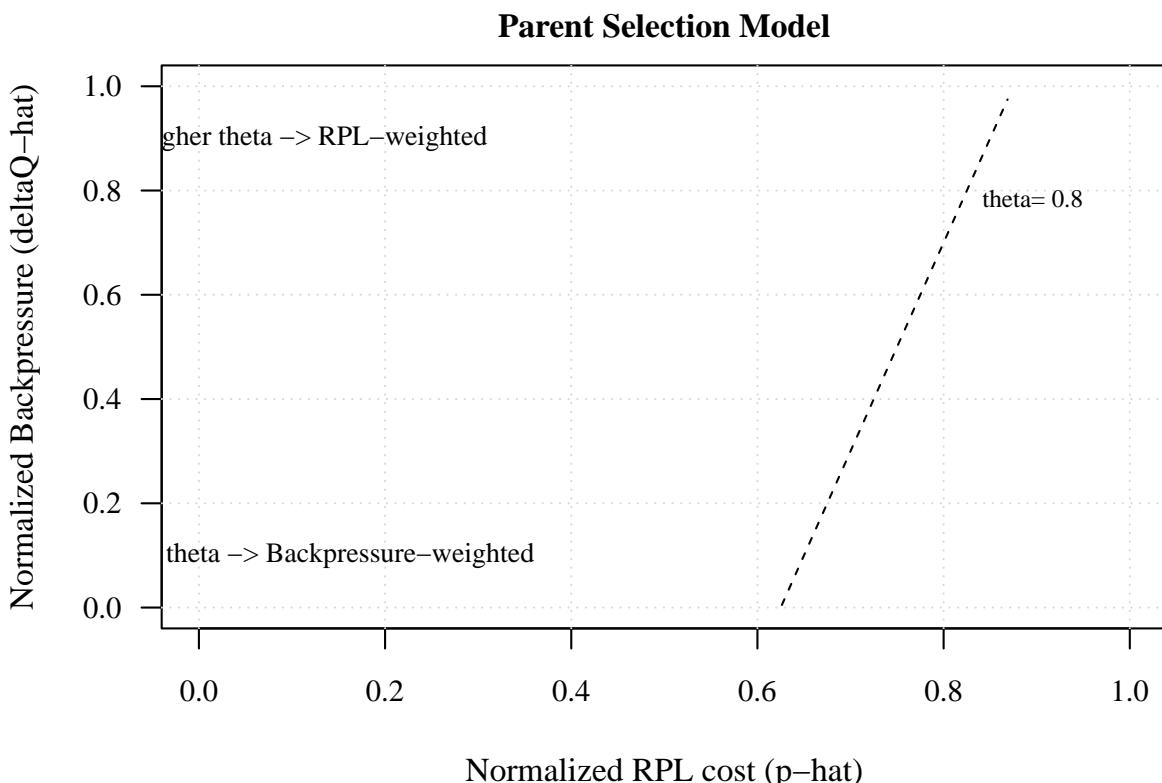


Fig. 4. Parent 선택 개념도: θ 가 클수록 RPL 비용 중심, 작을수록 백프레셔 중심으로 선택

VII. 예비 실험 결과

본 절은 2026-02-04 수행한 예비 실험 결과(총 61회 실행)를 요약한다. 실험 매트릭스는 시나리오(A/B/C/D)와 공격률 α 를 조합하여 구성하였으며, B(20)에서 노드 수 증가 효과를 함께 확인하였다.

A. 실험 실행 요약

총 61회 실행이 수행되었으며, simulations/output/scenario_*.log 및 *_COOJA.testlog 기반으로 모두 정상 완료를 확인하였다. 반복 수는 시나리오별로 상이하며, B(10), C(10)은 $\alpha \in \{0, 0.4, 0.8, 1.0\}$ 에서 각 5회, A와 D는 $\alpha \in \{0, 1.0\}$ 에서 각 3회, B(20)은 $\alpha \in \{0, 0.8, 1.0\}$ 에서 각 3회 수행되었다.

B. 헥심 결과 1: High Exposure(B)에서 PDR* 급락

Fig. 5는 시나리오 B에서 α 증가에 따른 PDR* 변화를 보여준다. High Exposure 구조에서는 공격률 증가에 따라 PDR*이 급격히 감소하였고, $\alpha = 1.0$ 에서 B(10)은 약 0.11, B(20)은 약 0.05까지 감소하였다. 이는 공격 노드가 트래픽 경로에 포함되는 비율이 높을 때, 공격이 성능 지표로 명확히 관측됨을 의미한다.

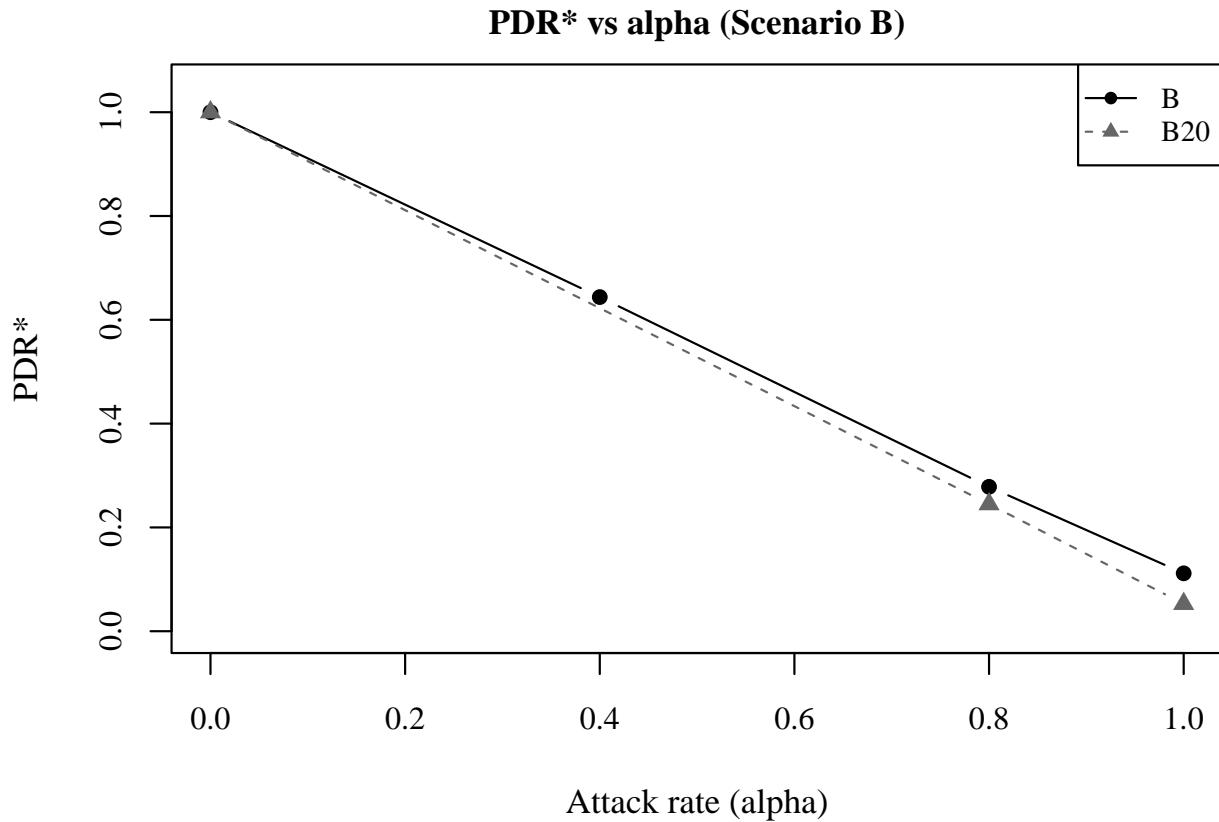


Fig. 5. Scenario B(High Exposure)에서 공격률 α 에 따른 PDR* 변화(B(10) vs B(20)).

C. 헥심 결과 2: Low Exposure(A/D)에서 공격이 “보이지 않음”

Fig. 6는 시나리오별 PDR* 변화를 비교한다. A와 D는 α 가 1.0에 가까워져도 PDR*이 거의 1.0을 유지하였다. 이는 공격이 존재하더라도 구조적으로 우회(bypass)될 경우 성능 저하가 관측되지 않을 수 있음을 보여준다.

D. 헥심 결과 3: High Path Diversity(C)의 완화 효과

시나리오 C는 α 증가에 따라 PDR*이 감소하지만, 시나리오 B보다 완만한 감소를 보였다(Fig. 6). 이는 경로 다양성이 공격 효과를 희석시키거나 우회 경로를 제공하여 관측 가능성을 낮추는 방향으로 작용할 수 있음을 시사한다.

E. 규모 효과: B(10) vs B(20)

노드 수 증가가 관측 가능성을 어떻게 변화시키는지 확인하기 위해 B(10)과 B(20)을 비교하였다. Fig. 7에서 보이듯, 노드 수 증가 시 PDR 저하가 더욱 커지며 관측 가능성이 강화되는 경향이 확인되었다. 이는 규모 증가가 노출 확률을 증가시키거나, 병목 경로를 강화하여 공격 효과가 더 명확히 드러날 수 있음을 시사한다.

F. 노출(Exposure)과 관측 가능성의 관계

Fig. 8는 노출과 PDR* 간 관계를 시각화한다. 노출이 증가할수록 PDR 저하가 커지는 경향이 관찰되었으며, 이는 “공격률보다 노출이 관측 가능성을 지배”한다는 중심 가설을 1차적으로 지지한다. 본 단계에서는 parent switching 통계로부터 계산된 E_{mix} 를 사용하였다.

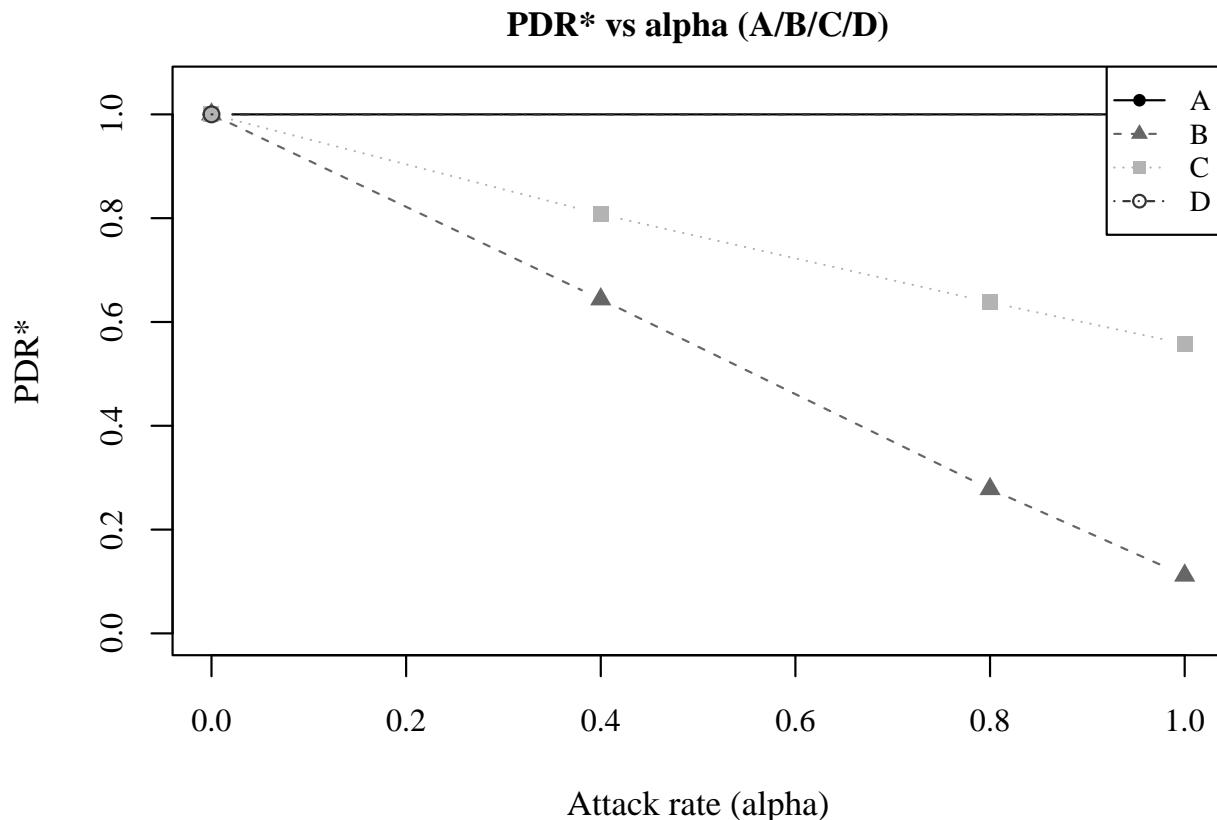


Fig. 6. 시나리오 A/B/C/D에서 공격률 α 에 따른 PDR* 변화 비교.

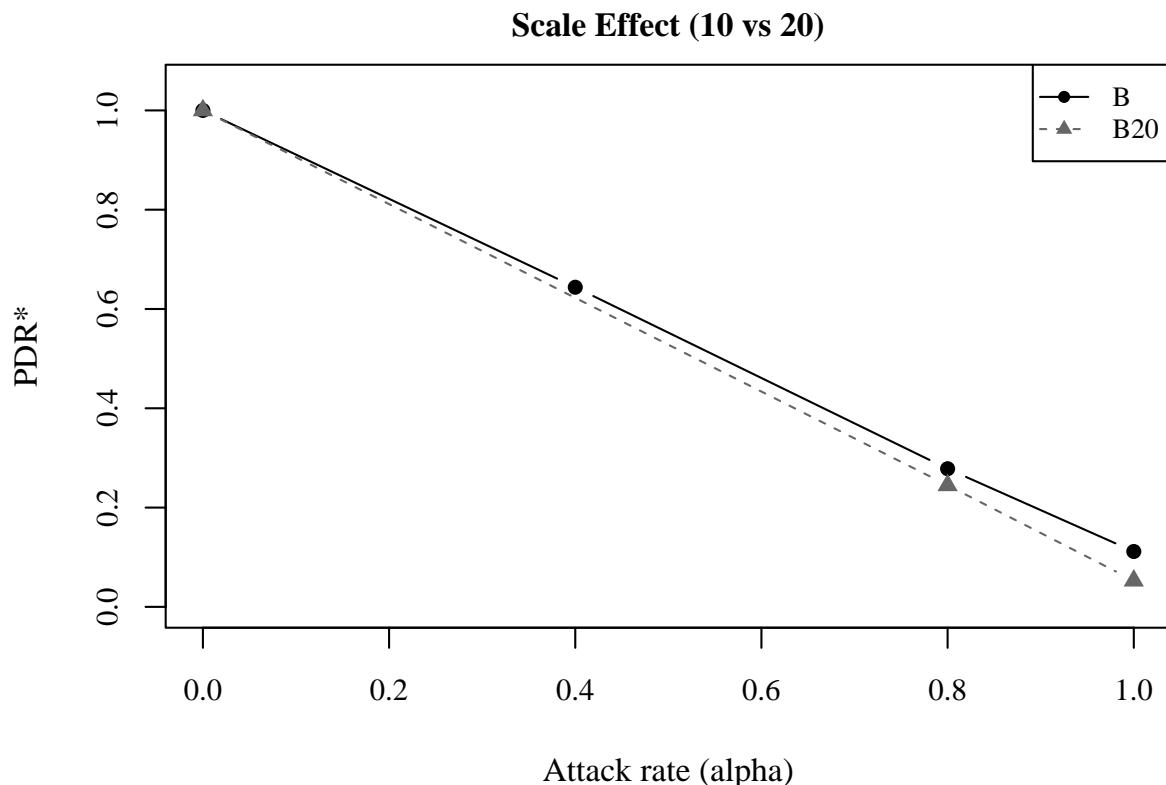


Fig. 7. 규모 효과: Scenario B에서 10노드 대비 20노드에서 관측 저하가 더 큼.

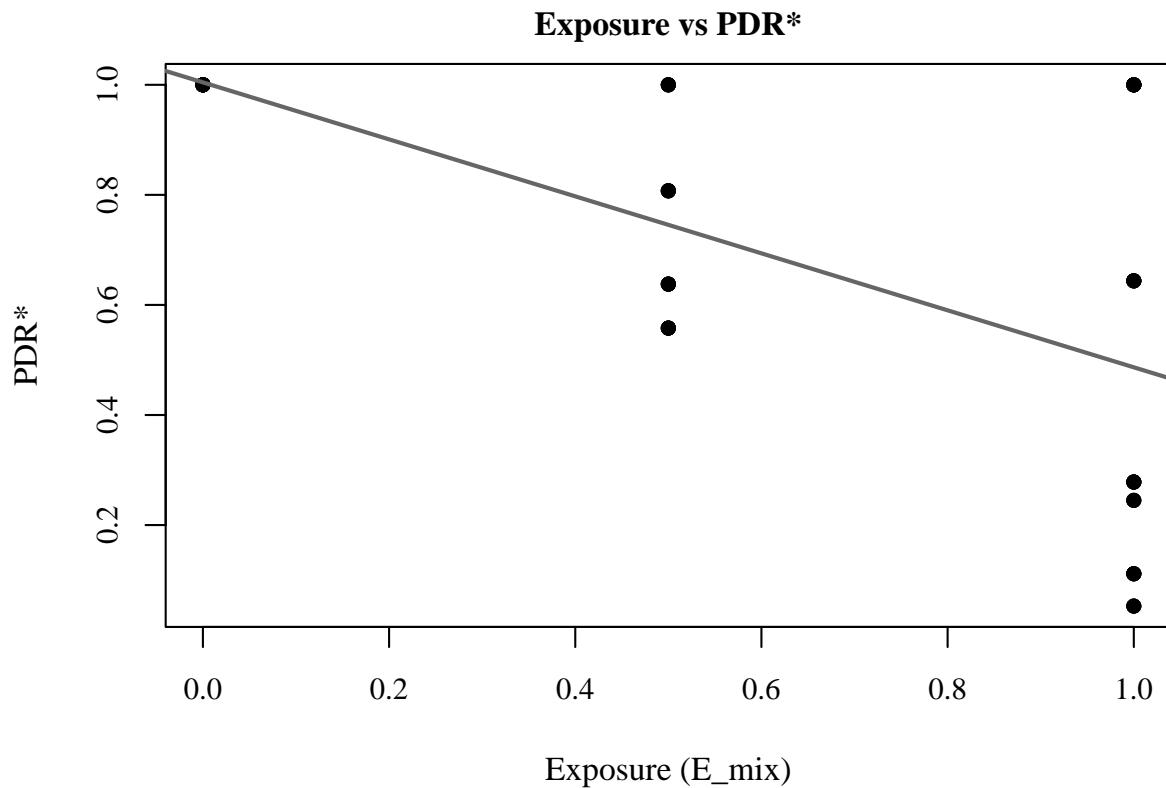


Fig. 8. 노출(E_{mix})과 PDR*의 관계.

G. 노출 추정치 비교 및 PDR 근사 검증

Fig. 9는 로그 기반 노출(E_{log})과 모델 기반 노출(E_{mix})의 관계를 비교한다. 또한 Fig. 10는 PDR^* 와 $\alpha \cdot E_{mix}$ 의 선형 근사 관계를 시각화한다.

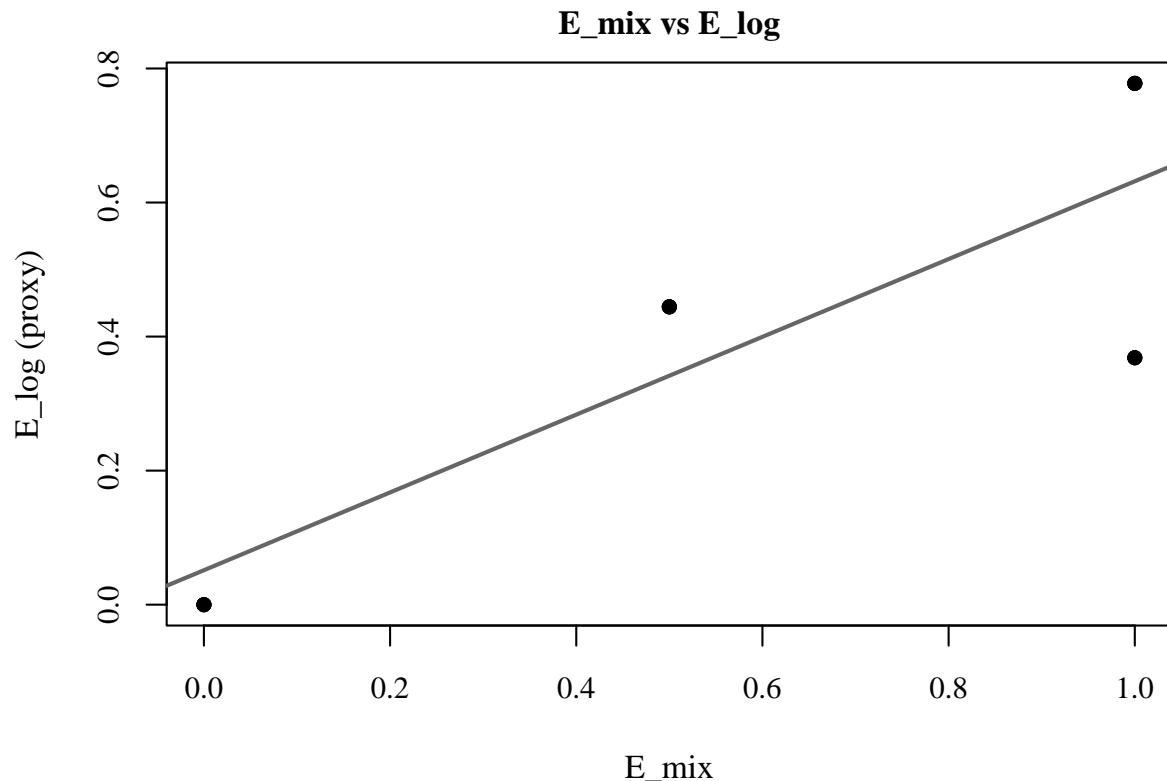


Fig. 9. E_{mix} 와 E_{\log} 비교 산점도.

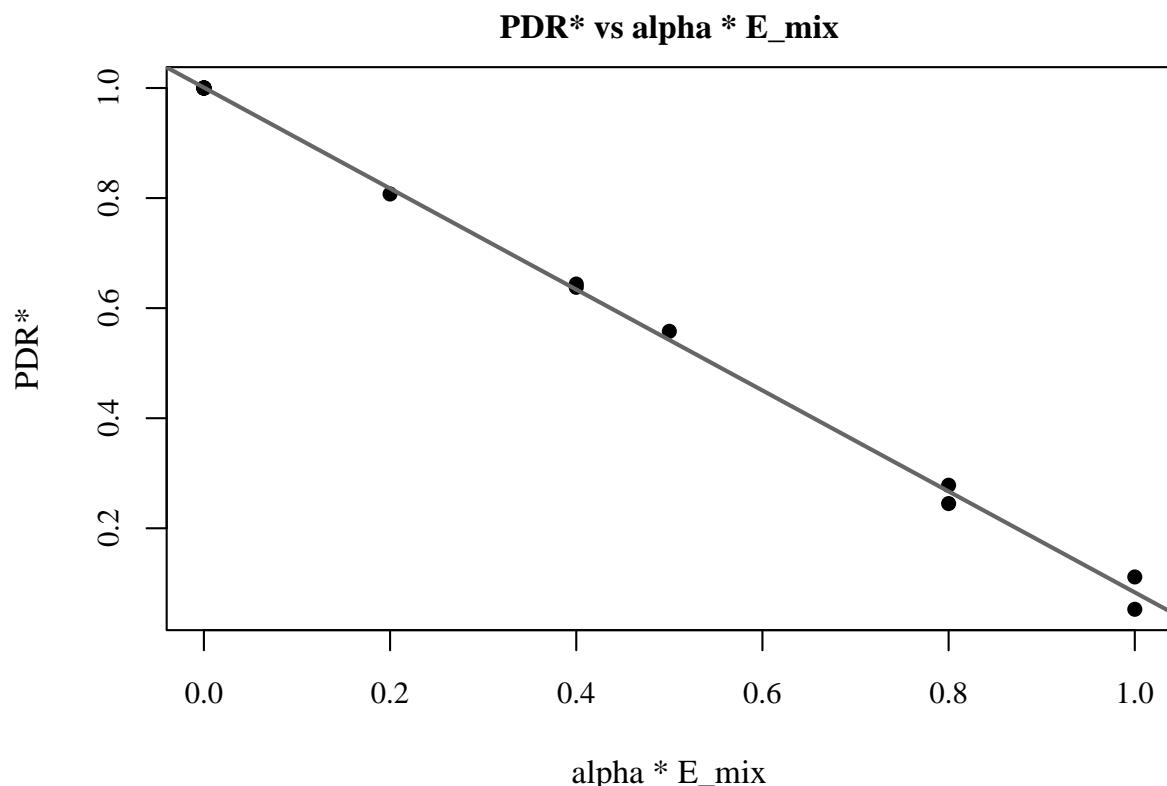


Fig. 10. PDR^* vs. $\alpha \cdot E_{\text{mix}}$ (근사 검증).

H. 요약 히트맵 및 parent 구성 분석

Fig. 11는 시나리오 $\times\alpha$ 전반의 결과를 요약한다. 또한 Fig. 12는 parent 구성 비율을 통해 Low Exposure 환경에서 공격자를 우회하는 경로가 지배적임을 확인한다.

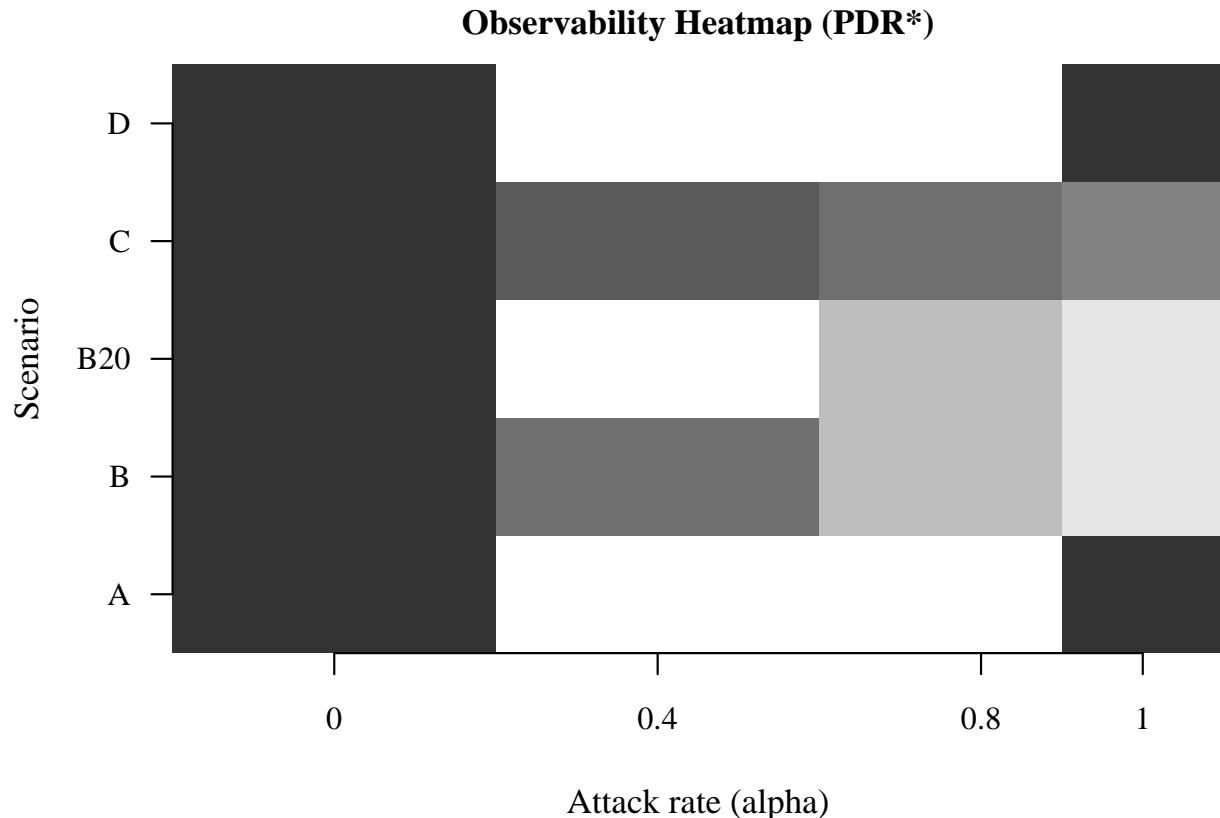


Fig. 11. 관측 가능성 요약 히트맵(PDR*).

I. 정량 요약표

Table II는 시나리오 $\times\alpha$ 조합별 평균 PDR*과 95% CI를 제시한다.

TABLE II
시나리오 $\times\alpha$ 별 평균 PDR* 및 95% CI

"scenario"	"attack_rate_logged"	"mean"	"sd"	"n"	"ci"
"scenario_a_low_exposure"	0	1	0	3	0
"scenario_b_high_exposure"	0	1	0	5	0
"scenario_b_high_exposure_20"	0	1	0	3	0
"scenario_c_high_pd"	0	1	0	5	0
"scenario_d_apl_bc"	0	1	0	3	0
"scenario_b_high_exposure"	0.4	0.6438	0	5	0
"scenario_c_high_pd"	0.4	0.8074	0	5	0
"scenario_b_high_exposure"	0.8	0.2782	0	5	0
"scenario_b_high_exposure_20"	0.8	0.2449	0	3	0
"scenario_c_high_pd"	0.8	0.6378	0	5	0
"scenario_a_low_exposure"	1	1	0	3	0
"scenario_b_high_exposure"	1	0.1116	0	5	0
"scenario_b_high_exposure_20"	1	0.0528	0	3	0
"scenario_c_high_pd"	1	0.5579	0	5	0
"scenario_d_apl_bc"	1	1	0	3	0

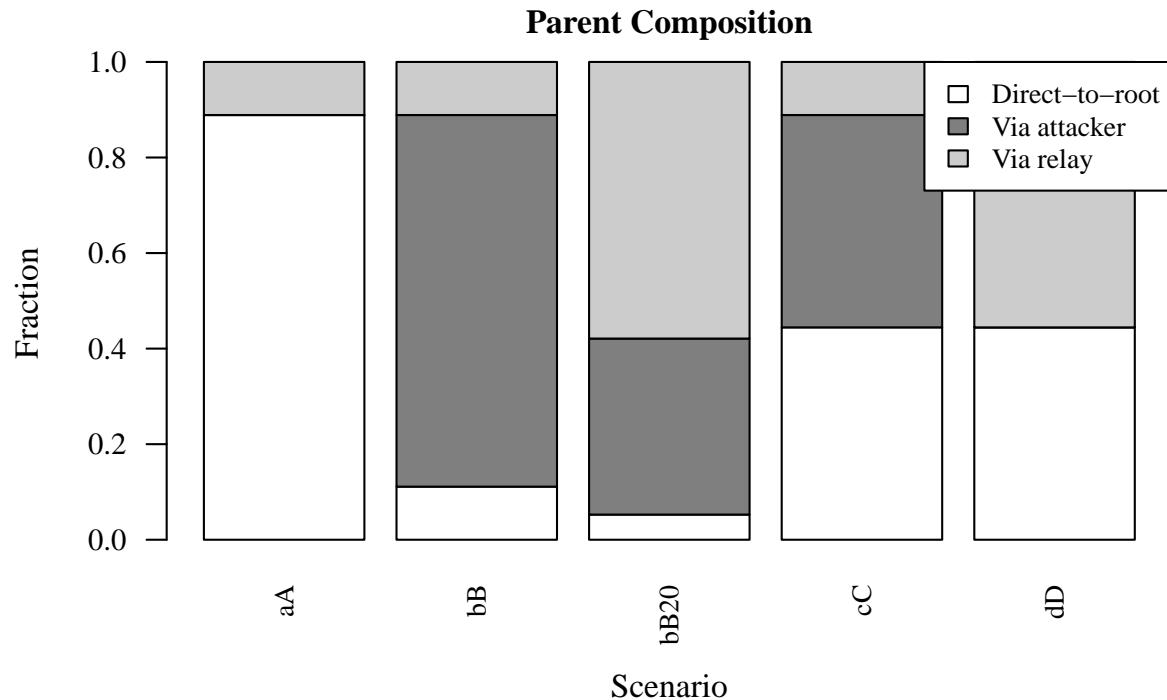


Fig. 12. Parent 구성 비율: Direct / via attacker / via relay 분해.

VIII. 논의

A. 노출이 관측 가능성을 지배하는 이유(구조적 해석)

예비 실험 결과는 다음의 구조적 해석과 일관된다. High Exposure 구조(B)에서는 공격 노드가 사실상 cut-vertex/병목 역할을 하며, 다수 송신 트래픽이 공격자를 경유하게 된다. 따라서 α 증가가 곧 PDR 감소로 연결되어 관측이 용이하다. 반면 Low Exposure 구조(A/D)에서는 루트 직접 연결 또는 대체 중계가 지배적이며, 공격 노드가 경로에서 배제되기 쉬워 공격 효과가 숨겨진다. High Path Diversity(C)에서는 경로 다양성이 우회/분산을 제공하여 공격 효과가 완만하게 나타난다.

B. 탐지가 실패하는 구조적 원인(왜 “보이지” 않는가)

관측이 어려운 경우는 단순히 공격이 약해서가 아니라, 구조적으로 공격 효과가 측정 지표에 반영되지 않는 조건이 존재하기 때문이다. 대표적인 원인은 다음과 같다.

- parent switching: 시간에 따라 parent가 바뀌며 공격 경유가 단속적으로 발생
- bypass paths: 루트 직접 경로 또는 대체 중계로 공격자를 회피
- path diversity: 다중 경로로 트래픽이 분산되어 단일 공격자의 영향이 희석

따라서 탐지 기법 설계 이전에, 해당 네트워크가 구조적으로 관측 가능한지(노출이 충분한지)를 점검하는 것이 중요하다.

C. 중간보고 시점의 함의

본 중간보고 수준에서의 결론은 다음과 같이 요약된다.

- 동일 공격률에서도 관측 가능성은 구조(노출)에 의해 크게 달라진다.
- 공격이 “안 보이는” 경우는 존재하며, 이는 탐지 실패 가능성을 내재한다.
- 경로 다양성은 공격 효과를 완화하는 방향으로 작용할 수 있다.

IX. 타당도 위협 및 한계(THREATS TO VALIDITY)

본 절은 결과 해석의 한계와 향후 개선 방향을 명시한다.

A. 측정 타당도(Measurement Validity)

PDR이 1을 초과하는 현상이 관찰되었다. 이는 RX/TX 카운트 집계 기준의 불일치 가능성이 있으며, 본 보고서는 PDR*로 클리핑하여 보고하였다. 향후에는 TX/RX 정의를 명확히 분리하고, 로그 포인트를 일관된 계층(애플리케이션/네트워크)에서 수집하도록 개선한다.

B. 내적 타당도(Internal Validity)

일부 조합에서 반복 실험의 분산이 0으로 계산되었다. 이는 동일 seed, 결정적 경로 선택, 트래픽 지터 부족 등으로 인해 반복 간 변동성이 충분히 발생하지 않았을 가능성이 있다. 향후에는 seed 분리, 트래픽 지터 강화, 더 긴 실행 시간 및 반복 수 증가로 통계적 신뢰도를 개선한다.

C. 외적 타당도(External Validity)

본 예비 실험은 정적 토플로지 및 제한된 노드 수에 기반한다. 실제 환경의 동적 링크 품질 변화, 이동성, 간섭, TSCH 등을 고려하지 않았다. 따라서 본 결론은 “정적 LLN + RPL/BRPL + 특정 시나리오” 범위에서의 1차 검증으로 해석해야 한다.

D. 구성 타당도(Construct Validity)

노출(Exposure)은 로그 기반 근사치(E1' proxy)로 측정하였다. 후속 연구에서는 노출을 독립 변수로 설계/제어하거나, parent 선택 확률 모델과 결합하여 보다 엄밀한 지표로 확장한다.

X. 향후 연구 계획

중간보고 이후의 구체적 확장 계획은 다음과 같다.

- 1) 노출/다양성/중심성의 수치 스윕: 토플로지를 라벨이 아닌 수치 독립 변수로 생성(.csc 자동 생성 포함)
- 2) 지역/오버헤드 지표 포함: PDR뿐 아니라 지역, 컨트롤 메시지 오버헤드까지 확장
- 3) seed/node/지터/반복 수 확장: 분산 0 이슈 해결 및 신뢰구간 안정화
- 4) RPL vs BRPL 비교 강화: 혼잡 조건에서 BRPL의 parent 전환/경유 변화가 관측 가능성에 미치는 영향 분석

XI. 결론

본 문서는 RPL/BRPL 기반 IoT 네트워크에서 선택적 포워딩 공격의 관측 가능성이 공격률 자체보다 구조적 노출(Exposure)에 의해 지배됨을 예비 실험으로 확인하였다. High Exposure 구조에서는 공격률 증가에 따라 PDR*이 급락하여 관측이 용이하였고, Low Exposure 구조에서는 공격이 거의 관측되지 않았다. High Path Diversity 구조에서는 감소가 완만하여 완화 효과가 관찰되었다. 또한 본 문서는 재현 가능한 실험 워크플로우와 BRPL 구현 아키텍처를 함께 제시하여, 후속 대규모 실험 확장을 위한 기반을 마련하였다.

APPENDIX A 재현을 위한 산출물 및 경로 요약

본 보고서의 실험 및 산출물은 다음 경로 체계를 따른다.

- GitHub 리포지터리: <https://github.com/zeetee1235/rpl-structural-attack-observability>
- 시나리오: simulations/scenarios/*.csc
- 펌웨어: simulations/firmware/rpl-node.c, simulations/firmware/Makefile
- 실행: scripts/run_experiments.sh, scripts/run_cooja_headless.py
- 로그: simulations/output/*_COOJA.testlog, simulations/output/scenario_*.log
- 분석: scripts/analyze_results.py
- 요약 CSV: simulations/output/simulation_summary_20260204_230503.csv
- Figure/Table 생성: Rscript scripts/generate_figures.R

APPENDIX B FIGURE/TABLE 삽입 위치 가이드(요약)

본 문서에서 사용한 Figure/Table의 목적 및 삽입 위치는 다음과 같다.

- Fig.1: 워크플로우(Section 4 서두)
- Fig.2: 시나리오 토플로지(Section 4.3)
- Fig.3: BRPL 아키텍처(Section 5 서두)
- Fig.4: parent 선택 개념(Section 5.4)
- Fig.5/6/7/8/9/10: 결과 및 해석(Section 6-7)
- Table 1/2: 파라미터 및 PDR 요약(Section 4, Section 6)

REFERENCES

- [1] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "Rpl: Ipv6 routing protocol for low-power and lossy networks," RFC 6550, 2012. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6550>
- [2] P. Thubert, "Objective function zero for the routing protocol for low-power and lossy networks (rpl)," RFC 6552, 2012. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6552>
- [3] O. Gnawali and P. Levis, "The minimum rank with hysteresis objective function," RFC 6719, 2012. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6719>
- [4] Y. Tahir, S. Yang, and J. A. McCann, "Brpl: Backpressure rpl for high-throughput and mobile iots," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 29–43, 2018.
- [5] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Proceedings of the First IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2006)*, nov 2006.
- [6] "Contiki-ng documentation," <https://docs.contiki-ng.org/>, 2026, accessed 2026-02-04.