Early Detection of Signaling Storms in RAN

Yasintha Rumesh[1], Ege Alper[1], Pawani Porambage[1,2], Samuel Marchal[1], and Sumudu Samarakoon[2]
[1]VTT Technical Research Centre of Finland
[2]University of Oulu, Finland

Problem Definition & Motivation

- Signaling storm (SS) attacks overload radio resource control (RRC) layer in radio access network (RAN)
- Initial RRC setup messages (Msg3-Msg5) are unencrypted and weakly bound to UE identity [1]
- Malicious user equipments (UEs) can trigger repeated RRC attempts with controlled delays
- **Result:** gNB RRC capacity exhaustion → RRC rejection → Denial of access to gNB services
- **Goal:** Detect SSs before the first RRC rejection occurs

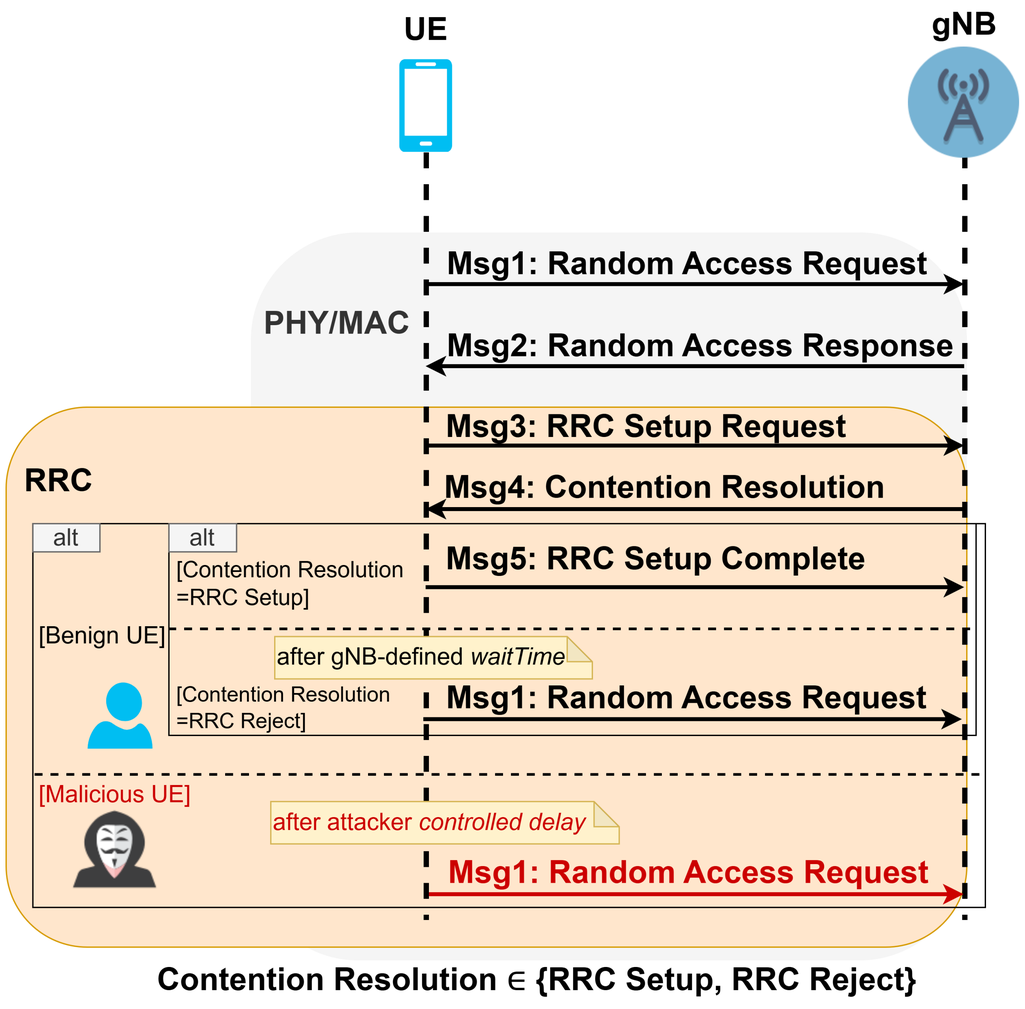

Figure 1. Initial random-access procedure (Msg1-Msg4) and RRC connection establishment procedure (Msg3-Msg5) under benign traffic [1] and SS attack.

Log-Rank Detector

- gNB-level detector using observable RRC events
- Monitored statistic: RRC setup completion duration. i.e., if Msg5 is observed, Msg4-Msg5 duration; else, right-censored at drop out time.
- Survival analysis comparison:
  - Global survival function (benign, offline)
  - Local survival function (recent traffic, online)
- One-sided log-rank test for statistically significant shift
- False positive rate (FPR) is controlled via Bonferroni-adjusted α_B

Experimenting

- Validation with over-the-air 5G RAN testbed
- Comparison against: Static [2] and Transient UE [3] detectors

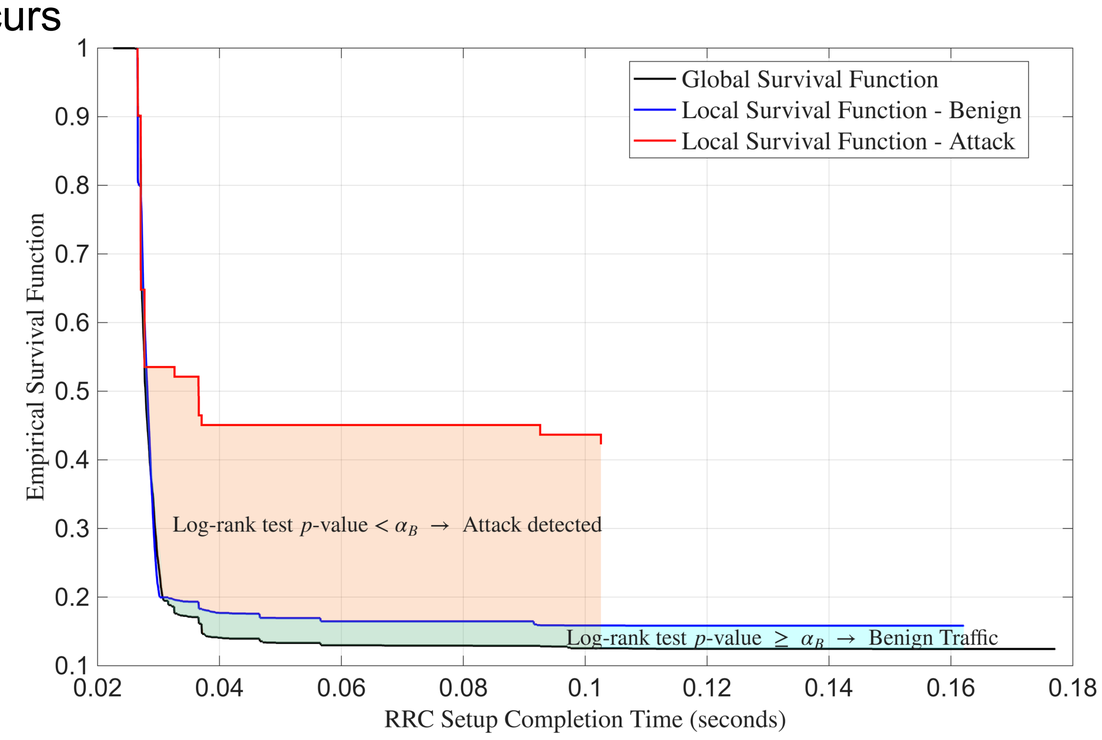

Figure 2. Survival functions of RRC setup completion times. RRC setup completes in benign survival functions (local/global) leading to a steep decay. During SSs, incomplete and delayed RRC setup procedures accumulate, causing an increased right-censoring. The one-sided log-rank test detects this statistically significant shift.

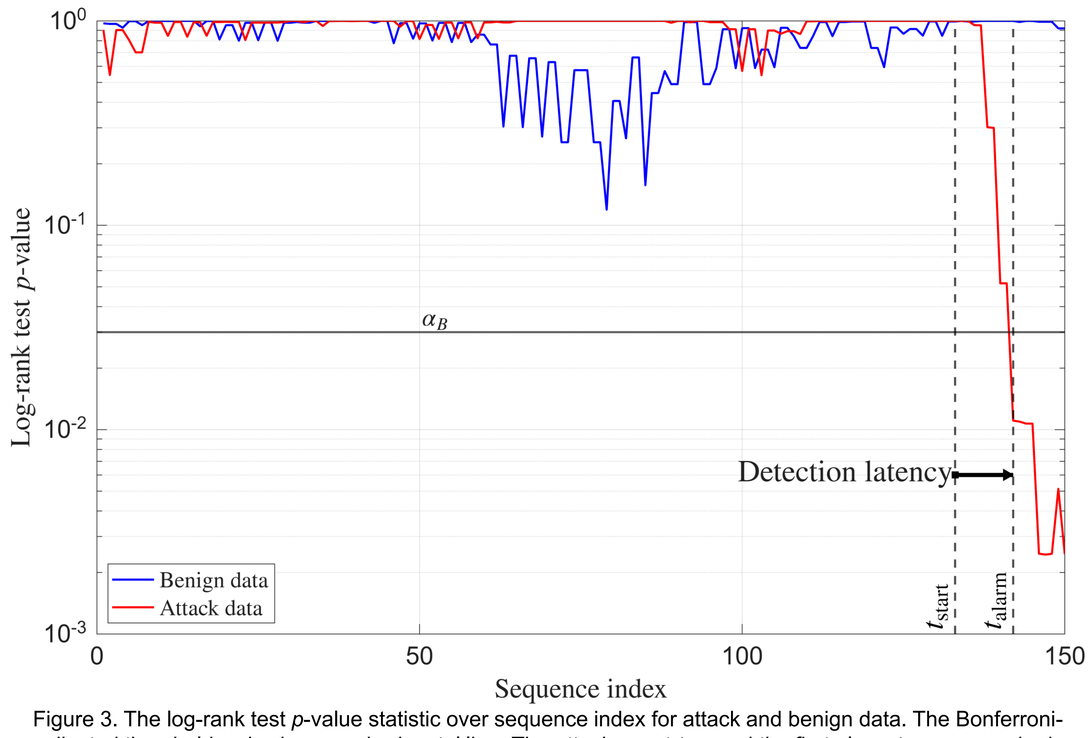

Figure 3. The log-rank test p-value statistic over sequence index for attack and benign data. The Bonferroni-adjusted threshold α_B is shown as horizontal line. The attack onset t_{start} and the first alarm t_{alarm} are marked.

Table 1. Median detection latency in seconds for adversarial attack rates evaluated under benign Msg1 arrival rate in reference data . No detection from the detector indicated by "-".

λ (Msg1s^{-1})	1				4			
Empirical - Attack rate (Msg1s^{-1})	1.08	2.08	3.12	4.53	1.09	2.08	3.10	4.49
Static [2]	43.22	-	-	-	12.16	2.8	2.9	**0.6**
Transient UE [3]	-	2.6	1.96	1.36	1.78	1.58	**1**	1.08
Log-Rank	**2.14**	**1.89**	**1.28**	**1.1**	**1.04**	**0.74**	**1**	1.06

Key Takeaways

- **Generalizable across different traffic intensities.**
- **Consistent early detection even under adversarial attackers.**
- **Minimal parameter tuning.**
- **The Log-Rank detector is robust, tunable, and deployment friendly.**

[1]. 3GPP, "NR; Radio Resource Control (RRC); Protocol Specification,"3rd Generation Partnership Project (3GPP), TS 38.331.
[2]. D. K. Nguyen, R. E. Malki and F. Rebecchi, "RRC Signaling Storm Detection in O-RAN," 2025 IEEE Symposium on Computers and Communications (ISCC), Bologna, Italy, 2025, pp. 1-7, doi: 10.1109/ISCC65549.2025.11326128.
[3]. Wen, Haohuang, Phillip A. Porras, Vinod Yegneswaran, Ashish Gehani, and Zhiqiang Lin. "5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service." NDSS. 2024.

www.vttresearch.com

Contact: Yasintha Rumesh
Email: firstname.lastname@vtt.fi

Acknowledgements: XcARet project funded by Research Council of Finland.

beyond the obvious