IEEE International Conference on Cyber Security and Resilience // EPES-SPR Workshop · Lisbon, Portugal · August 03–05, 2026

Federated Detection Of KNX Attacks With Network Flow Statistics In Industrial Environments

Flow Statistics for Intrusion Detection in Building Automation

Panagiotis Radoglou-Grammatikis · pradoglou@k3y.bg
C. Dalamagkas · P. Radoglou-Grammatikis · A. Sarigiannidis · E. K. Markakis · MA. Kourtis · T. Lagkas · G. Th. Papadopoulos · V. Argyriou · P. Sarigiannidis
DUTH · K3Y · HMU · NCSR Demokritos · HUA · Kingston University London · UOWM

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

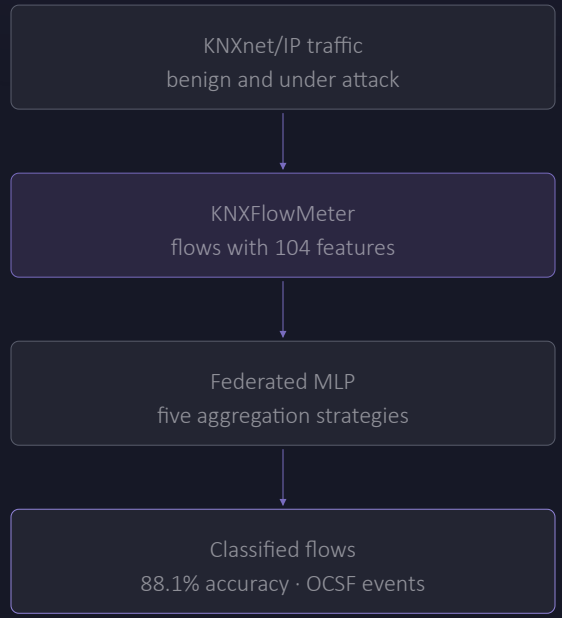
Outline

01 KNX, and why it is exposed

02 Eight attacks against KNXnet/IP

03 KNXFlowMeter and the federated IDS

04 Results and what they mean



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

01

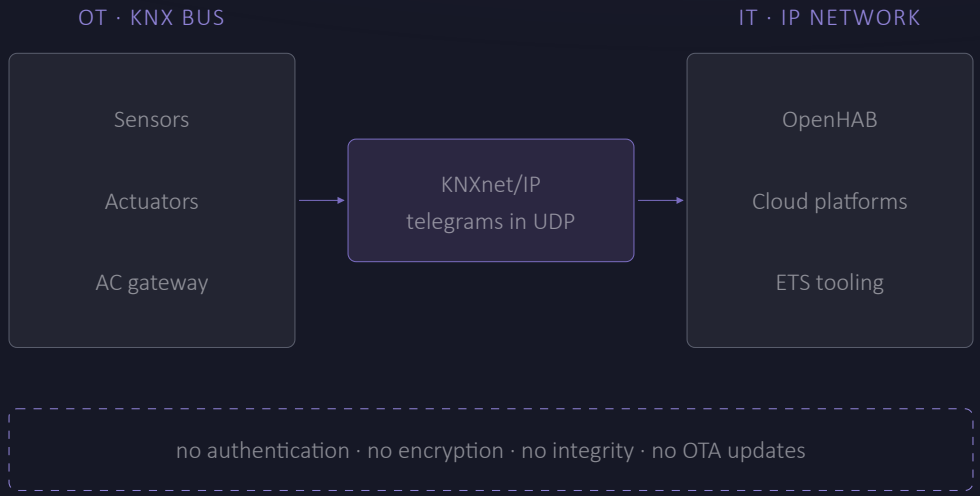
KNX, And Why It Is Exposed

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

One Bus, Now Reachable From IT

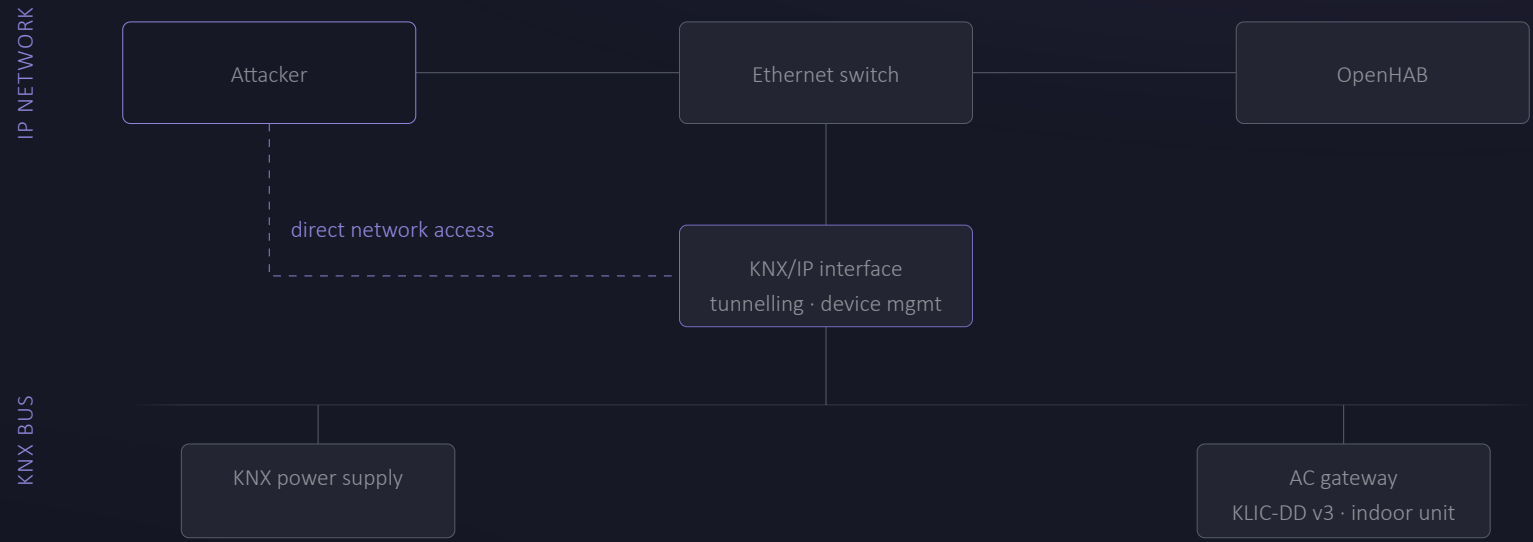
- KNX covers the whole stack — TP, powerline, radio, IP
- KNXnet/IP wraps telegrams in UDP for the IT side
- Anything that reaches the interface reaches the bus

A static risk analysis of KNX puts overall risk near 67%.



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The Testbed



The attacker reaches the interface from the LAN; the bus is then in scope.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

02

Eight Attacks Against KNXnet/IP

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The Catalogue



01 · Property fuzzing

Mutated M_PropRead.req over device management.

02 · Device reset

M_Reset.req every 125 ms drops every connection.

03 · Interface discovery

Multicast Search and Description requests.

04 · Bus scanning

DevDescrRead across a pool of addresses.

05 · Valid flood

Heartbeat writes to 0/0/2, at line rate.

06 · Randomised flood

Random source, group address and payload.

07 · Read flood

GroupValueRead — disruption plus extraction.

08 · Unauthorised access

One valid write that shuts the computer-room AC.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Management Plane: Fuzzing And Reset

- Device-management connection, then mutated M_PropRead.req
- The gateway answers — and returns the memory value
- A reset needs one unauthenticated message, repeated

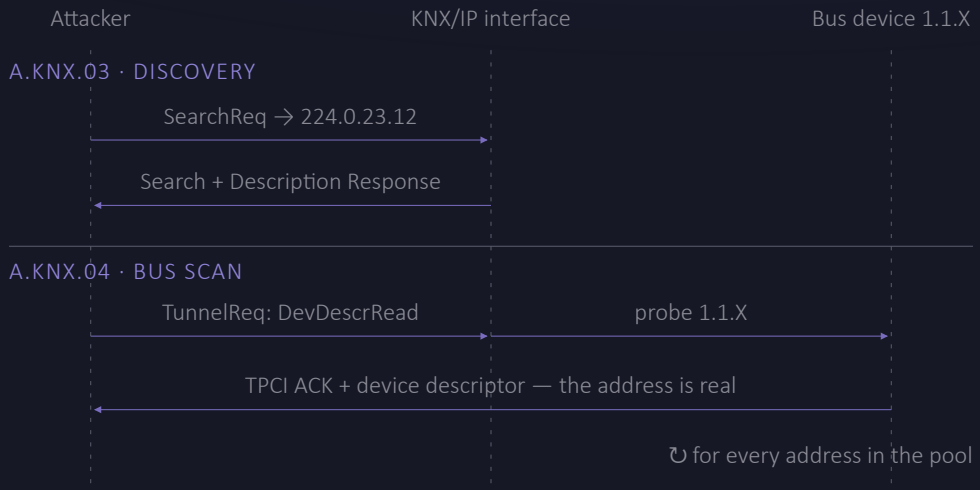


Signal — M_PropRead spread over object types; any M_Reset.req at all.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Reconnaissance: Interfaces, Then Devices

- Multicast search finds every KNX/IP interface on the LAN
- Then the bus behind it is walked, address by address
- An answer means a real device — and its descriptor



Signal — Search counts, and DevDescrRead across many addresses.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Flooding: Three Variations On One Loop

- One tunnel per telegram — connect, send, ack, disconnect
- No pause between iterations; the gateway pays for each
- Only the telegram in the middle changes across 05, 06, 07



THE TELEGRAM IN THE MIDDLE

- 05 · **GroupValueWrite** to 0/0/2
  a valid heartbeat — only the rate is wrong
- 06 · same write, randomised addresses
  source IA, group address and payload
- 07 · **GroupValueRead** instead
  disruption, plus state pulled back out

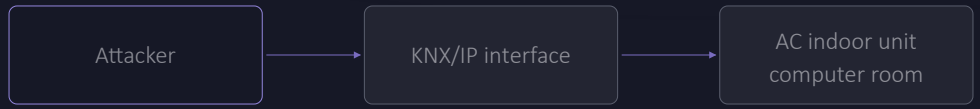
Signal — group-service counts, and unique addresses rising with them.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

A.KNX.08 — One Message, No Statistics

- One well-formed write to a sensitive group address
- 0/0/54 closes the computer room's AC indoor unit
- Ordinary rate, ordinary shape — nothing to flag

A rule, not a model — legitimate group addresses are known at commissioning.



GroupValueWrite → 0/0/54 · close

WHAT THE FLOW RECORD SEES

Operator, via ETS	=	Attacker
1 write · 0/0/54 · 1 packet		1 write · 0/0/54 · 1 packet

identical statistics — nothing for a model to learn

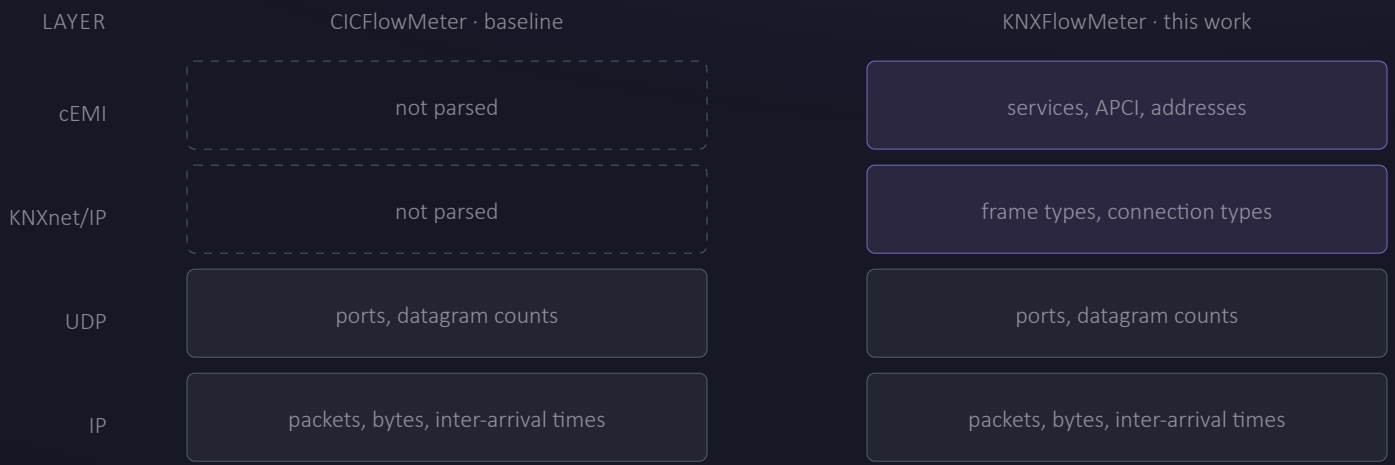
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

03

KNXFlowMeter And The Federated IDS

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Where The Evidence Lives

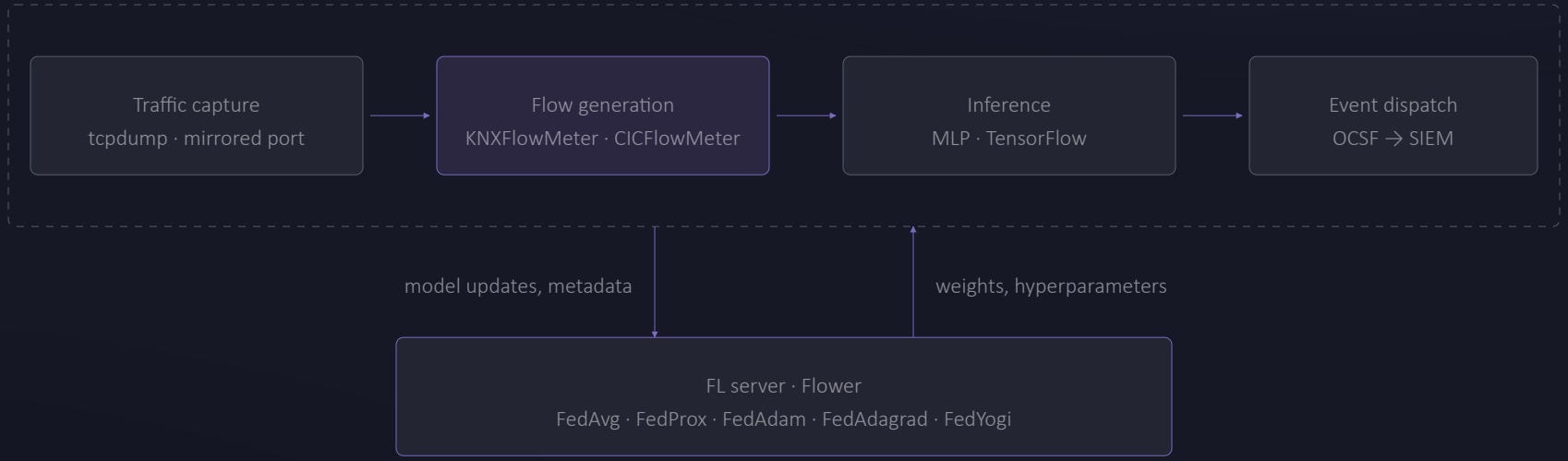


Every observation from the attack analysis sits in the upper two layers — and UDP leaves the baseline no TCP cues to fall back on. KNXFlowMeter emits 104 features.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The IDS, And The Federated Loop

NETWORK IDS / FL CLIENT — ONE PER SITE



Raw traffic never leaves the site — only model updates do.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

How The Local Models Are Merged

FedAvg



The weighted mean of the client models, by sample count.

$w_{t+1} = \Sigma_k (n_k/n)\, w_k$

FedProx



A proximal term keeps each client near the global model.

$\min F_k(w) + (\mu/2)\|w - w_t\|^2$

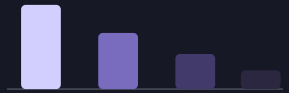
FedAdam



Momentum and a decayed second moment smooth the server step.

$w_{t+1} = w_t + \eta\, m_t / (\sqrt{v_t} + \tau)$

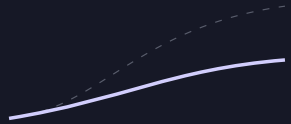
FedAdagrad



Squared updates accumulate, so the step size only shrinks.

$v_t = v_{t-1} + \Delta_t^2$

FedYogi



The same idea, with the second moment held from growing too fast.

$v_t = v_{t-1} - (1-\beta_2)\Delta_t^2$

$\mathrm{sign}(v_{t-1} - \Delta_t^2)$

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

04

Results And What They Mean

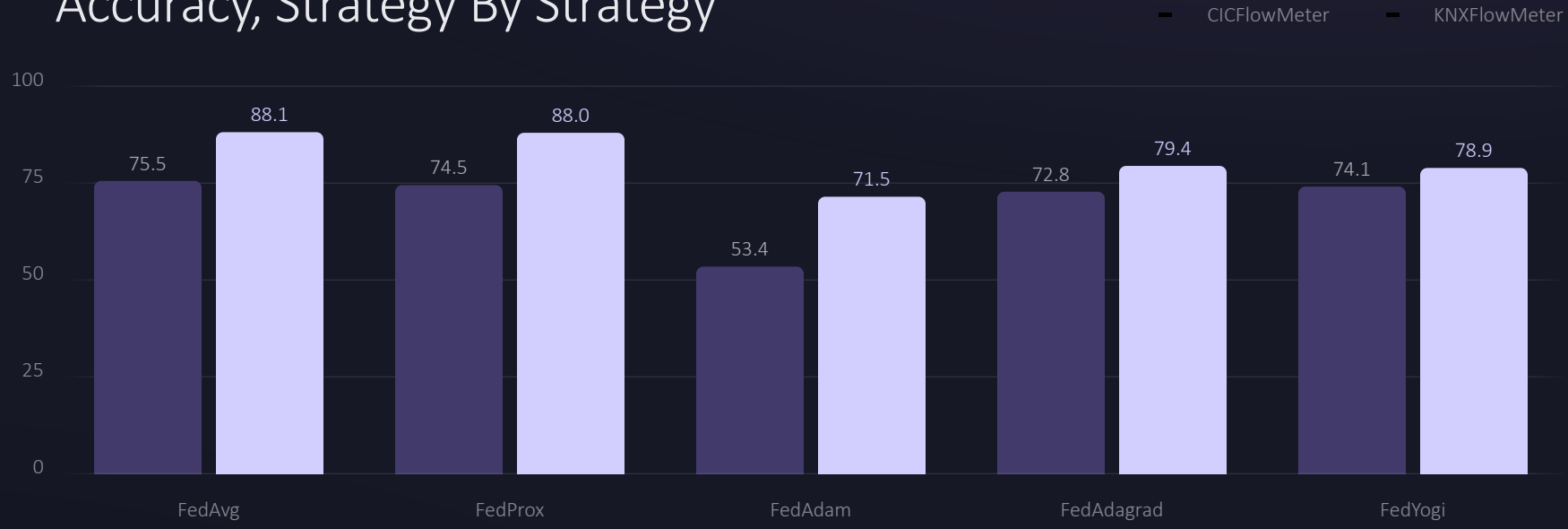
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Same Traffic, Same Model, Two Flow Records

AGGREGATION STRATEGY	ACC · CIC	ACC · KNX	F1 · CIC	F1 · KNX	FPR · CIC	FPR · KNX
FedAvg	75.53%	88.12%	72.34%	85.76%	4.07%	1.97%
FedProx	74.47%	87.95%	73.67%	87.54%	4.25%	2.01%
FedAdam	53.43%	71.46%	48.78%	64.33%	7.76%	4.75%
FedAdagrad	72.75%	79.41%	70.16%	75.69%	4.54%	3.42%
FedYogi	74.07%	78.89%	70.68%	75.25%	4.32%	3.51%

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Accuracy, Strategy By Strategy



Accuracy in percent — the gain holds under every strategy.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

What We Take From This

- Application-layer visibility decides it — roughly 20% across the metrics
- Federation is practical: traffic stays on site, FedAvg stays strongest
- Rules cover what statistics cannot

Next — explainability over the 104 features, then a tighter feature set.



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Thank You

Questions · Answers

Panagiotis Radoglou-Grammatikis · pradoglou@k3y.bg

C. Dalamagkas · P. Radoglou-Grammatikis · A. Sarigiannidis · E. K. Markakis · MA. Kourtis · T. Lagkas · G. Th. Papadopoulos · V. Argyriou · P. Sarigiannidis

DUTH · K3Y · HMU · NCSR Demokritos · HUA · Kingston University London · UOWM



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225719 (SALUS) — Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.