라우팅 공격 환경에서 복원력을 갖춘 신뢰 기반 Backpressure RPL(Trust-Aware BRPL)

이건형

Abstract

Low-Power and Lossy Network(LLN)은 무선 링크 손실과 혼잡(congestion) 상황에서도 안정적인 라우팅이 필요하며, 이를 위해 RPL과 backpressure 기반 변형인 BRPL이 활용된다. 그러나 기존 RPL/BRPL은 내부자 라우팅 공격(insider routing attack)—예를 들어 데이터 평면(data-plane)의 전달(forwarding)을 조작하거나, 제어 평면(control-plane)의 광고(advertisement, 예: rank)를 조작하는 행위—을 명시적으로 고려하지 않는다. 이로 인해 토폴로지와 라우팅 구조에 따라 특정 공격 강도(attack intensity)를 넘으면 성능이 급격히 붕괴(collapse)할 수 있다. 본 문서는 BRPL의 라우팅 결정에 신뢰(trust) 기반 패널티(penalty)를 경량으로 통합한 *Trust-Aware BRPL*을 정리한다. 데이터 평면 신뢰도는 EWMA 기반 평활화를 적용한 Beta 추정기로 모델링하고, 제어 평면 이상 징후는 rank 불일치 및 안정성(stability) 신호로 포착한다. Contiki-NG/Cooja 시뮬레이션에서 공격 강도, 토폴로지 클래스, 네트워크 규모를 스윕(sweep)하는 재현 가능한 실험을 구성하며, BRPL과 Trust-Aware BRPL을 패킷 전달률(PDR), 종단간 지연(end-to-end delay), 제어 오버헤드(control overhead), 부모 변경률(parent churn) 관점에서 비교한다. 결과(추후 삽입)는 신뢰 파라미터가 붕괴 임계값(collapse threshold)을 어떻게 이동시키는지 정량화하고, 복원력(resilience)과 오버헤드 간 트레이드오프(trade-off)를 분석하도록 구성된다.

Keywords: RPL, BRPL, backpressure, trust, LLN, IoT 보안, selective forwarding, sinkhole, Contiki-NG, Cooja

1 Introduction

LLN은 엄격한 전력/메모리 제약(power/memory constraint) 하에서 동작하는 IoT 센싱 및 제어 시스템에 널리 사용되며, 손실이 큰 무선 링크(lossy wireless link)를 통해 통신한다. RPL은 DODAG 형성(DODAG formation), rank, 부모 선택(parent selection)에 기반한 LLN용 표준 IPv6 라우팅 프레임워크를 제공한다 [4]. BRPL은 backpressure 기반 의사결정을 통해 RPL을 확장하여, 혼잡(congestion) 상황에서 경로 다양성(path diversity)을 활용함으로써 처리율(throughput)과 지연(latency)을 개선한다 [8].

그럼에도 LLN 라우팅은 내부자 공격(insider attack)에 취약하다. 대표적인 위협으로 (i) *선택적 전달(selective forwarding)*(grayhole/blackhole) 공격이 있으며, 손상된 전달자(compromised forwarder)가 확률적으로 패킷을 드롭(drop)한다. (ii) *싱크홀(sinkhole)* 공격은 오해를 유발하는 제어 평면 광고(misleading control-plane advertisement, 예: rank 조작)를 통해 트래픽을 유인한 뒤 전달을 방해한다 [5, 13, 6, 7]. 경험적으로 이러한 공격은 상전이(phase transition)에 유사한 거동을 보인다. 공격 강도(attack intensity)가 낮을 때는 성능 저하가 제한적이지만, 토폴로지(topology)와 라우팅 구조(routing structure)에 의존하는 임계값(threshold)을 넘어서면 성능이 급격히 붕괴한다.

1.1 Goal and Approach

본 문서의 목표는 경량 신뢰 신호(lightweight trust signal)를 BRPL의 의사결정 과정(decision process)에 통합하여 이러한 붕괴를 지연시키거나 완화하는 것이다. 무거운 암호 기법(heavy cryptographic mechanism)이나 독립적인 침입 탐지(standalone intrusion detection)를 추가하는 대신, 신뢰를 라우팅 메트릭(routing metric)의 *패널티(penalty)*로 통합한다. 즉, 의심되는 노드는 전달자/

부모로서 덜 매력적이 되도록 만들면서도, BRPL의 혼잡 인지(congestion-aware) 장점은 유지하는 방향을 지향한다.

1.2 Contributions

- **Trust-Aware BRPL 설계:** backpressure 기반 적응성(adaptivity)을 유지하면서 신뢰도가 낮은 이웃(neighbor)을 down-weight하는 경량 trust-penalized BRPL 메트릭을 정리한다.
- **이중 평면(dual-plane) 신뢰 모델:** 데이터 평면(data-plane) 신뢰는 Beta 추정(Beta estimation) + EWMA 평활화(smoothing)로, 제어 평면(control-plane) 신뢰는 RPL 의미론(semantics)에서 도출한 rank 불일치(inconsistency) 및 안정성(stability) 신호로 모델링한다.
- **재현 가능한 평가 프레임워크:** Contiki-NG/Cooja 구현과 스크립트 기반 스윕(scripted sweep)을 통해 토폴로지 클래스, 규모(scale; S/M/L), 공격 강도를 체계적으로 변화시키며 selective forwarding, sinkhole, 복합(combined) 공격을 평가한다.
- **붕괴 임계값(collapse-threshold) 분석 구성:** 신뢰 파라미터가 붕괴 지점을 어떻게 이동시키는지, 그리고 복원력(resilience)이 오버헤드(overhead) 및 churn과 어떻게 트레이드오프 되는지 정량화하도록 결과를 구성한다.

1.3 문서 구성

Section 2에서는 배경 및 관련 연구를 정리한다. Section 3에서는 시스템/위협 모델을 정의한다. Section 4에서는 Trust-Aware BRPL 설계를 제시한다. Section 5에서는 구현 사항을 설명한다. Section 6에서는 실험 설정을 기술한다. Section 7 및 Section 8에서는 결과 보고 및 논의를 수행한다. Section 9에서 결론을 정리한다.

2 Background and Related Work

2.1 RPL과 BRPL

RPL은 싱크(sink)를 루트(root)로 하는 DODAG를 구성하고, rank를 사용해 루프 회피(loop avoidance)와 수렴(convergence)을 보장한다 [4]. BRPL은 backpressure 원리를 RPL에 접목하여 큐 차이(queue differential)와 라우팅 비용(routing cost)을 결합함으로써 혼잡 환경에서 처리율과 지연을 개선하고, 가능한 경우 다중 경로(multi-path)를 활용한다 [8].

2.2 LLN 라우팅 공격

선택적 전달(selective forwarding) 및 싱크홀/랭크(sinkhole/rank) 공격은 LLN의 전달 성능(delivery)과 안정성(stability)을 크게 저하시킬 수 있는 위협으로 보고되어 왔다 [5, 13, 6, 7]. 특히 sinkhole은 오해를 유발하는 제어 평면 정보(misleading control-plane information)로 트래픽을 유인하며, 중요 경로(critical path)에 위치한 이후에는 방해(disruption)를 증폭시키기 쉽다.

2.3 신뢰 기반 라우팅

신뢰 기반 라우팅(trust-based routing)은 행동적 신뢰(behavioral reliability)를 라우팅 결정에 반영하는 접근으로, 직접 관찰(direct observation) 및/또는 평판(reputation) 시스템을 활용한다 [2, 3, 9]. LLN에서는 무선 관찰의 불완전성 및 overhearing 제약 때문에, full watchdog 방식보다는 경량 추정기(lightweight estimator)와 평활화(smoothing)가 실용적이다.

3 System and Threat Model

3.1 System Model

Contiki-NG와 Cooja를 사용하여 RPL/BRPL 라우팅이 포함된 6LoWPAN/IPv6 LLN 스택(stack)을 시뮬레이션한다. 트래픽은 센서 노드(sensor node)에서 루트(root)로의 다대일(many-to-one) 주기적(periodic) 패턴을 따른다. 각 노드는 이웃 테이블(neighbor table)을 유지하며, 기반 라우팅 로직(underlying routing logic)에 따라 선호 부모(preferred parent)를 선택한다 [4, 8].

3.2 Threat Model

단일 내부자 공격자(single insider attacker)를 고려한다(다중 공격자는 향후 과제). 공격자는 정상 노드로 참여하되 다음 중 하나를 수행한다:

- **선택적 전달(selective forwarding):** 전달 중인 트래픽에 대해 확률적 패킷 드롭(probabilistic drop)을 수행하며, 드롭 확률(drop probability)을 공격 강도(attack intensity)로 스윕한다.
- **싱크홀(sinkhole; rank manipulation):** 트래픽 유인을 위해 인위적으로 낮은 rank를 광고(advertise)하는 등 제어 평면을 조작한다. 드롭과 결합되지 않는 경우에는 정상 전달을 수행한다.
- **복합(combined) 공격:** sinkhole로 유인한 이후, 유인된 플로우(captured flow)에 선택적 전달을 결합한다.

루트(root)는 악의적이지 않다고 가정한다. 암호 기반 인증(authentication)과 secure bootstrapping은 범위 밖으로 둔다.

4 Trust-Aware BRPL Design

본 절에서는 신뢰 신호(trust signal)를 정의하고, 이를 BRPL 결정에 반영하는 방법을 기술한다. 관측 노드를 i, 이웃 후보(neighbor candidate; parent/forwarder)를 j로 표기한다. 신뢰 값(trust value)은 $[0, 1]$로 정규화하며, 값이 클수록 신뢰도가 높다.

4.1 Data-Plane Trust for Selective Forwarding

전달 신뢰도를 이웃이 패킷을 성공적으로 전달할 확률로 모델링한다. s_j와 f_j는 각각 j에 귀속된 전달 성공/실패 이벤트 관측치(예: log-based inference)를 나타낸다. Bernoulli 전달 결과에 대해 Beta 사전분포(prior) (α_0, β_0)를 적용하면 [2, 3], posterior mean은

$$\hat{T}_{\text{gray}}(j) = \frac{\alpha_0 + s_j}{\alpha_0 + \beta_0 + s_j + f_j} \tag{1}$$

이다. 단기 잡음(short-term noise)을 줄이기 위해 EWMA 평활화(EWMA smoothing)를 적용한다:

$$T_{\text{gray}}(j; t) = \rho\, T_{\text{gray}}(j; t-1) + (1 - \rho)\, \hat{T}_{\text{gray}}(j), \tag{2}$$

여기서 $\rho \in [0, 1)$는 평활화 강도를 제어한다.

4.2 Control-Plane Trust for Sinkhole Behavior

Sinkhole 공격은 주로 제어 평면(control-plane) 광고(advertisement)에 영향을 준다. RPL의 rank 의미론은 가능한 부모 관계(feasible parent relation)에 monotonicity constraint를 부과한다 [4]. R_i를 노드 i의 current rank, R_j를 이웃 j가 광고한 advertised rank로 둔다. 다음을 정의한다:

$$\Delta_{ij} = R_j + \text{MIN\_HOPRANKINC} - R_i. \tag{3}$$

j가 i 대비 비현실적으로 낮은 rank를 광고하면 Δ_{ij}가 음수가 된다. 허용 오차(tolerance) $\tau \geq 0$를 두고 deviation score를

$$s_{ij} = \max(0,\, -\Delta_{ij} - \tau) \tag{4}$$

로 정의한 뒤, exponential trust decay로 매핑한다 [12, 1]:

$$T_{\text{adv}}(j) = \exp(-\lambda_{\text{adv}}\, s_{ij}), \tag{5}$$

여기서 $\lambda_{\text{adv}} > 0$는 민감도(sensitivity)를 설정한다.

또한 sinkhole은 rank evolution 및 부모 선택(parent selection)의 불안정(instability)을 유발할 수 있다. Window W에 대해 rank increase를

$$\Delta R_i = R_i(t) - R_i(t - W) \tag{6}$$

로 정의하고, $\kappa \geq 0$를 넘는 비정상 증가(abnormal increase)를 패널티한다:

$$u_i = \max(0,\, \Delta R_i - \kappa), \qquad T_{\text{stab}}(t) = \exp(-\lambda_{\text{stab}}\, u_i). \tag{7}$$

제어 평면 신호(control-plane signal)는 곱셈적으로 결합한다:

$$T_{\text{sink}}(j) = (T_{\text{adv}}(j))^{w_1}\, (T_{\text{stab}}(t))^{w_2}\,, \tag{8}$$

여기서 $w_1, w_2 \geq 0$는 각 신호의 가중치(weight)이다.

4.3 Total Trust Aggregation

데이터 평면 및 제어 평면 신뢰는 weighted geometric mean으로 집계한다:

$$T_{\text{total}}(j) = (T_{\text{gray}}(j))^{\alpha}\, (T_{\text{sink}}(j))^{1-\alpha}\,, \tag{9}$$

여기서 $\alpha \in [0, 1]$는 selective forwarding과 sinkhole 신호 사이의 강조 비율을 제어한다.

4.4 Trust-Penalized BRPL Metric

BP_{ij}를 노드 i에서 이웃 j에 대한 baseline BRPL weight/utility로 둔다(BRPL의 backpressure와 cost 결합으로 정의됨) [8]. Trust penalty factor를

$$\phi(T) = \frac{T^{\gamma}}{1 + \lambda\,(1 - T)^{\gamma}}, \tag{10}$$

로 정의하며, $\lambda \geq 0$는 회피 강도(avoidance aggressiveness), $\gamma \geq 1$은 위험 민감도(risk sensitivity)를 제어한다. Trust-aware metric은

$$BP_{ij}^{(\text{trust})} = BP_{ij} \cdot \phi(T_{\text{total}}(j)) \tag{11}$$

이다. 본 형태는 trust가 균일할 때 ordering을 보존하며, λ 또는 γ가 증가할수록 low-trust neighbor를 더 강하게 down-weight한다. 조정 가능한 패널티 파라미터(tunable penalty parameter)의 사용은 stochastic network optimization의 drift-plus-penalty 및 risk-sensitive control 직관과 부합한다 [10].

4.5 Algorithm Outline

각 decision epoch에서 노드 i는 다음을 수행한다:

1. 신뢰 값(trust value; data-plane 및/또는 control-plane)을 업데이트하고 $[0, 1]$로 clamp한다.
2. 각 이웃 후보 j에 대해 $BP_{ij}^{(\text{trust})}$를 계산한다.
3. Trust-penalized objective를 최대화하는 선호 부모(preferred parent) 또는 다음 홉(next hop)을 선택하며, churn 감소를 위해 선택적으로 hysteresis를 적용할 수 있다.

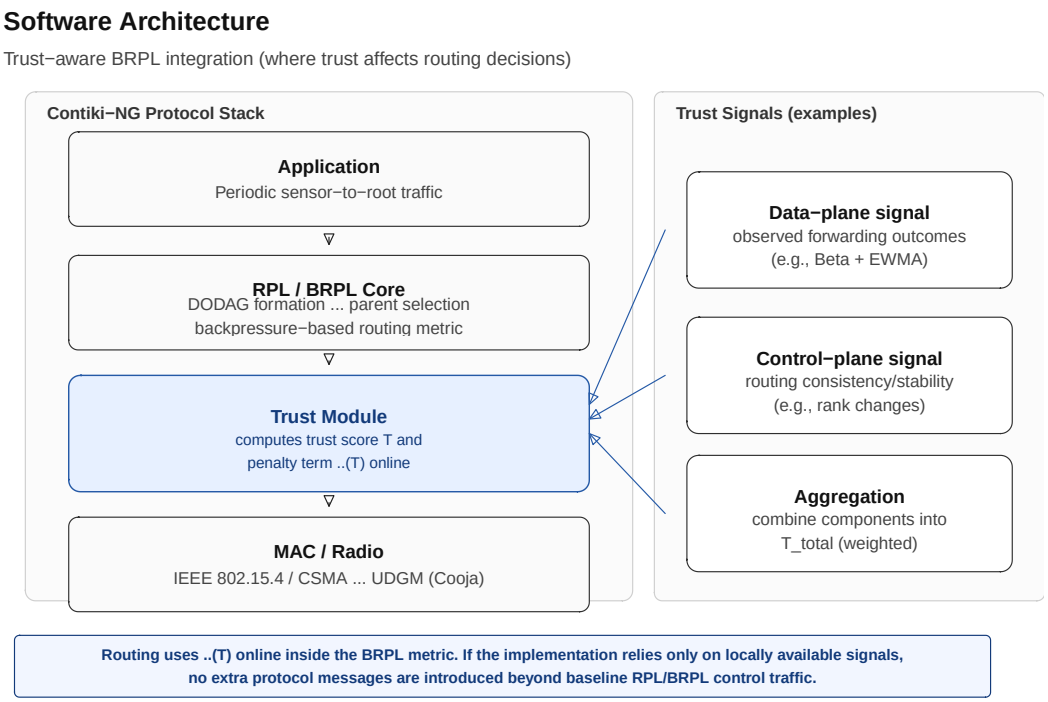

Figure 1: Software architecture of Trust-Aware BRPL and its integration into the Contiki-NG protocol stack.

4.6 Overhead

Trust 유지를 위해 노드당 $O(\deg)$ 값을 저장하며, 여기서 deg는 이웃 차수(neighbor degree)이다. 메트릭 계산은 decision당 $O(\deg)$ 산술 연산을 추가한다. 설계상 추가 제어 패킷(additional control packet)은 요구되지 않으며, 추가 오버헤드는 변경된 routing dynamics(예: parent switching)에서 발생할 수 있다.

5 Implementation in Contiki-NG

Trust-Aware BRPL은 Contiki-NG에서 trust penalty를 BRPL metric computation 및 parent selection path에 통합하는 방식으로 구현한다. Attacker node는 (i) 선택적 전달을 위한 확률적 드롭(probabilistic drop), (ii) sinkhole을 위한 rank advertisement manipulation, (iii) 복합(combined) 동작을 지원한다.

라우팅 결정에 사용되는 모든 trust 값은 simulation runtime 동안 각 노드에서 *online*으로 계산되어 즉시 적용된다. 별도로 수행되는 trust engine의 *offline* log-based analysis는 measurement/visualization/reproducibility 목적에 한정되며, offline 결과가 라우팅 결정으로 피드백되는 일은 없다.

재현성을 위해 seed/topology/attack parameter에 대해 batch experiment를 수행하고, Cooja log에서 metric을 추출하는 scripted pipeline을 유지한다. 구현 세부 파일명 및 스크립트는 본문에서는 생략하며, code repository와 함께 artifact로 제공할 수 있다.

6 Experimental Setup

6.1 Simulation Environment

Cooja의 UDGM Distance Loss radio model을 사용한다 [11]. 별도로 명시하지 않는 한 simulation은 600 s 동안 실행되며 warm-up은 120 s로 둔다. Sensor node는 30 s마다 root로 periodic traffic

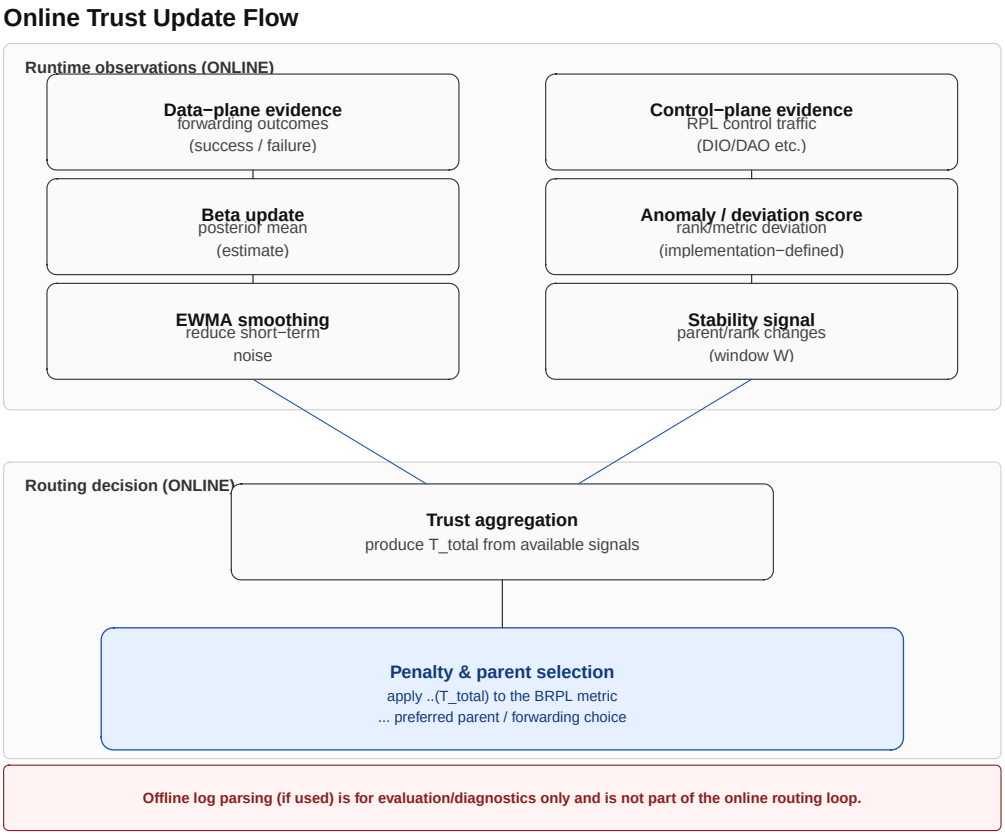

Figure 2: Online trust update and routing decision flow executed at each node during simulation runtime.

을 생성한다. RPL Trickle parameter는 안정성(stability)과 제어 오버헤드(control overhead) 간 trade-off를 고려한 표준 구성을 따른다 [4].

6.2 Topologies and Scales

서로 다른 경로 다양성(path diversity) regime을 포괄하기 위해 다음 topology *class*를 평가한다:

- **Grid:** 경로 다양성이 높아 attack을 부분적으로 우회할 수 있음.
- **Two-cluster with bottleneck:** bottleneck이 존재하는 constrained cut 구조로, attacker가 bottleneck 근처에 위치할 때 공격 효과가 증폭됨.
- **Corridor/chain:** 경로 다양성이 낮아 낮은 intensity에서도 collapse가 발생할 수 있음.
- **Ring/spokes:** 중간 수준의 다양성으로, root-near 및 mid-path 영향이 두드러짐.

네트워크 규모(scale)는 S/M/L(예: root 포함 16/36/64 nodes)로 확장하되, class별 placement rule은 유지한다. Attacker placement는 ad-hoc tuning을 피하기 위해 rule-based selection(예: central relay candidate 또는 bottleneck vicinity)을 따른다.

6.3 Attack Configuration

Selective forwarding은 drop probability(예: 0/30/50/70%)로 parameterize한다. Sinkhole intensity는 rank manipulation delta(예: 1/2/4)로 parameterize한다. 세 가지 모드를 평가한다: selective forwarding only, sinkhole only, combined.

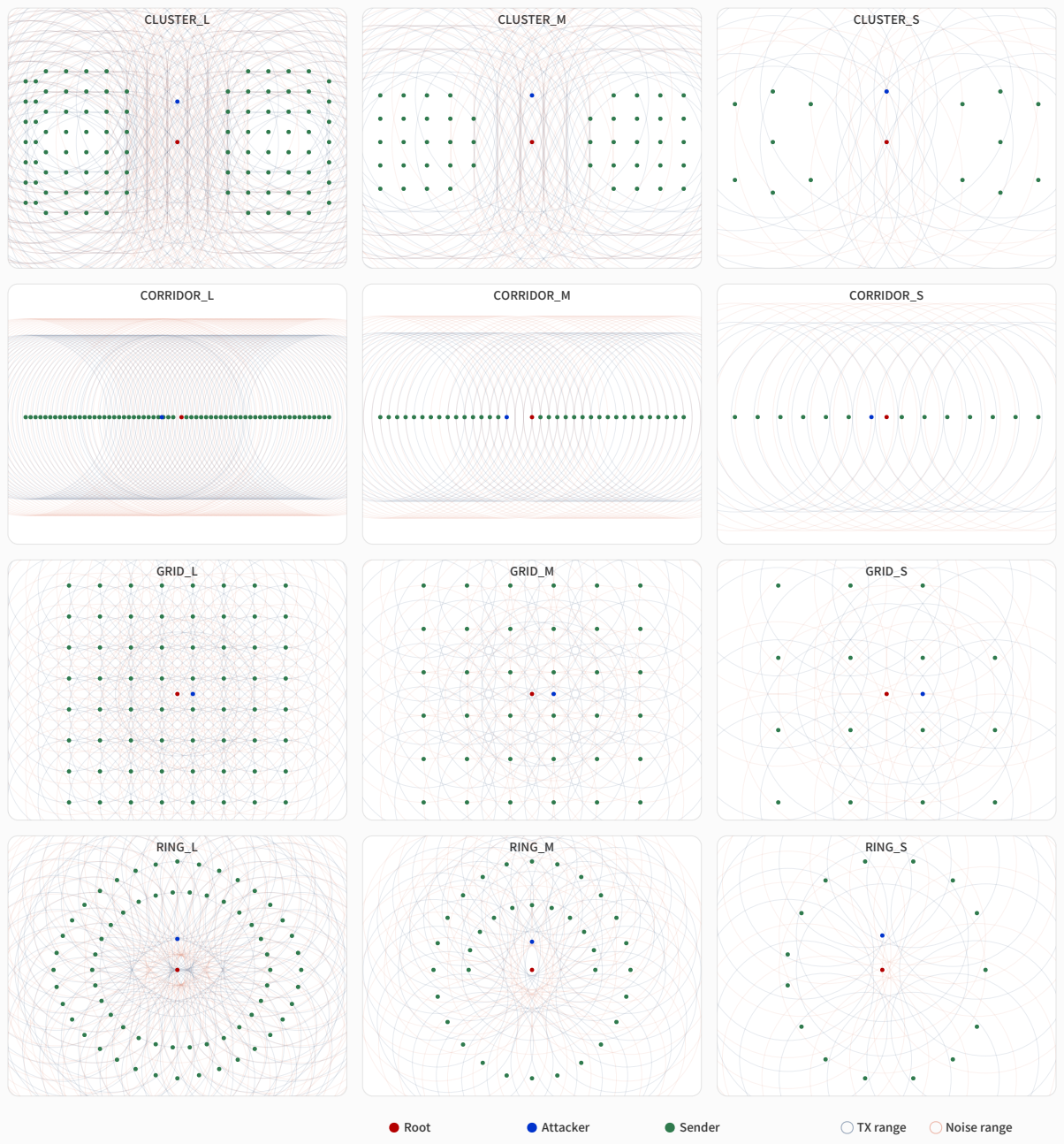

Figure 3: Topology layouts used for evaluation, covering different path diversity regimes and attacker positions.

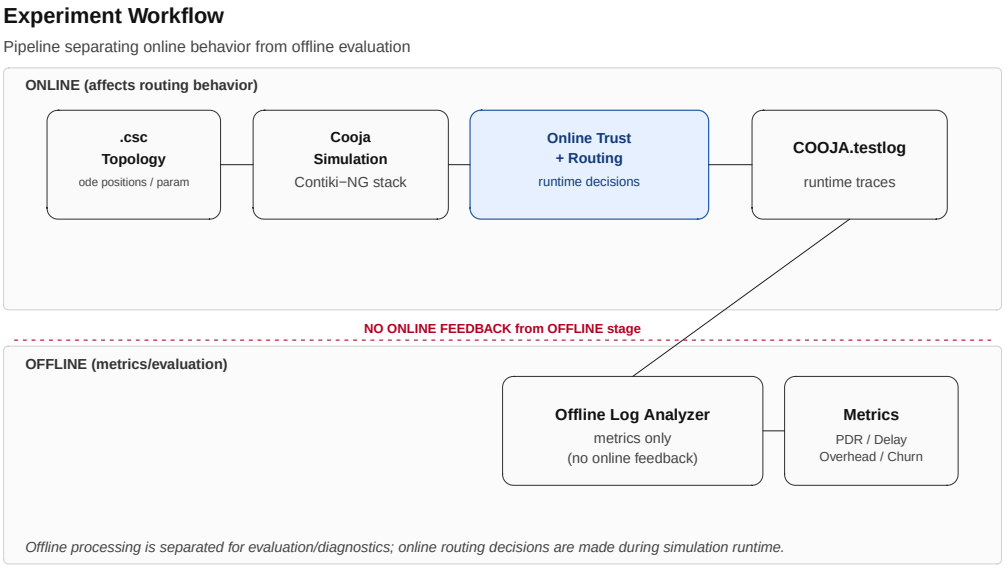

Figure 4: Experiment workflow from simulation execution to offline metric extraction.

6.4 Trust Model Parameters

Table 1는 실험 전반에서 사용한 trust 관련 parameter를 요약한다. 별도로 명시하지 않는 한, scenario별 튜닝을 피하기 위해 모든 topology 및 scale에 동일 구성을 적용한다.

6.5 Metrics

다음 metric을 보고한다:

- **PDR:** $\mathrm{RX}_{\mathrm{root}}/\mathrm{TX}_{\mathrm{senders}}$.
- **종단간 지연(end-to-end delay):** source에서 root까지의 per-packet latency.
- **제어 오버헤드(control overhead):** control-plane transmission(예: DIO/DAO) 및 routing-related overhead.
- **부모 변경률(parent churn):** parent switching rate로, routing stability를 반영.
- **노출(exposure, optional):** delivered packet 중 attacker를 traverse한 비율 및/또는 attacker가 preferred parent인 시간 비율(attack effectiveness 해석용).

6.6 Parameter Sweeps

다음을 스윕한다: (i) attack intensity, (ii) topology class 및 scale, (iii) trust aggregation weight α, (iv) trust-aware case에 대한 penalty parameter (λ, γ). Mean 및 variability를 보고하기 위해 multiple random seed를 사용한다.

7 Results

본 절은 데이터 수집 이후 최종화한다. 분석은 (i) 붕괴 임계값(collapse threshold) 거동과 (ii) trust penalty로 유발되는 trade-off를 강조하도록 구성한다.

Table 1: Trust model parameters used in experiments.

Parameter	Description	Value
α_0	Beta prior (success)	1
β_0	Beta prior (failure)	1
ρ	EWMA smoothing factor	0.8
W	Rank stability window	5 sampling intervals
τ	Rank deviation tolerance	0
κ	Rank increase tolerance	0
λ_{adv}	Rank anomaly sensitivity	0.01
λ_{stab}	Rank instability sensitivity	0.01
w_1	Weight of rank inconsistency trust	0.5
w_2	Weight of rank stability trust	0.5
α	Grayhole vs. sinkhole trust weight	$\{1.0, 0.5\}$
λ	Trust penalty strength	$\{0, 1, 3, 10\}$
γ	Risk sensitivity exponent	$\{1, 2, 4\}$

Table 2: Core experimental parameters (default).

Parameter	Value
Field size	200 m × 200 m
Radio model	UDGM Distance Loss
TX range / Interference range	45 m / 90 m
Simulation time / Warm-up	600 s / 120 s
Traffic interval	30 s
Root ID	1
Attacker count	1 (default)

8 Discussion

본 절에서는 topology-dependent path diversity와 attacker placement가 collapse threshold에 미치는 영향, 그리고 trust penalty가 임계값을 어떻게 이동시키는지 논의한다. 또한 (i) 무선 손실(wireless loss) 및 transient dynamics에서의 false positive 가능성, (ii) $(\lambda, \gamma, \alpha)$에 대한 민감도(sensitivity), (iii) churn 및 overhead에 반영되는 안정성(stability) 영향을 분석한다. 제안 메커니즘은 암호 기반 보호(cryptographic protection) 및 secure bootstrapping을 *대체*하는 것이 아니라 *보완*하기 위한 것으로, full authentication이 불가능하거나 비실용적인 환경에서도 복원력(resilience) 향상을 목표로 한다.

9 Conclusion and Future Work

본 문서는 데이터 평면 전달 신뢰(data-plane reliability)와 제어 평면 이상 신호(control-plane anomaly signal)를 함께 활용하여 BRPL 라우팅 결정에 경량 trust penalty를 통합하는 Trust-Aware BRPL을 정리하였다. 평가 설계는 selective forwarding 및 sinkhole 공격 하에서 trust parameter가 성능 붕괴(performance collapse)를 얼마나 지연시키는지 정량화하고, topology 및 scale 전반에서 resilience–overhead trade-off를 특성화하도록 구성된다. 향후 과제로는 colluding multiple attacker, trust penalty parameter의 adaptive tuning, real testbed 검증(validation)을 포함한다.

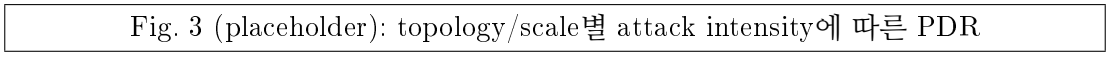

Figure 5: PDR vs. attack intensity (placeholder).

Figure 6: End-to-end delay vs. attack intensity (placeholder).

References

[1] D. Chen and P. K. Varshney. Trust-based routing for wireless sensor networks. In *Proceedings of IEEE MASS*, 2010.

[2] Saurabh Ganeriwal and Mani Srivastava. Reputation-based framework for high integrity sensor networks. In *Proceedings of SecureComm*, 2004.

[3] Saurabh Ganeriwal, Laura Balzano, and Mani B. Srivastava. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, 4(3), 2008.

[4] IETF. Rpl: Ipv6 routing protocol for low-power and lossy networks. RFC 6550, 2012. Internet Engineering Task Force.

[5] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2–3):293–315, 2003.

[6] Anh Le et al. The impact of rank attack on RPL-based networks. In *Proceedings of IEEE ICC*, 2013.

[7] A. Mayzaud, R. Badonnel, and I. Chrisment. A taxonomy of attacks in RPL-based internet of things. *IEEE Communications Surveys & Tutorials*, 18(2):169–184, 2016.

[8] Scott Moeller et al. Brpl: Backpressure RPL for high-throughput and low-latency in LLNs. In *Proceedings of IEEE INFOCOM*, 2016.

[9] M. Momani and S. Challa. Survey of trust models in different network domains. *IEEE Communications Surveys & Tutorials*, 12(2):1–21, 2010.

[10] Michael J. Neely. *Stochastic Network Optimization with Application to Communication and Queueing Systems*. Morgan & Claypool, 2010.

[11] Fredrik Osterlind, Adam Dunkels, Joakim Eriksson, Niclas Finne, and Thiemo Voigt. Cross-level sensor network simulation with COOJA. In *Proceedings of ACM SenSys*, 2006.

[12] Yan Sun, Wei Yu, Zhu Han, and K. J. Ray Liu. Trust modeling and evaluation in ad hoc networks. In *Proceedings of IEEE GLOBECOM*, 2005.

[13] Anthony D. Wood and John A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, 2002.

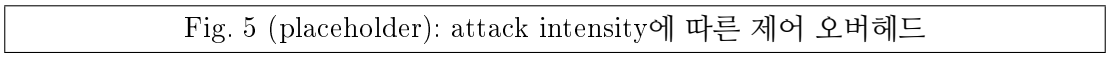

Figure 7: Control overhead vs. attack intensity (placeholder).

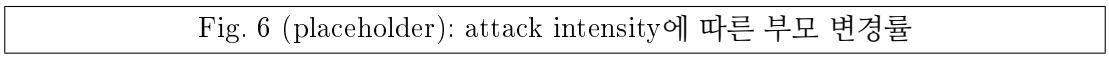

Figure 8: Parent churn vs. attack intensity (placeholder).

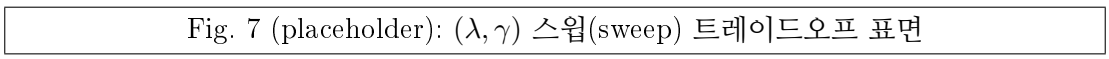

Figure 9: Trade-off under trust penalty sweeps (placeholder).