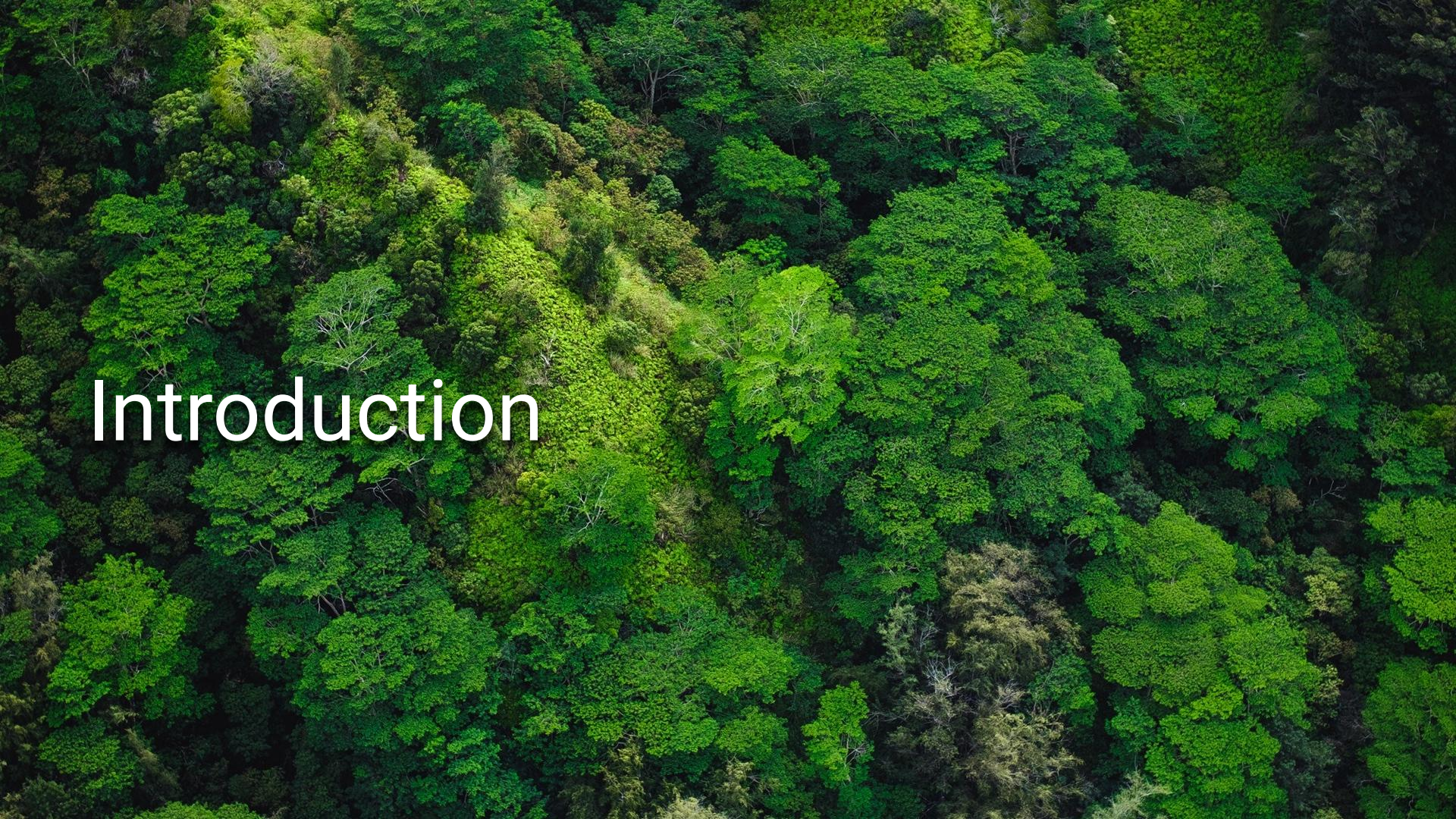
pForest: In-Network Inference with Random Forests

Adrien Prost
Benno Schneeberger
Roberto Rossini


Introduction

Problem Context

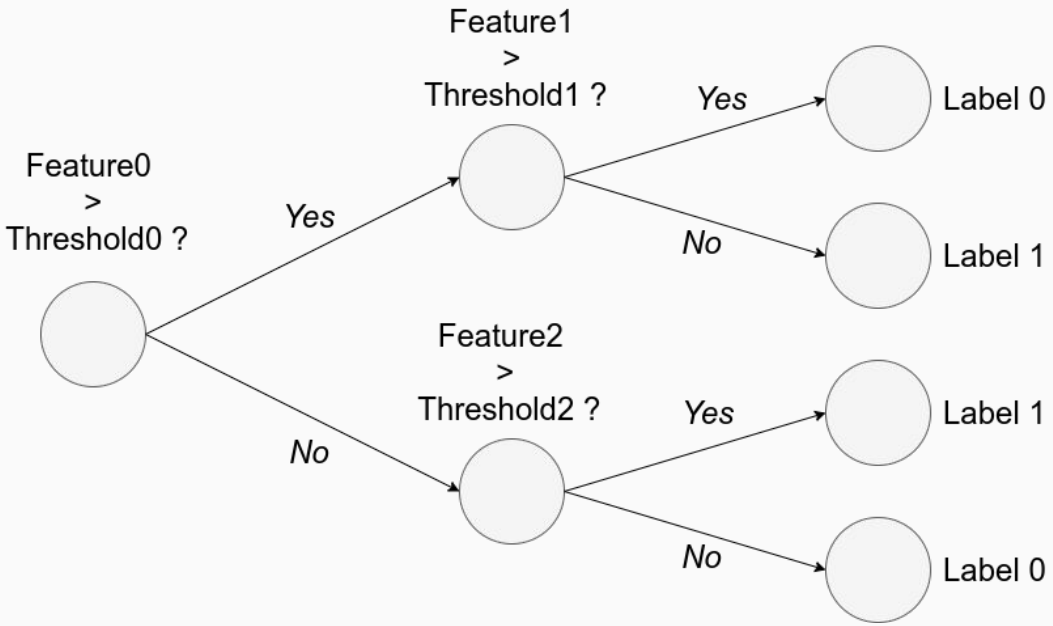
- Malicious traffic can be detected using machine learning models
- Detection is faster and more effective if the classifier can be integrated directly on the data plane
- How do we fit the model in a switch with limited capabilities?

pForest

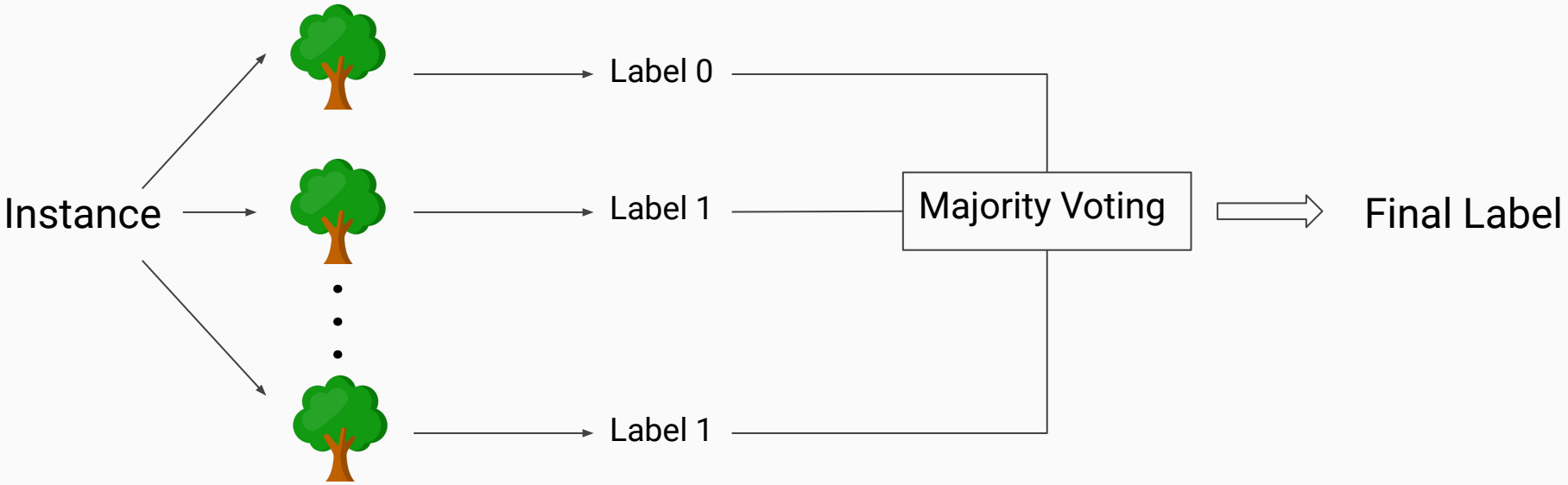
- Multiple Random Forest models trained on packet flow statistics
- Framework for efficiently integrating the models in ***P4***

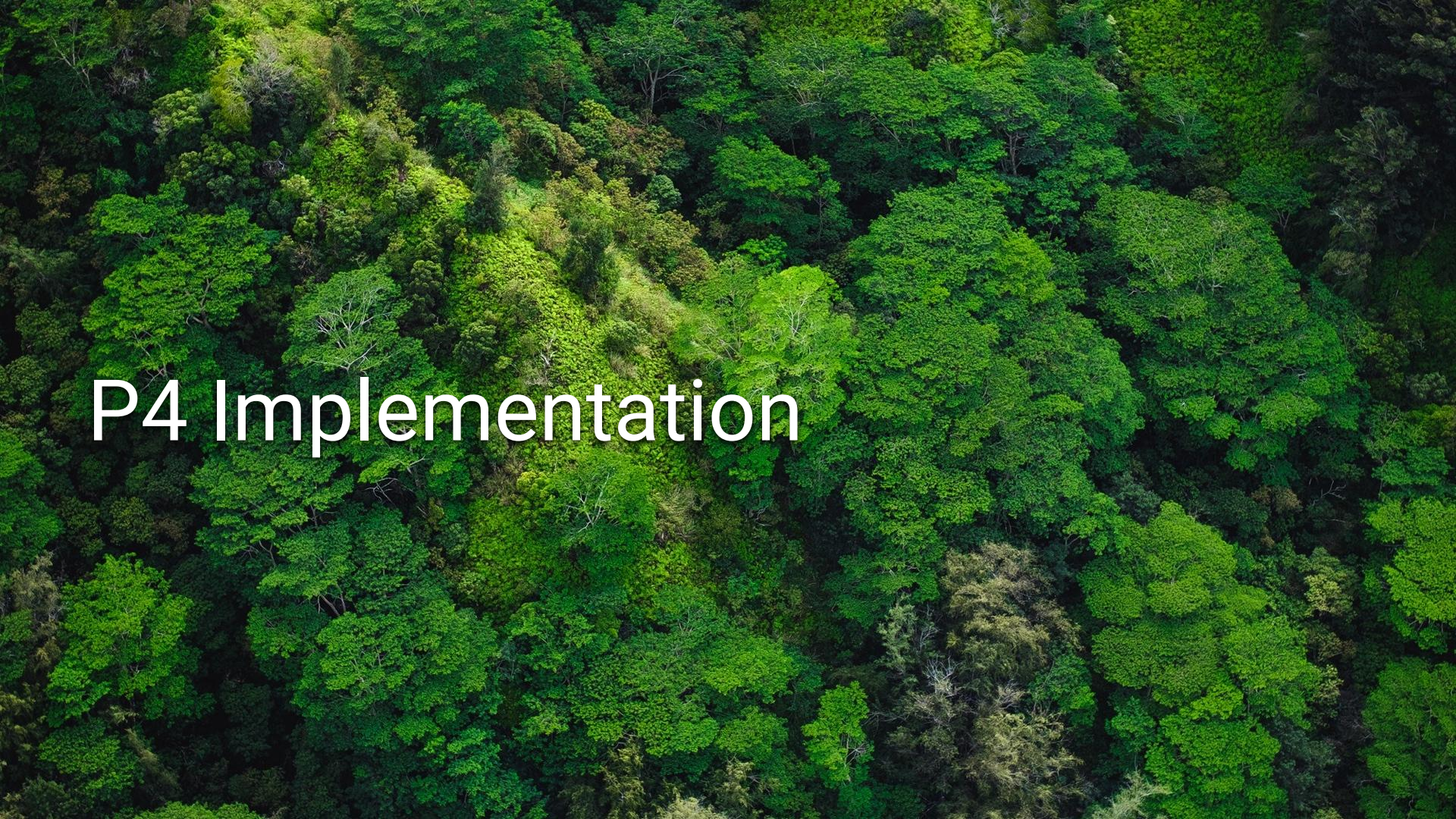

Random Forest Classifier

Decision Tree



Random Forest Classifier




P4 Implementation

Flow Features

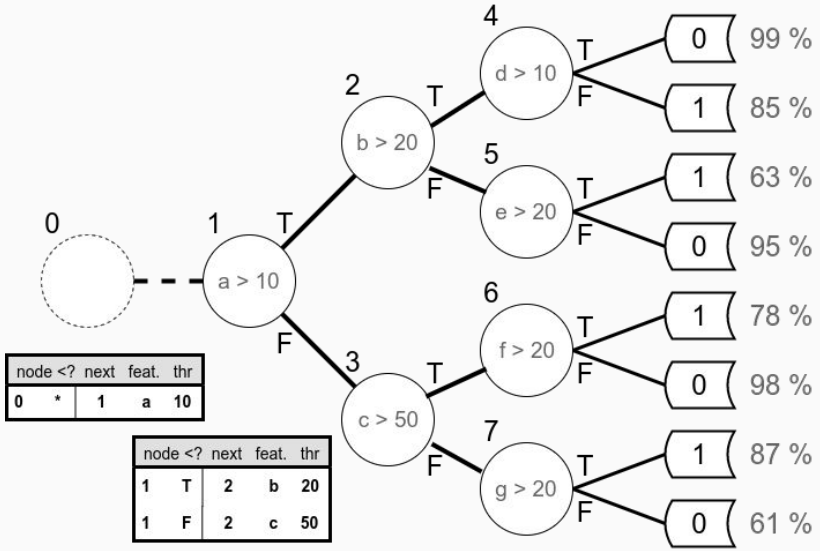
- Packets are classified according to various statistics of their flow :
  - Packet Inter-arrival time
  - Packet length
  - Flow duration
  - TCP flag counts
  - Number of packets

Handling Features

- Switch maintains multiple registers to store flow features
- Storage is organized using hash tables
- Features are updated at each subsequent packet of the same flow

Random Forest to Table Entries

- One match-action table per decision tree per level



node	<?	next	feat.	thr
0	*	1	a	10

node	<?	next	feat.	thr
1	T	2	b	20
1	F	2	c	50

node	<?	next	feat.	thr
2	T	4	d	10
2	F	5	e	20
3	T	6	f	20
3	F	7	g	20

node	<?	label	certainty
4	T	0	99 %
4	F	1	85 %
5	T	1	63 %
5	F	0	95 %
6	T	1	78 %
6	F	0	98 %
7	T	1	87 %
7	F	0	61 %

Classification

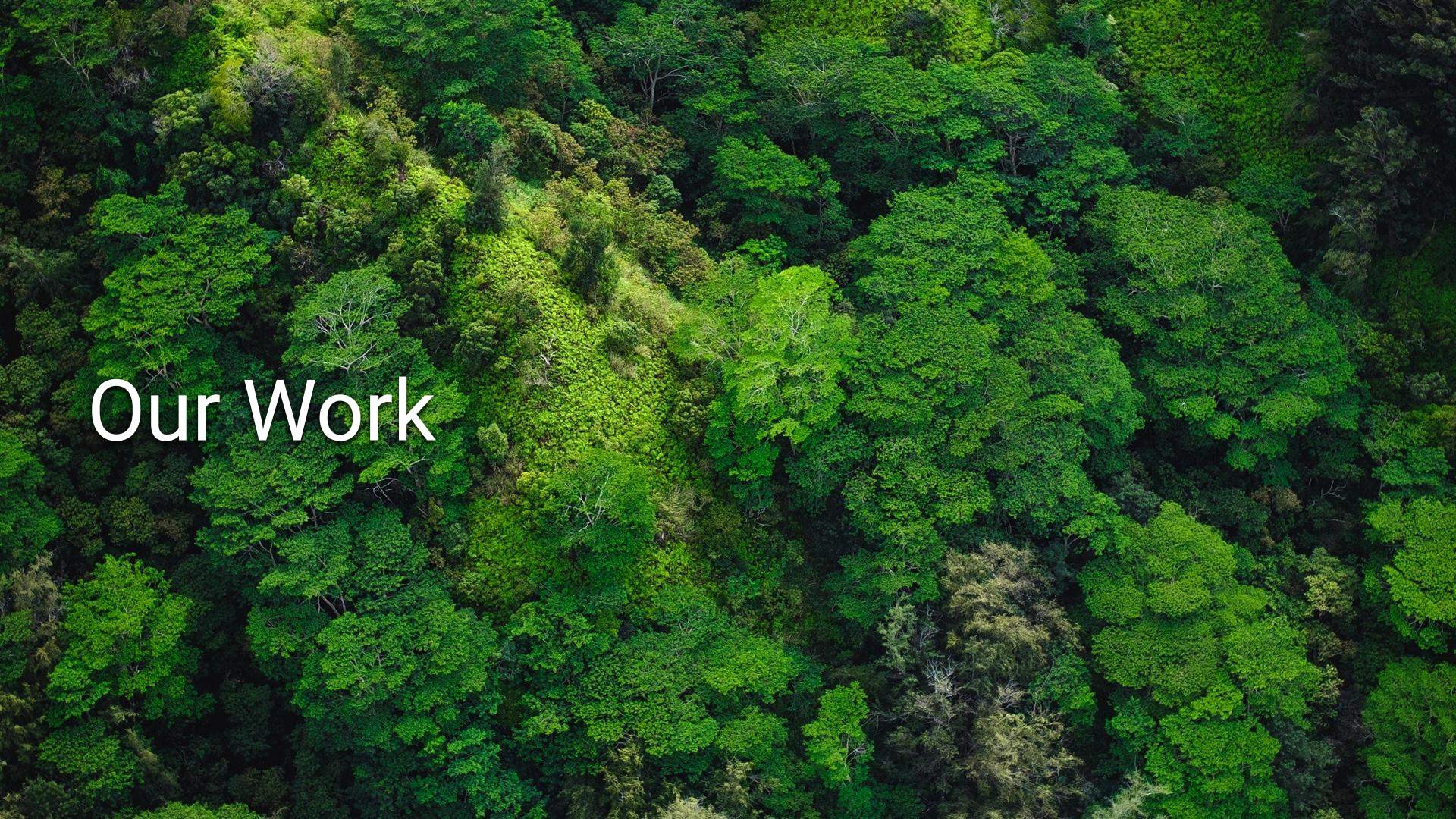
- Apply all the tables of each trees until the leaves are reached
- Perform majority voting and compute total certainty
- Classify the packet if certainty of the prediction is above the wanted threshold

P4 Code Generation

- Various elements (such as table entries, tables, actions, etc.) depend on the model chosen and P4 has no loops

  ⇨ It becomes necessary to have a script that generates the code

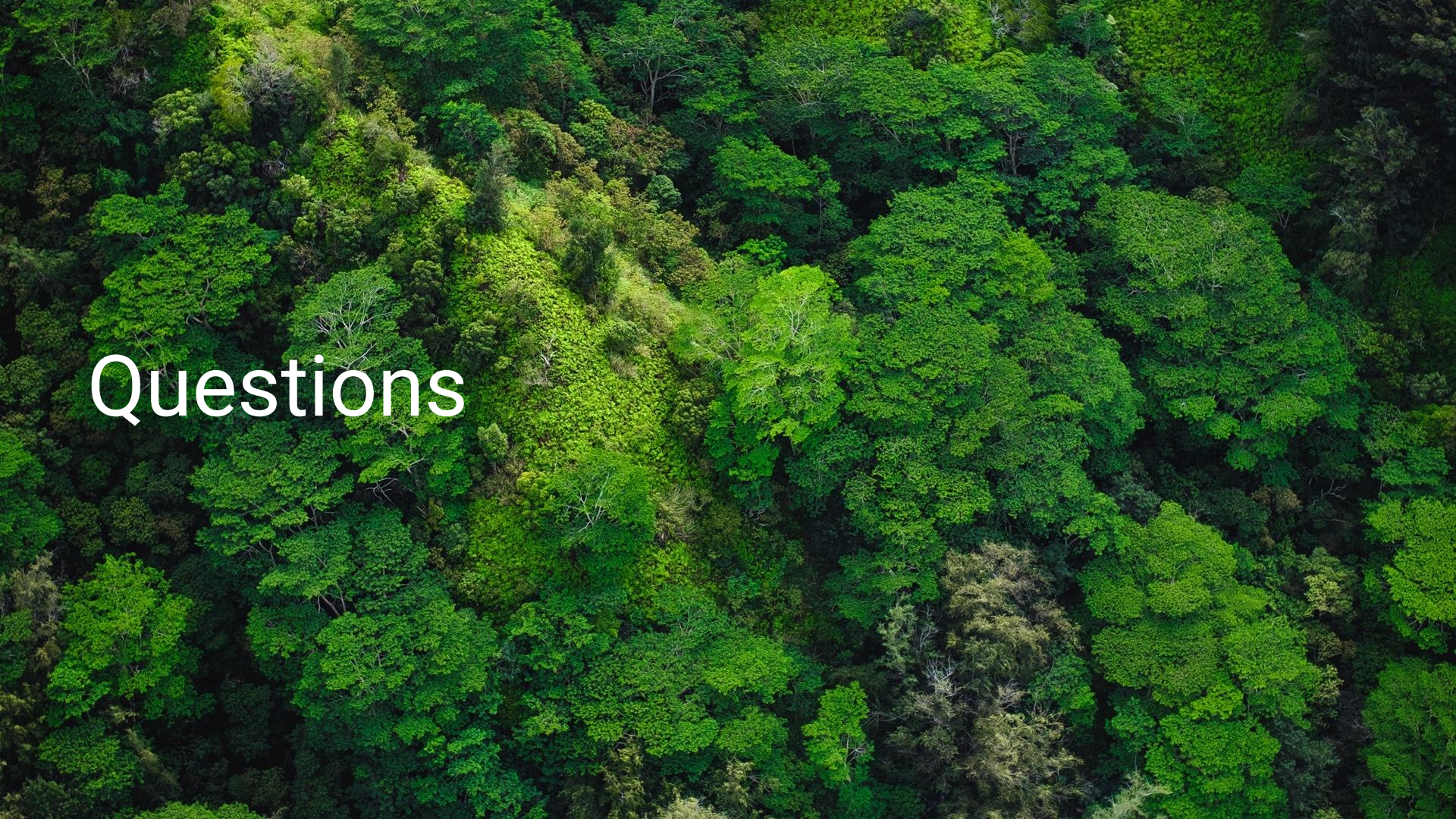
- Python script that trains a model, then generates all the match-action table entries and the P4 code


Our Work

Our Work

- CICIDS Dataset Analysis
- Random Forest model training & testing
- ***P4*** code and table entries generation


DEMO


Questions


Thank You
And
Merry
Christmas!