Machine Learning-Based Detection and Defense Against Routing Attacks in Delay Tolerant Networks

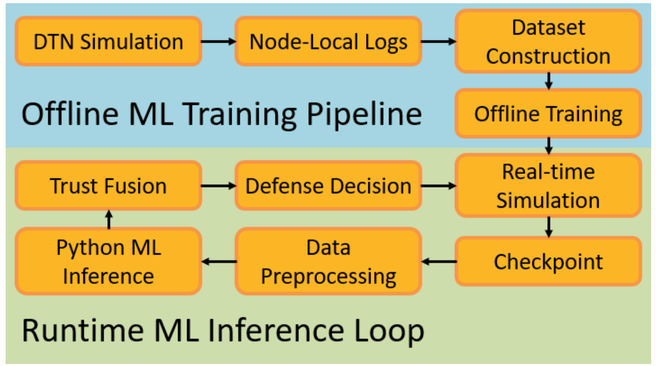
Will Cai, Computer Science
Mentor: Ozgur Ozmen, Assistant Professor
School of Computing and Augmented Intelligence

Background and Threat Model

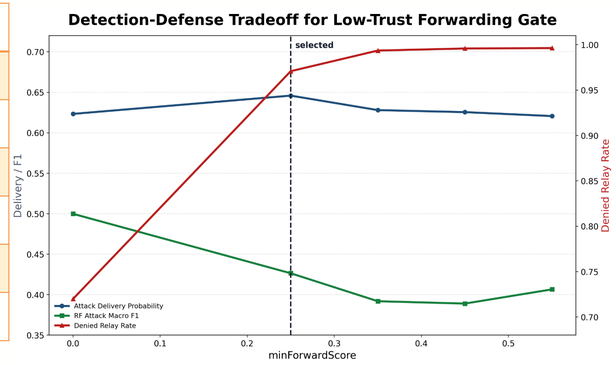
Delay Tolerant Networks (DTNs) rely on store-carry-forward relays under intermittent connectivity. This makes them vulnerable to routing attacks that reduce delivery reliability. We study flooding, grayhole, selective forwarding, and adaptive attack, with adaptive attack being the most difficult due to its trust-driven switching behavior.

System Overview

Our framework is built on The ONE simulator and combines machine learning with trust-based ratings. Each node uses only local observations to detect malicious behavior and perform real-time inference. The resulting ML-based trust score is then fused with rating-based trust to guide subsequent detection and defense decisions.



Simulation Time	7200 s
Routing Core	PROPHET-based Router
Window Size	300 s
ML Interval	120 s
Trust Fusion Weight	70%
Forwarding Threshold	0.25
Main Model	Random Forest

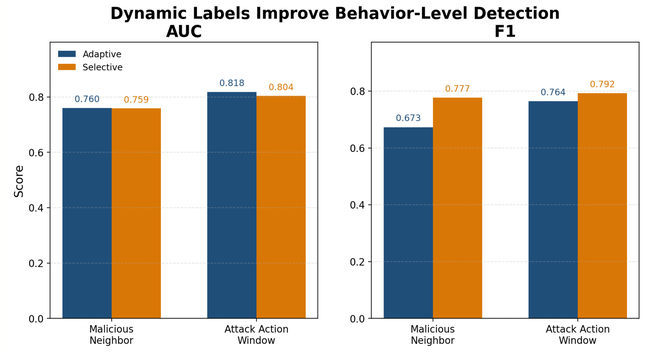


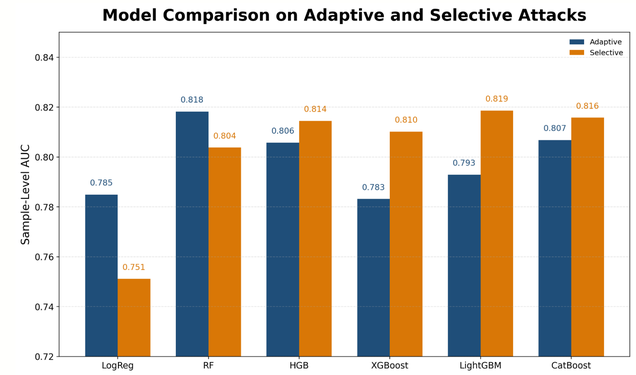
Defense Tradeoff

We tuned system parameters to balance detection accuracy, trust stability, and network performance. The final configuration supports a practical, trust-aware defense loop rather than only offline analysis.

Main Results

We evaluated Logistic Regression, Random Forest, HistGradientBoosting, XGBoost, LightGBM, and CatBoost. Random Forest achieved the strongest overall performance and performed best on the most difficult scenario: adaptive attacks.





Conclusion

Machine learning can effectively detect and stop malicious behavior in DTN.
Among the tested models, Random Forest provides the best overall performance, especially against adaptive attacks.
The three-label design significantly improves behavior-level detection by separating malicious identity from actual attack actions.
Real-time ML inference and trust fusion further enable a practical closed-loop defense framework for DTNs.

FURI

Ira A. Fulton Schools of Engineering
Arizona State University