
# Dynamic ML Models for Evolving Networks: What, Where and How?

# Dynamic ML Models for Evolving Networks: What, Where and How?

**Aleksandra Knapińska[1,*] and Marija Furdek[2]**

[1]*Dept. of Systems and Computer Networks, Wrocław University of Science and Technology, Wrocław, Poland*
[2]*Dept. of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden*

[*]*aleksandra.knapinska@pwr.edu.pl*

**Abstract:** Modern networks and threats evolve rapidly, challenging deployed machine-learning models. We address performance degradation of offline-trained models in post-failure traffic prediction and threat detection by proposing data-stream-based updating strategies for real-time optical network resilience evolution.

## 1. Introduction

Communication networks are dynamic environments that continuously evolve and change over time. For example, traffic patterns can fluctuate daily, weekly, or in response to events such as sports championships or release of popular music albums. Optical backbone networks, as critical infrastructure, are also persistently targeted [1] by malicious actors who adapt their techniques as defenses improve. These evolving conditions introduce distribution shifts in network traffic and threat patterns. Consequently, machine-learning (ML) models used for traffic-aware network optimization [2,3] and security [4,5] can quickly become outdated, as models trained under static assumptions may struggle to generalize to changing operational conditions.

Figure 1 illustrates the behavior of static (top row) and dynamic (bottom row) models under evolving traffic conditions. When the traffic pattern matches the training data (left column), both models perform well. However, as traffic patterns change (middle and right columns), the limitations of static models become evident. A static model fails to capture subsequent amplitude and frequency variations because it lacks feedback on its performance and the evolving ground truth, leading to systematic prediction errors. In contrast, a dynamic model adapts to changing temporal characteristics and maintains accurate predictions over time.

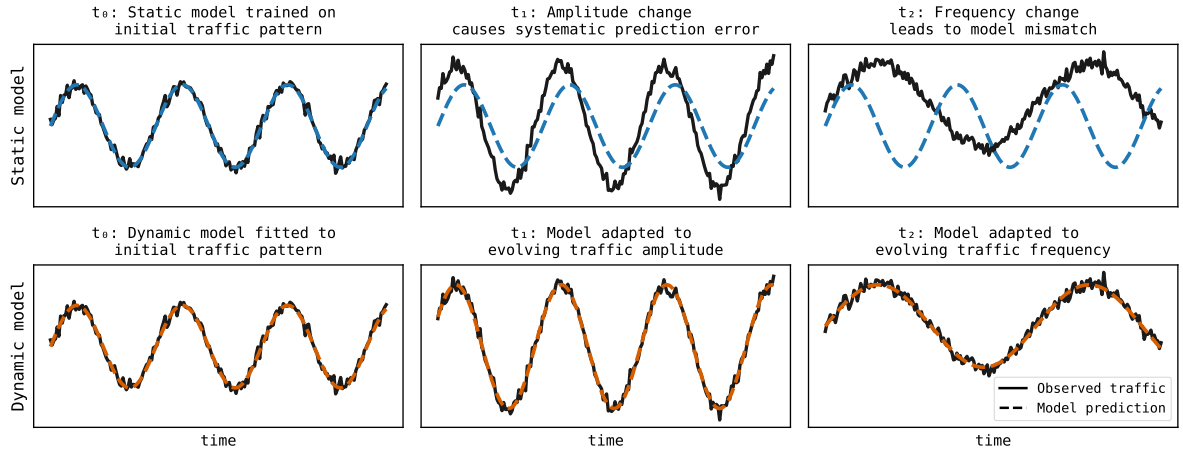


Fig. 1: Illustration of evolving traffic patterns and their impact on static (top) and dynamic (bottom) prediction models.

In this paper, we identify and study two representative evolving network tasks addressed by ML: traffic prediction in the presence of data center (DC) failures, formulated as a regression problem, and attack detection, formulated as a classification problem. We highlight the limitations of static ML models and investigate the benefits of dynamic modeling approaches in maintaining accurate predictions and effective detection as network conditions change over time.

## 2. Case study: prediction of network traffic upon data center (DC) failures

Network traffic carried by optical backbone infrastructure exhibits strong daily periodicity due to the high aggregation of individual client connections, as evidenced by public statistics from internet exchange points (e.g., [6]). Consequently, effective prediction methods can be constructed by learning the relationship between current traffic and measurements taken one day or one week earlier [7]. However, following unexpected events such as intrusions or failures, traffic on nodes and links adjacent to the failure can change rapidly and fundamentally challenge prediction accuracy [8].

This section examines a data center (DC) failure scenario in which connections are rerouted to another facility, causing rapid and substantial changes in traffic on nearby network links, on an example of the *nobel-eu* topology [9]. We simulate traffic changes on links adjacent to the failed DC, as well as in DCs which take over the rerouted traffic, resulting in a semi-synthetic dataset comprising 150 observed links. Data are collected at a 5-minute sampling rate over 67 days, with the failure occurring on day 50. Experiments are conducted using static and dynamic prediction models to forecast the bitrate for the upcoming day. Both models use a small neural network–multilayer perceptron regressor (MLP)–as the base algorithm, with traffic measurements from one day and one week earlier as input features. The static model is trained on 35 days of historical data and generates daily predictions without further updates. The dynamic model performs chunk-based ensemble learning, as proposed in [10]: it trains a small MLP each day and averages the predictions of models trained over the previous three days.

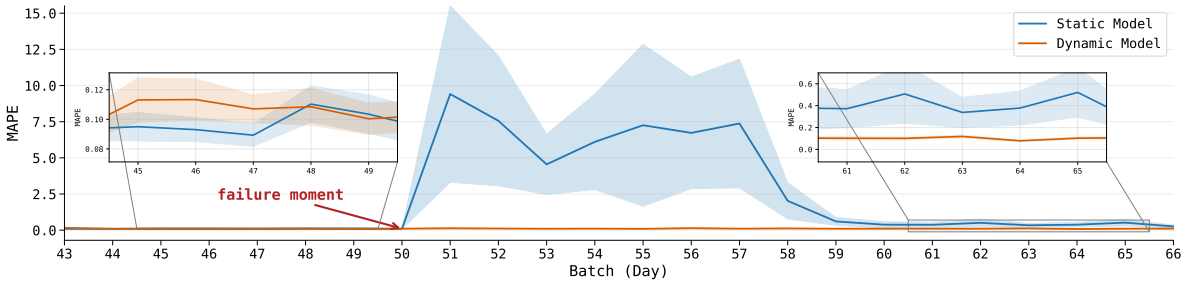


Fig. 2: Mean absolute percentage error (MAPE) over time for the static and dynamic traffic prediction algorithm, average and standard deviation from 150 datasets.

Figure 2 shows the prediction performance expressed as the mean absolute percentage error (MAPE) over time for the static and dynamic approaches. Under normal traffic conditions (before the failure), both approaches perform well, with an average MAPE of around 10%. When the traffic pattern shifts due to the failure on day 50, the prediction error of the static approach increases sharply, while the dynamic model adapts quickly. After approximately ten days of highly unreliable predictions, the static model returns to a more stable regime; however, its error does not recover to pre-failure levels. In contrast, the dynamic approach fully adapts and returns to the stable pre-failure MAPE level of around 10 shortly after the failure.

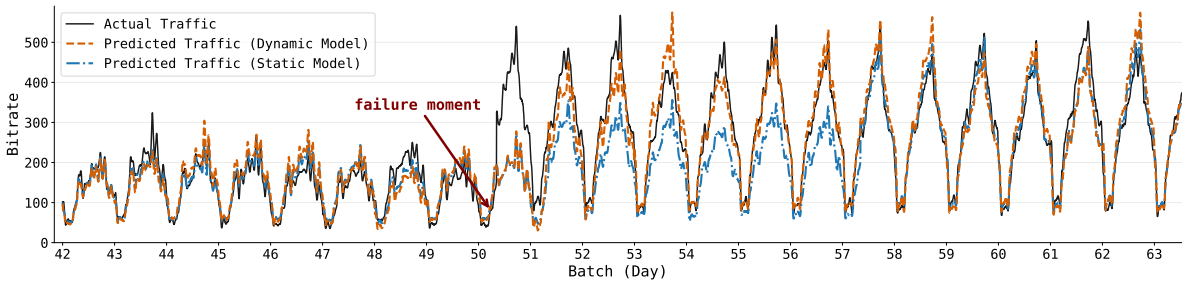


Fig. 3: Actual traffic and its predictions from the static and dynamic models around the failure happening at day 50.

Figure 3 illustrates the model behavior on a representative network link. Because it is adjacent to the failure zone, the carried bitrate increases rapidly. The failure on day 50 triggers a dramatic shift in network traffic patterns, as shown by the black solid line. The dashed lines represent the predictions of the dynamic model (orange), which quickly adapts to the new pattern and closely tracks the traffic just one day after the failure. In contrast, the static model's predictions (blue) remain unreliable for approximately one week, until the input features—based on past traffic measurements—begin to reflect the altered traffic characteristics.

## 3. Case study: detection of evolving optical layer attacks

Optical network security represents another example of an evolving problem, in which ML-based threat detection models become obsolete as malicious actors continuously refine their techniques. As a result, detection models must be regularly updated to incorporate previously unseen intrusion patterns. In this section, we examine this behavior using a physical-layer attack detection task and an experimental dataset from [11]. The dataset includes six intrusion types, i.e., light and strong in-band jamming, out-of-band jamming, and polarization scrambling.

In our experiment, optical performance monitoring (OPM) data are collected by coherent receivers and streamed to the ML analytics module. 15% of samples correspond to attacks while the rest represent normal operating conditions. After every 200 batches of 100 samples, the active attack type is changed. Similarly to the traffic prediction experiment, the static approach consists of an MLP model trained on the initial 100 batches of data and then kept fixed. In contrast, the dynamic model—also based on an MLP—is updated (*partial fit*) after each data batch using the newly acquired samples, following the approach proposed in [12]. The experiment is repeated 100 times with random attack orderings.

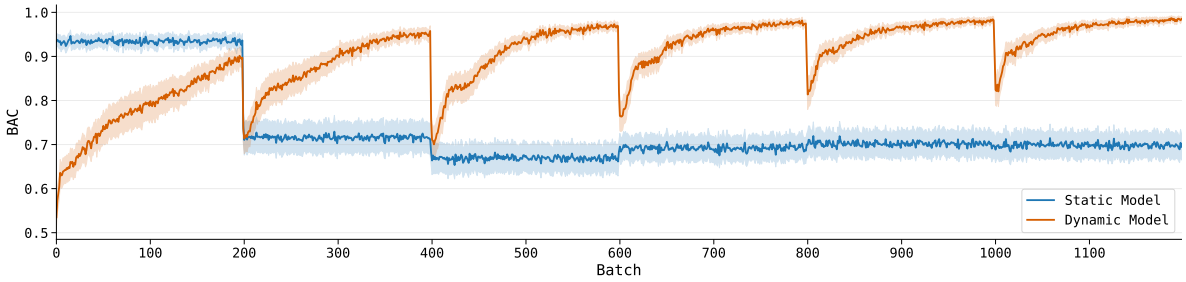


Fig. 4: Balanced Accuracy (BAC) over time for the static and dynamic attack detector, average and standard deviation from 100 experiment replications.

Figure 4 presents the results of our experiment, reporting the balanced accuracy score (BAC) and clearly demonstrating the benefits of dynamic modeling. The static model (blue) maintains a high detection accuracy above 90% until the attack type changes, after which its BAC rapidly degrades to approximately 70%. In contrast, the dynamic approach initially achieves a lower BAC of around 60%, but quickly improves as additional data batches are processed. Although the introduction of new attack types inevitably causes a temporary drop in detection accuracy, it is followed by rapid recovery. Moreover, successive attack changes result in smaller performance drops and faster convergence, highlighting the model's ability to accumulate knowledge and adapt over time.

## 4. Conclusions

In this paper, we addressed the problem of performance degradation in ML models employed for networking tasks. We demonstrated that dynamically updated models can effectively adapt to changing network conditions caused by failures or evolving attacks. Through case studies on network traffic prediction following DC failures and on detection of evolving physical-layer attacks, we highlighted the importance of dynamic ML models for reliable operation in continuously changing network environments. These results indicate that static training paradigms are insufficient for many real-world networking scenarios characterized by distribution shifts. Incorporating adaptive learning mechanisms into ML-based networking solutions is therefore a practical and necessary step toward maintaining stable and accurate performance over time.


## Acknowledgment

This work was supported by the statutory funds of the Department of Systems and Computer Networks, Wrocław University of Science and Technology, Poland, and the European Commission through the 5G-TACTIC (101127973) project.


## References


1. J. Rak *et al.*, Opt. Switch. Netw. 2021.
2. T. Panayiotou *et al.*, IEEE Commun. Surv. Tutor. 2023.
3. F. Musumeci *et al.*, IEEE Commun. Surv. Tutor. 2019.
4. M. Furdek *et al.*, J. Opt. Commun. Netw. 2020.
5. F. Musumeci *et al.*, J. Light. Technol. 2019.
6. https://www.seattleix.net/statistics/.
7. A. Knapińska *et al.*, ONDM 2024.
8. R. Goścień and A. Knapińska, ONDM 2022.
9. S. Orlowski *et al.*, Networks: An Int. J. 2010.
10. A. Knapińska *et al.*, Appl. Soft Comput. 2022.
11. M. Furdek *et al.*, J. Light. Technol. 2020.
12. A. Knapinska and M. Furdek, ECOC 2025.