Timing vs Covert Detours: A Benchmarking Study in Path Validation

Dorine CHAGNON[(1)] dorine.chagnon@doctorant.uca.fr
Gérard CHALHOUB[(1)] gerard.chalhoub@uca.fr
Kevin THIRY-ATIGHEHCHI[(2)] kevin.thiry@ecole-air.fr

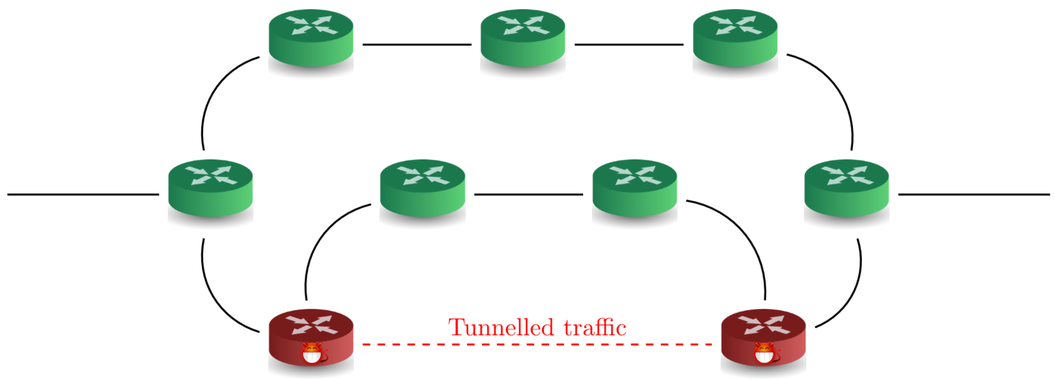
[(1)]LIMOS, Université Clermont-Auvergne, CNRS, Mines Saint-Etienne, France
[(2)]CRéA, École de l'Air et de l'Espace, France

Objectives

1. Build a synthetic dataset of one-way delays from ns-3 simulations with configurable detour length and cross-traffic intensity under realistic queuing.
2. Derive simple flow-level delay features and compare threshold-based rules with supervised classifiers and deep autoencoders.
3. Identify regimes where delay thresholds become fragile due to overlap between direct and detoured delays.

Introduction

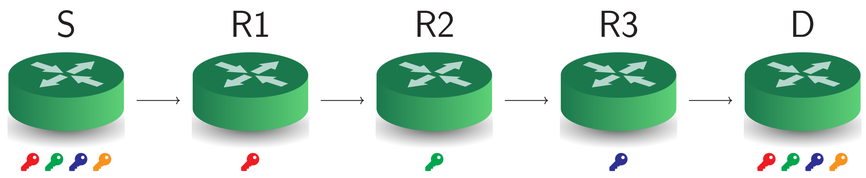
- Detour attacks, such as wormhole attack, are difficult to detect [1].
- The wormhole attack is a traffic alteration attack that creates fake links.



- Might a longer-than-expected routing path explain a potential increase in end-to-end delay?
- Most path validation protocols include timestamps within their proof [2].

Simple path validation protocol (inspired by [3])

Path P, Path Validation Field PVF, Origin and Path Validation field OPV



Initialisation by S:

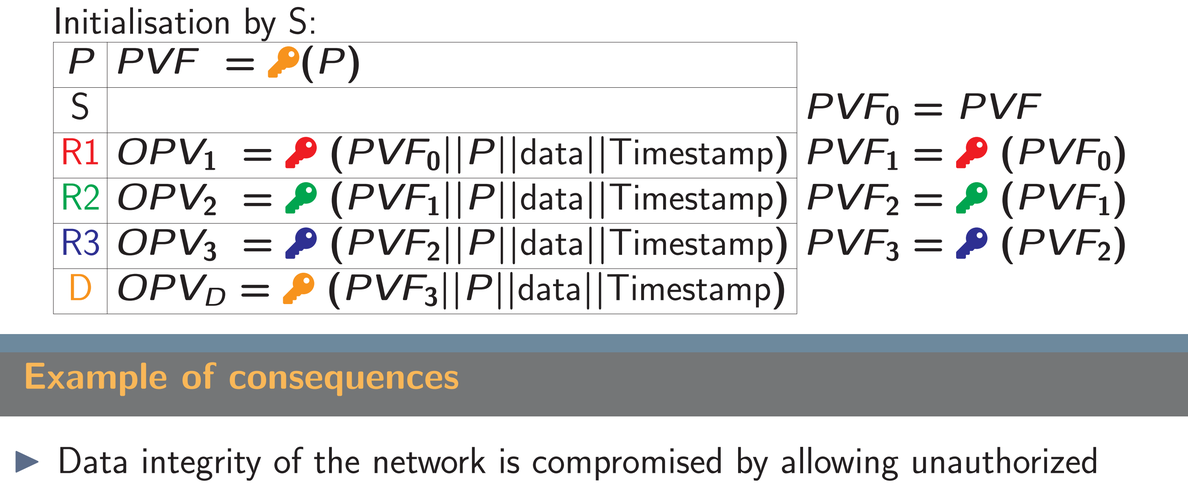
P	$PVF = \mathcal{K}(P)$	
S		$PVF_0 = PVF$
R1	$OPV_1 = \mathcal{K}(PVF_0 \| P \| \text{data} \| \text{Timestamp})$	$PVF_1 = \mathcal{K}(PVF_0)$
R2	$OPV_2 = \mathcal{K}(PVF_1 \| P \| \text{data} \| \text{Timestamp})$	$PVF_2 = \mathcal{K}(PVF_1)$
R3	$OPV_3 = \mathcal{K}(PVF_2 \| P \| \text{data} \| \text{Timestamp})$	$PVF_3 = \mathcal{K}(PVF_2)$
D	$OPV_D = \mathcal{K}(PVF_3 \| P \| \text{data} \| \text{Timestamp})$	

Example of consequences

- Data integrity of the network is compromised by allowing unauthorized access inside the tunnel to sensitive data.
- A network provider announces a certain level of service by transiting through a fast link but provides in reality a lower service.

Evolution of the variation of delays

Direct-flow delays (blue crosses) and detour-flow delays (red crosses).



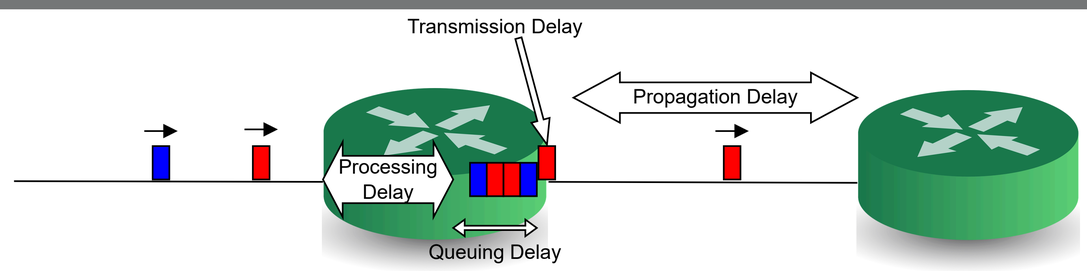
(a) 1 on-detour router

(b) 2 on-detour routers

(c) 4 on-detour routers

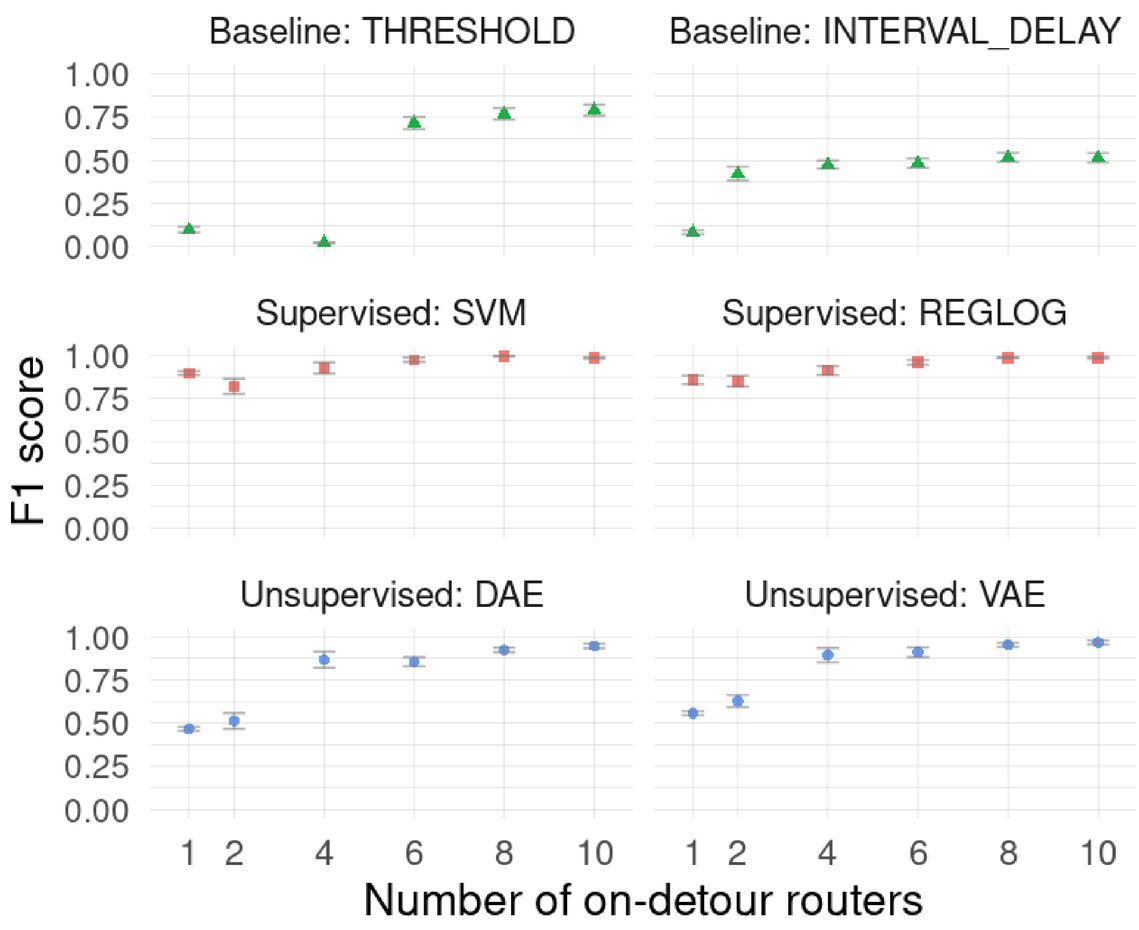
(d) 10 on-detour routers

Scheme of network delay decomposition [4]



Preliminary results of machine learning analysis

- 6 different models: 2 baseline models based on simple statistical criteria defined by Arfaoui et al.[5], 2 supervised models (Support Vector Machines (SVM) and Logistic Regression (REGLOG)) and 2 autoencoders (Denoising Autoencoder (DAE) and Variational Autoencoder (VAE)).
- F_1-scores subject of the influence of the number of on-detour routers with grey confidence interval.
- Default parameters: Flow size: 9 packets; Proportion of detoured flows: 10%; Bandwidth: 120 Mbps; Path length: 4 routers; Parasite rate: 60 Mbps.



Future Work

- Study the impact of the path length or the network congestion.
- Study the robustness of the methods when faced with unseen delay values.

Acknowledgments

- The authors acknowledge the support of the Chaire de Confiance Numérique (12LIMO11LIMOS on FCA)

References

[1] Dorine Chagnon, Kevin Thiry-Atighehchi, and Gérard Chalhoub.
A Survey on Path Validation: Towards Digital Sovereignty.
Computer Networks, 256:110905, January 2025.

[2] Kai Bu, Avery Laird, Yutian Yang, Linfeng Cheng, Jiaqing Luo, Yingjiu Li, and Kui Ren.
Unveiling the Mystery of Internet packet forwarding: A Survey of Network Path Validation.
ACM Comput. Surv., 53(5):104:1–104:34, September 2020.

[3] Tiffany Hyun-Jin Kim, Cristina Basescu, Limin Jia, Soo Bum Lee, Yih-Chun Hu, and Adrian Perrig.
Lightweight source authentication and path validation.
In *Proceedings of the ACM SIGCOMM*, pages 271–282, August 2014.

[4] James F. Kurose and Keith W. Ross.
Computer Networking: A Top-Down Approach, Global Edition.
Pearson Education, 2021.

[5] Ghada Arfaoui, Gildas Avoine, Olivier Gimenez, and Jacques Traoré.
ICRP: internet-friendly cryptographic relay-detection protocol.
Cryptogr., 6(4):52, 2022.