DTU DTU ELECTRO
Department of Electrical and Photonics Engineering

DEPARTMENT OF ENGINEERING SCIENCE
UNIVERSITY OF OXFORD

P4Pir: In-Network Analysis for Smart IoT Gateways

Mingyuan Zang[1], Changgang Zheng[2], Radostin Stoyanov[2], Lars Dittmann[1], and Noa Zilberman[2]

[1] Technical University of Denmark, [2] University of Oxford

P4Pir Planter

➢ Problem Statement

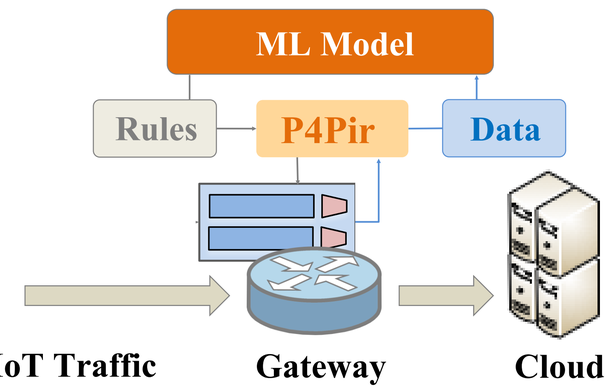
Diverse use cases
Dynamic IoT deployments
Increasing security threats

How to do traffic analysis & first-line of defense at gateway? ML? How to be efficient?

Multi-source Input	Predefined protocol stacks • Hardware-based • Software-based
	Flexible in-band data parsing?
ML Inference	Server-based ML • Network-pipeline -> CPU/GPU
	Reduced transmission overhead?
Model Update	• Unsupervised online learning • Supervised model retraining
	Reliable runtime ML update?

"Smart" IoT gateway:

Programmable Data Plane
+
In-network ML
+
Runtime rule update



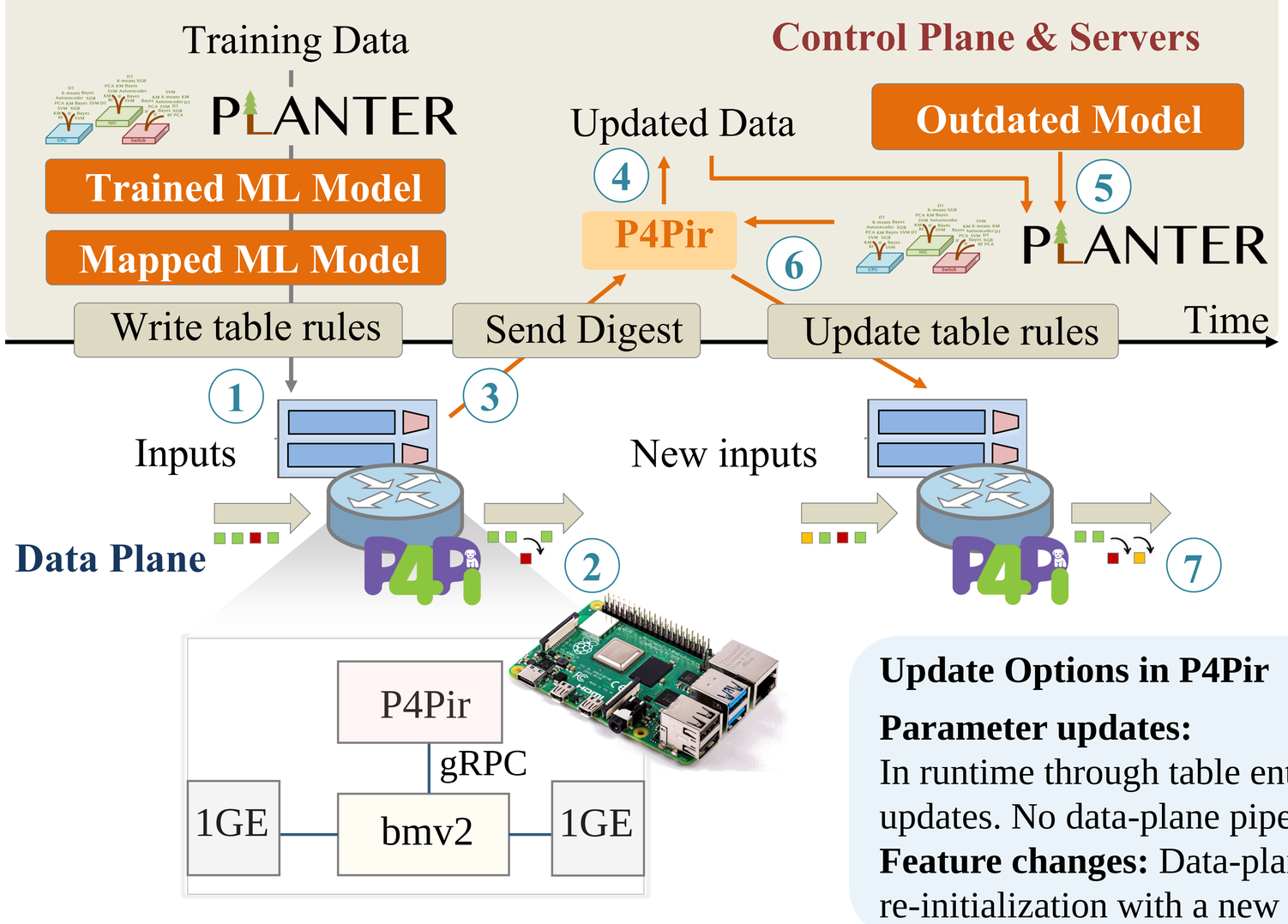
➢ System Design

Logging & Mitigation

1. Trained ML → M/A table rules & P4 code
2. Identify malicious traffic: Benign – forward; Malicious – drop & log
3. Log by encapsulating extracted features in digest

Retraining & Updating

4 + 5. P4Pir uses digest data to retrain the model and generate an updated mapping
6. Insert updated rules & Remove outdated rules
7. Detect & mitigate new abnormal traffic



Update Options in P4Pir

Parameter updates:
In runtime through table entry / control-plane updates. No data-plane pipeline updates.
Feature changes: Data-plane updates, requires re-initialization with a new P4 program.

➢ Preliminary Results

			SYN → SCAN		SYN → HTTP		SYN → UDP	
		Initial	Baseline	P4Pir	Baseline	P4Pir	Baseline	P4Pir
Decision Tree	ACC	0.995	0.460	0.998	0.360	0.999	NaN	0.886
	F1	0.998	0.630	0.998	0.530	0.999	NaN	0.939
Random Forest	ACC	0.999	0.994	0.997	0.340	0.998	NaN	0.999
	F1	0.999	0.997	0.998	0.510	0.999	NaN	0.999

Table 1: Preliminary results based on public dataset Edge-IIoTset [2]
SYN - DDoS TCP SYN attack, SCAN - vulnerability scanning attack,
HTTP - HTTP flooding attack, UDP - UDP flooding attack.
Initial: results when model only learns SYN. Baseline: results from static server-based model.

➢ Acknowledgements

This work was partly funded by the Otto Mønsted Foundation and VMWare.

➢ References

[1] Laki, Sándor, et al. "P4Pi: P4 on Raspberry Pi for Networking Education". SIGCOMM Comput. Commun. Rev. 51. 3(2021): 17–21.
[2] Ferrag, Mohamed Amine et al. "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning". IEEE Access 10. (2022): 40281-40306.