라우팅 공격 하에서 복원력을 갖춘 Trust-Aware Backpressure RPL

이건형

Abstract

Low-Power and Lossy Networks(LLNs)는 lossy wireless link와 congestion 환경에서도 안정적인 라우팅을 위해 RPL과 backpressure 기반 변형인 BRPL에 의존한다. 그러나 기존 RPL/BRPL은 data-plane forwarding을 조작하거나 control-plane advertisement(예: rank)를 조작하는 insider routing attack을 명시적으로 고려하지 않으며, 토폴로지와 라우팅 구조에 따라 특정 attack intensity를 넘어서면 성능이 급격히 붕괴(collapse)할 수 있다. 본 논문은 BRPL의 라우팅 결정에 trust-derived penalty를 경량으로 통합한 *Trust-Aware BRPL*을 제안한다. Data-plane reliability는 EWMA smoothing을 적용한 Beta-based estimator로 모델링하고, control-plane anomaly는 rank inconsistency 및 stability signal을 사용해 포착한다. Contiki-NG/Cooja 환경에서 attack intensity, topology class, network scale에 대한 재현 가능한 parameter sweep을 수행하며, BRPL과 Trust-Aware BRPL을 packet delivery ratio(PDR), end-to-end delay, control overhead, parent churn 측면에서 비교한다. 실험 결과(추후 삽입)는 trust parameter가 collapse threshold를 어떻게 이동시키는지 정량화하고, 그에 따른 resilience–overhead trade-off를 분석하도록 구성된다.

Keywords: RPL, BRPL, Backpressure, Trust, LLN, IoT Security, Selective Forwarding, Sinkhole, Contiki-NG, Cooja

1 Introduction

LLNs는 엄격한 power/memory constraint 하에서 동작하는 IoT sensing 및 control 시스템에 널리 사용되며, lossy wireless link를 통해 통신한다. RPL은 DODAG formation, rank, parent selection에 기반한 LLN용 표준 IPv6 routing framework를 제공한다 [4]. BRPL은 backpressure-inspired decision을 통해 RPL을 확장하여, congestion 상황에서 path diversity를 활용함으로써 throughput과 latency를 개선한다 [8].

이러한 발전에도 불구하고, LLN 라우팅은 여전히 insider attack에 취약하다. 대표적인 위협으로는 (i) *selective forwarding*(grayhole/blackhole) 공격이 있으며, compromised forwarder가 확률적으로 패킷을 drop한다. (ii) *sinkhole* 공격은 misleading control-plane advertisement(예: rank manipulation)로 트래픽을 유인한 뒤 전달을 방해한다 [5, 13, 6, 7]. 경험적으로 이러한 공격은 *phase-transition-like* 거동을 보인다: attack intensity가 낮을 때는 성능 저하가 제한적이지만, topology 및 routing structure에 의존하는 threshold를 넘어서면 성능이 급격히 붕괴한다.

1.1 Goal and Approach

본 연구의 목표는 경량 trust signal을 BRPL decision process에 통합하여 이러한 collapse를 지연시키거나 완화하는 것이다. Heavy cryptographic mechanism이나 standalone intrusion detection을 도입하는 대신, trust를 routing metric의 *penalty*로 통합한다. 이를 통해 의심 노드는 forwarder/parent로서 덜 선호되면서도, BRPL의 congestion-aware 이점을 유지하도록 유도한다.

1.2 Contributions

- **Trust-Aware BRPL design:** backpressure 기반 adaptivity를 유지하면서 untrustworthy neighbor를 down-weight하는 경량 trust-penalized BRPL metric을 제안한다.

- **Dual-plane trust modeling:** data-plane trust는 Beta estimation + EWMA smoothing으로, control-plane trust는 RPL semantics에서 도출한 rank inconsistency 및 stability signal로 모델링한다.
- **Reproducible evaluation framework:** Contiki-NG/Cooja 구현 및 scripted sweep을 통해 topology class, scale(S/M/L), attack intensity를 체계적으로 스윕하며 selective forwarding, sinkhole, combined attack을 평가한다.
- **Collapse-threshold analysis:** trust parameter가 collapse point를 어떻게 이동시키는지, 그리고 resilience가 overhead 및 churn과 어떻게 trade-off되는지 정량화하도록 결과를 구성한다.

1.3 Paper Organization

Section 2에서는 background 및 related work를 다룬다. Section 3에서는 system/threat model을 정의한다. Section 4에서는 Trust-Aware BRPL 설계를 제시한다. Section 5에서는 구현을 설명한다. Section 6에서는 실험 설정을 기술한다. Section 7 및 Section 8에서는 결과 보고 및 논의를 수행한다. Section 9에서 결론을 맺는다.

2 Background and Related Work

2.1 RPL and BRPL

RPL은 sink를 root로 하는 DODAG를 구성하고, rank를 통해 loop avoidance 및 convergence를 보장한다 [4]. BRPL은 backpressure principle을 RPL에 접목하여 queue differential과 routing cost를 결합함으로써 congestion 하에서 throughput과 delay를 개선하고, 가능한 경우 multi-path를 활용한다 [8].

2.2 Routing Attacks in LLNs

Selective forwarding 및 sinkhole/rank attack은 LLN에서 delivery와 stability를 심각하게 저하시킬 수 있는 대표적 위협으로 알려져 있다 [5, 13, 6, 7]. 특히 sinkhole은 misleading control-plane information으로 트래픽을 유인하며, critical path에 위치한 이후 disruption을 증폭시키기 쉽다.

2.3 Trust-Based Routing

Trust-based routing은 behavioral reliability를 routing decision에 반영하는 접근으로, direct observation 및/또는 reputation system을 활용한다 [2, 3, 9]. LLN에서는 wireless observation의 불완전성과 overhearing의 한계로 인해, full watchdog보다는 lightweight estimator와 smoothing 기법이 실용적이다.

3 System and Threat Model

3.1 System Model

Contiki-NG 및 Cooja를 사용하여 RPL/BRPL routing을 포함하는 6LoWPAN/IPv6 LLN stack을 시뮬레이션한다. 트래픽은 sensor node에서 root로의 many-to-one periodic pattern을 따른다. 각 노드는 neighbor table을 유지하며 underlying routing logic에 따라 preferred parent를 선택한다 [4, 8].

3.2 Threat Model

단일 insider attacker를 고려한다(multiple attacker는 future work). 공격자는 정상 노드로 참여하되 다음 중 하나를 수행한다:

- **Selective forwarding:** forwarded traffic에 대해 확률적으로 packet drop을 수행하며, drop probability를 attack intensity로 스윕한다.
- **Sinkhole (rank manipulation):** control-plane 조작(예: artificially low rank advertisement)으로 트래픽을 유인하며, dropping과 결합되지 않는 경우에는 정상 forwarding을 수행한다.
- **Combined attack:** sinkhole attraction 이후 captured flow에 selective forwarding을 결합한다.

Root는 non-malicious하다고 가정한다. Cryptographic authentication 및 secure bootstrapping은 본 논문의 범위 밖이다.

4 Trust-Aware BRPL Design

본 절에서는 trust signal을 정의하고, 이것이 BRPL decision을 어떻게 조절(modulate)하는지 기술한다. 관측 노드를 i, neighbor candidate(잠재적 parent/forwarder)를 j로 표기한다. Trust value는 $[0, 1]$로 정규화되며 값이 클수록 신뢰도가 높다.

4.1 Data-Plane Trust for Selective Forwarding

Forwarding reliability를 neighbor가 패킷을 성공적으로 전달할 확률로 모델링한다. s_j와 f_j는 각각 j에 귀속된 forwarding success/failure 이벤트의 관측치로 둔다(예: log-based inference). Bernoulli forwarding outcome에 대해 Beta 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. Short-term noise를 줄이기 위해 EWMA smoothing을 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 smoothing 강도를 제어한다.

4.2 Control-Plane Trust for Sinkhole Behavior

Sinkhole attack은 주로 control-plane advertisement에 영향을 준다. RPL rank semantics는 feasible parent relation에 monotonicity constraint를 부과한다 [4]. R_i를 노드 i의 current rank, R_j를 neighbor j가 광고(advertise)한 rank로 둔다. 다음을 정의한다:

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

j가 i 대비 implausibly low rank를 광고하면 Δ_{ij}가 음수가 된다. Tolerance $\tau \geq 0$를 두고 deviation score를

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

로 정의하며, 이를 exponential trust decay로 매핑한다 [12, 1]:

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

여기서 $\lambda_{\text{adv}} > 0$는 sensitivity를 설정한다.

Sinkhole behavior는 rank evolution 및 parent selection의 instability를 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 abnormal increase를 패널티한다:

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

Control-plane signal은 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 weight이다.

4.3 Total Trust Aggregation

Data-plane trust와 control-plane trust는 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 forwarding vs. sinkhole signal의 강조 비율을 제어한다.

4.4 Trust-Penalized BRPL Metric

BP_{ij}를 노드 i에서 neighbor j에 대한 baseline BRPL weight/utility로 둔다(BRPL의 backpressure + 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 avoidance aggressiveness를, $\gamma \geq 1$은 risk sensitivity를 제어한다. Trust-aware metric은

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

이다. 본 형태는 trust가 uniform할 때 ordering을 보존하면서, λ 또는 γ가 증가할수록 low-trust neighbor를 강하게 down-weight한다. Tunable penalty parameter의 사용은 stochastic network optimization에서의 drift-plus-penalty 및 risk-sensitive control 직관과 부합한다 [10].

4.5 Algorithm Outline

각 decision epoch에서 노드 i는 다음을 수행한다:

1. Trust value(data-plane 및/또는 control-plane)를 업데이트하고 $[0, 1]$로 clamp한다.
2. 각 neighbor candidate j에 대해 $BP_{ij}^{(\text{trust})}$를 계산한다.
3. Trust-penalized objective를 최대화하는 preferred parent / forwarding next hop을 선택하며, churn 감소를 위해 optional hysteresis를 적용할 수 있다.

4.6 Overhead

Trust 유지에는 노드당 $O(\text{deg})$ 값 저장이 필요하며, 여기서 deg는 neighbor degree이다. Metric 계산은 decision당 $O(\text{deg})$ 산술 연산을 추가한다. 설계상 additional control packet은 요구되지 않으며, 추가 overhead는 변경된 routing dynamic(예: parent switching)에서 발생할 수 있다.

5 Implementation in Contiki-NG

Contiki-NG에서 Trust-Aware BRPL을 구현하기 위해 trust penalty를 BRPL metric computation 및 parent selection path에 통합하였다. Attacker node는 (i) selective forwarding을 위한 probabilistic forwarding drop, (ii) sinkhole behavior를 위한 rank advertisement manipulation, (iii) combined operation을 지원한다.

Routing decision에 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 routing decision에 피드백되는 일은 없다.

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

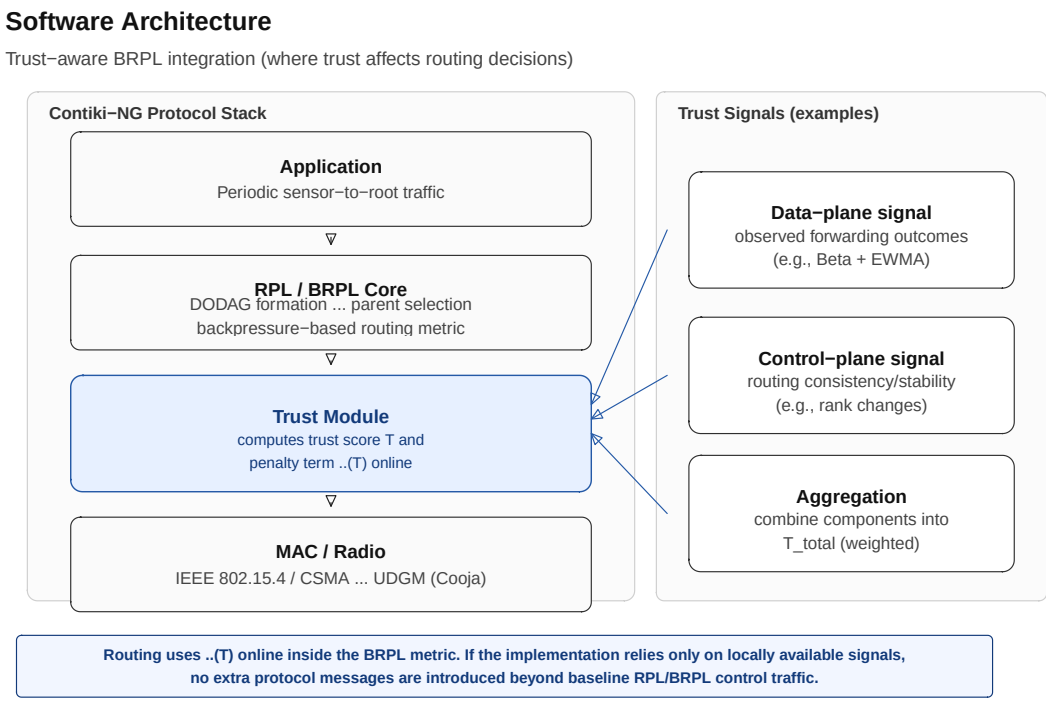

Figure 1: Software architecture of Trust-Aware BRPL and its integration into the Contiki-NG protocol stack.

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 traffic을 생성한다. RPL Trickle parameter는 stability와 control overhead 간 trade-off를 고려한 표준 구성을 따른다 [4].

6.2 Topologies and Scales

서로 다른 path diversity regime을 포괄하기 위해 다음 topology *class*를 평가한다:

- **Grid:** high path diversity; attack이 부분적으로 bypass될 수 있음.
- **Two-cluster with bottleneck:** constrained cut; attacker가 bottleneck 근처에 위치할 때 attack effect가 증폭됨.
- **Corridor/chain:** low path diversity; 낮은 intensity에서 collapse가 발생할 수 있음.
- **Ring/spokes:** intermediate diversity; root-near 및 mid-path 영향이 두드러짐.

Network size는 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 mode를 평가한다: selective forwarding only, sinkhole only, combined.

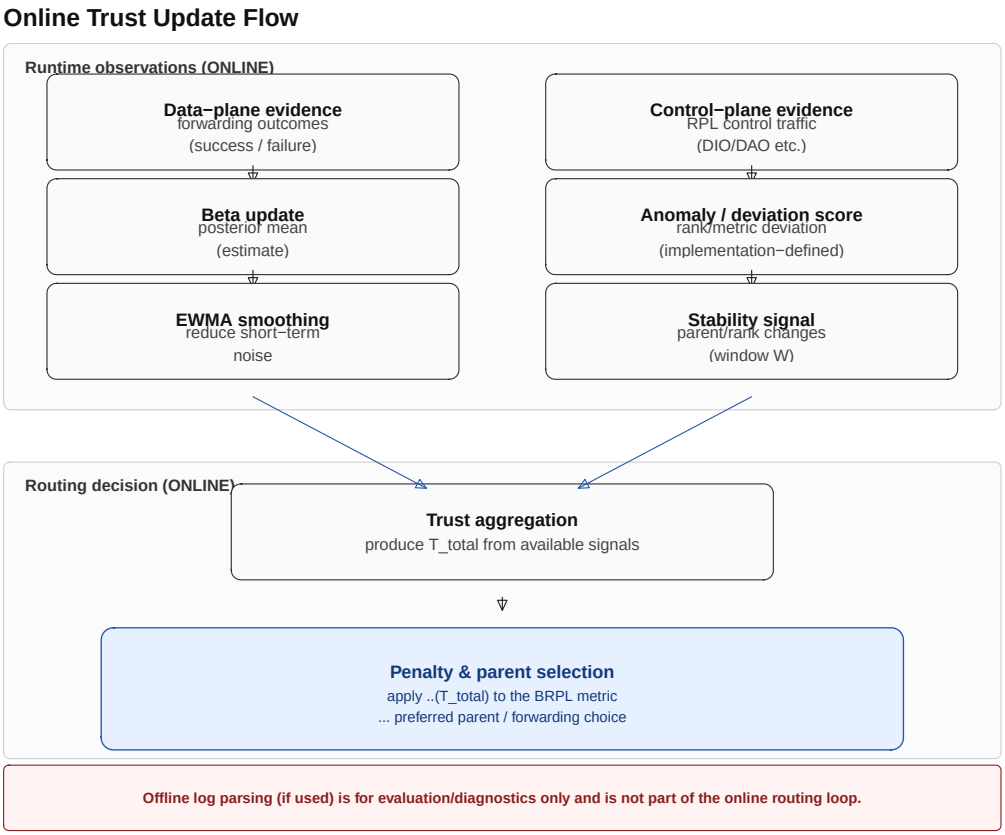

Figure 2: Online trust update and routing decision flow executed at each node during simulation runtime.

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:** $\mathrm{RX}_{\mathrm{root}}/\mathrm{TX}_{\mathrm{senders}}$.
- **End-to-end delay:** source에서 root까지의 per-packet latency.
- **Control overhead:** control-plane transmission(예: DIO/DAO) 및 routing-related overhead.
- **Parent churn:** parent switching rate로, routing stability를 반영.
- **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.

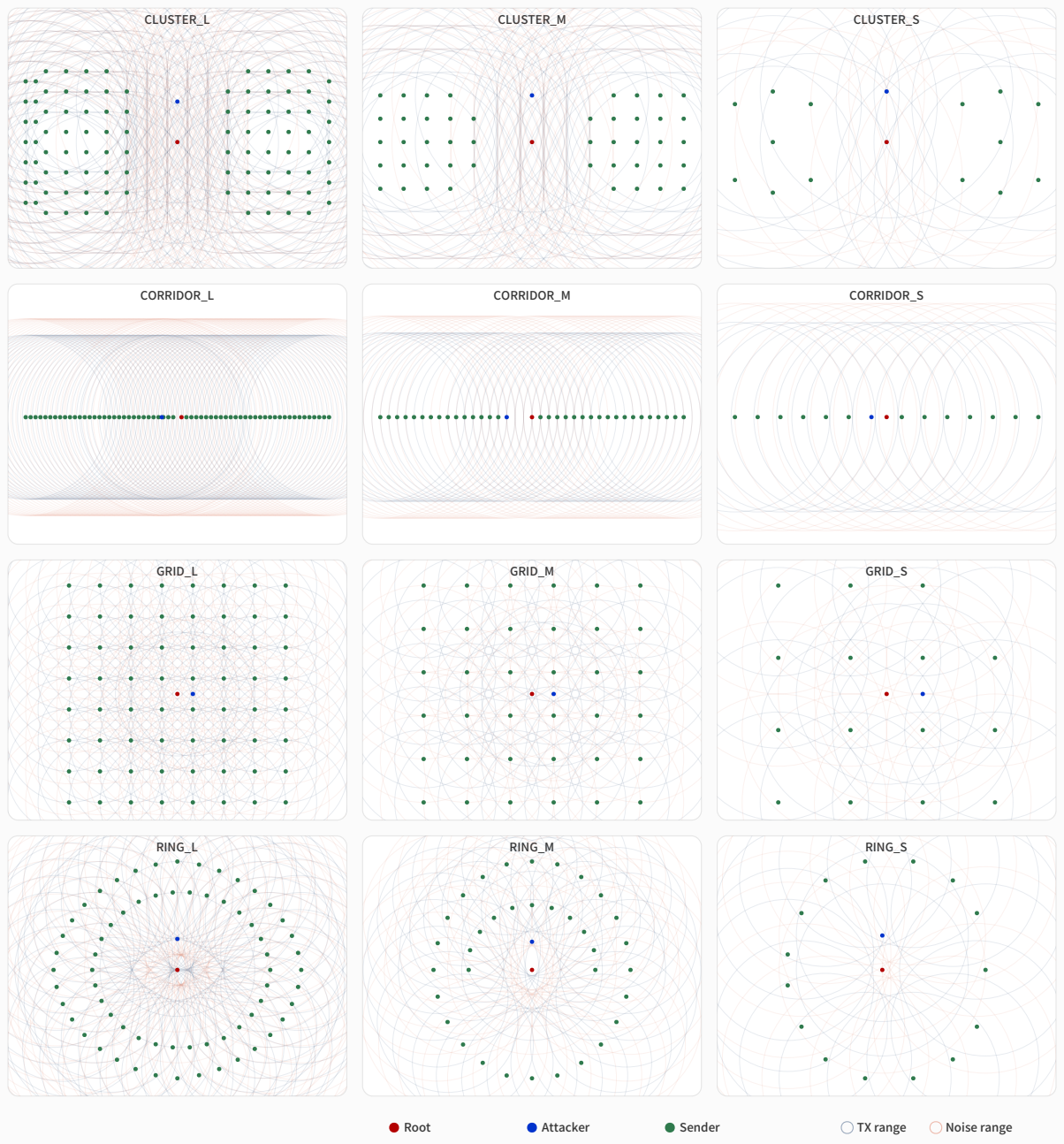

Figure 3: Topology layouts used for evaluation, covering different path diversity regimes and attacker positions.

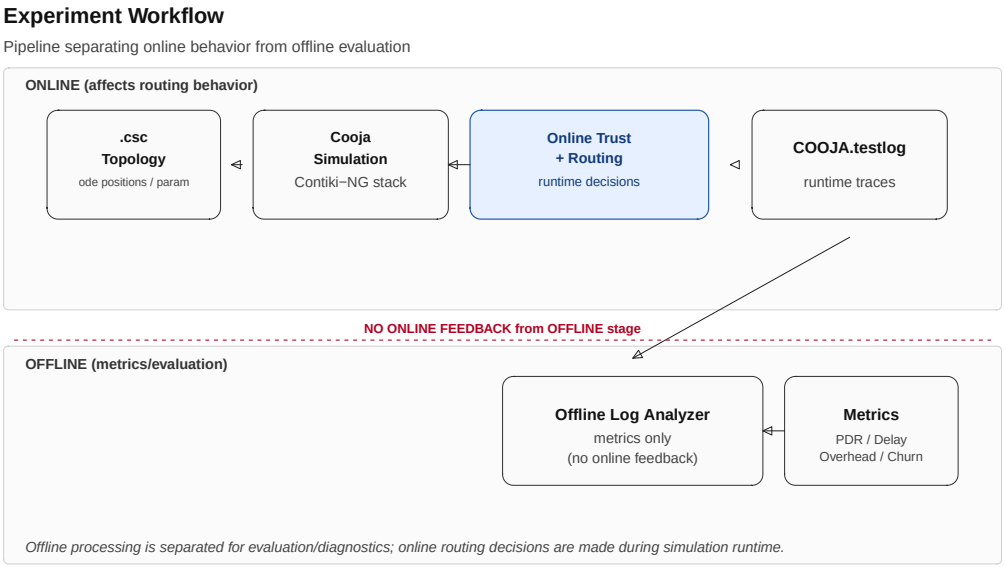

Figure 4: Experiment workflow from simulation execution to offline metric extraction.

Fig. 3 (placeholder): PDR vs. attack intensity by topology/scale

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

7 Results

본 절은 데이터 수집 이후 최종화한다. 분석은 (i) collapse threshold behavior와 (ii) trust penalization으로 유발되는 trade-off를 강조하도록 구성한다.

8 Discussion

Topology-dependent path diversity와 attacker placement가 collapse threshold에 미치는 영향, 그리고 trust penalization이 threshold를 어떻게 이동시키는지 논의한다. 또한 (i) wireless loss 및 transient dynamics에서의 false positive 가능성, (ii) $(\lambda, \gamma, \alpha)$에 대한 sensitivity, (iii) churn 및 overhead에 반영되는 stability 영향을 분석한다. 제안 메커니즘은 cryptographic protection 및 secure bootstrapping을 *대체*하는 것이 아니라 *보완*하기 위한 것으로, full authentication이 불가능하거나 비실용적인 환경에서도 resilience gain을 제공하는 것을 목표로 한다.

9 Conclusion and Future Work

본 논문은 data-plane reliability 및 control-plane anomaly signal을 함께 활용하여 BRPL routing decision에 경량 trust penalty를 통합한 Trust-Aware BRPL을 제시하였다. 평가 설계는 selective forwarding 및 sinkhole attack 하에서 trust parameter가 performance collapse를 얼마나 지연시키는지 정량화하고, topology 및 scale 전반에서 resilience–overhead trade-off를 특성화하도록 구성된다. 향후 연구로는 colluding multiple attacker, trust penalty parameter의 adaptive tuning, real testbed에서의 validation을 포함한다.

References

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

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)

[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.

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

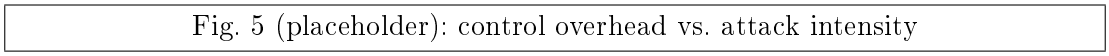

Figure 7: Control overhead vs. attack intensity (placeholder).

[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.

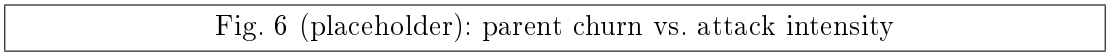

Figure 8: Parent churn vs. attack intensity (placeholder).

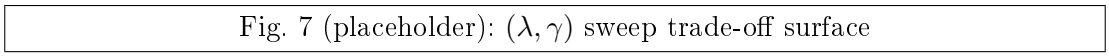

Figure 9: Trade-off under trust penalty sweeps (placeholder).