Soter: A Real-time Malicious Traffic Detection Framework Based on Deep Learning Enhancement of Programmable Switches

Cui ChuPeng[a]

[a] Tsinghua Shenzhen International Graduate School, Tsinghua, Shenzhen, 518055, China

INTRODUCTION

Problem Statement

- Network attacks are becoming more and more complex, challenging traditional traffic detection.
- The detection process of conventional deep learning detectors is time-consuming, which is difficult to meet the real-time detection of high-speed network.

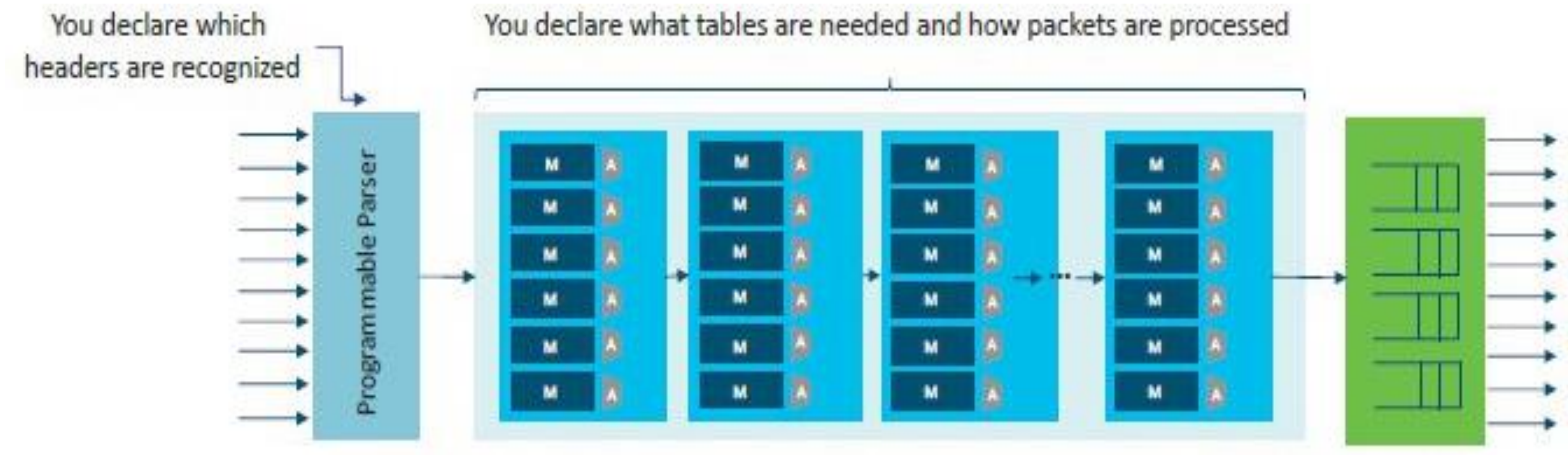
Motivation

- The lightweight neural network can reduce the number of parameters and the detection time.
- The programmable switches have high throughput and can adapt to high-speed network environment.

Approaches

- Soter, two-phase traffic detection framework based on programmable switches.
- Compressed decision tree deployed on programmable switch pipeline.
- A new lightweight convolution neural network BCN.

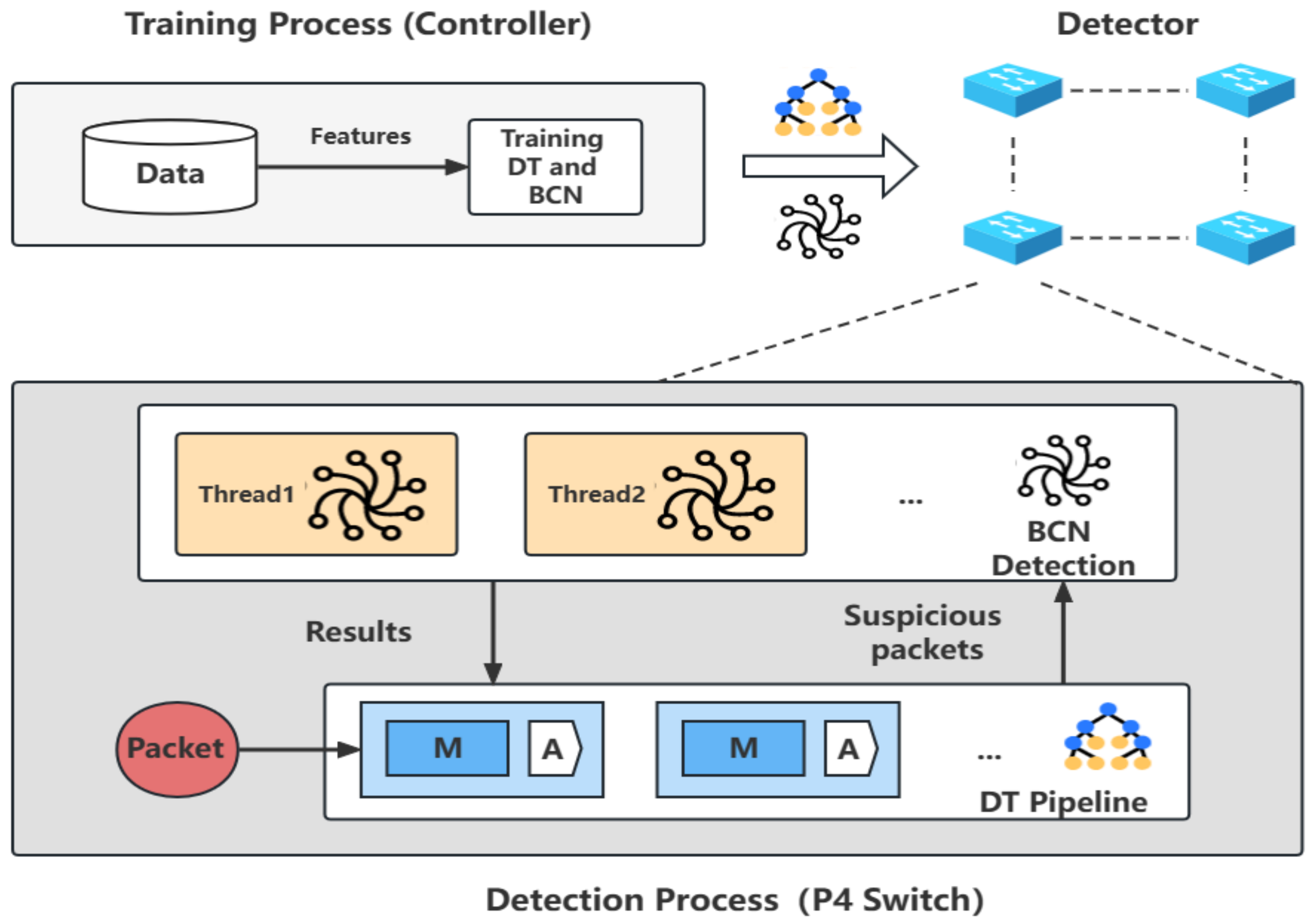
P4 SWITCHES


You declare which headers are recognized
You declare what tables are needed and how packets are processed
Programmable Parser
M
A

- Given the high throughput and capability of customized packet processing, P4 switches have been deployed in commercial data centers and cloud service networks.
- The P4 switch's data plane consists of a match-action pipeline for high-speed packet processing. Network administrators can define the rules and actions for packet matching in different tables.

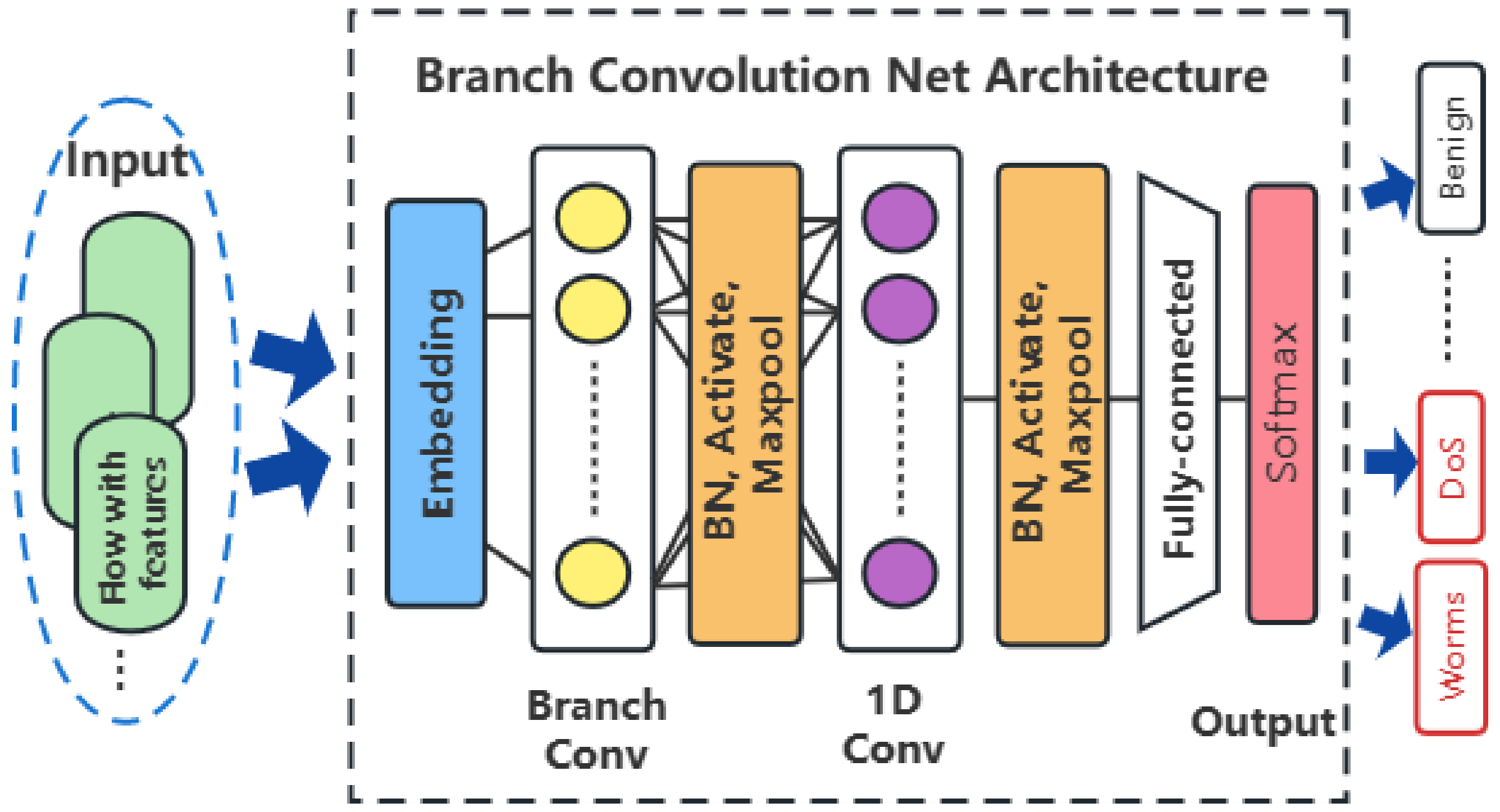
METHODS

Soter Framework



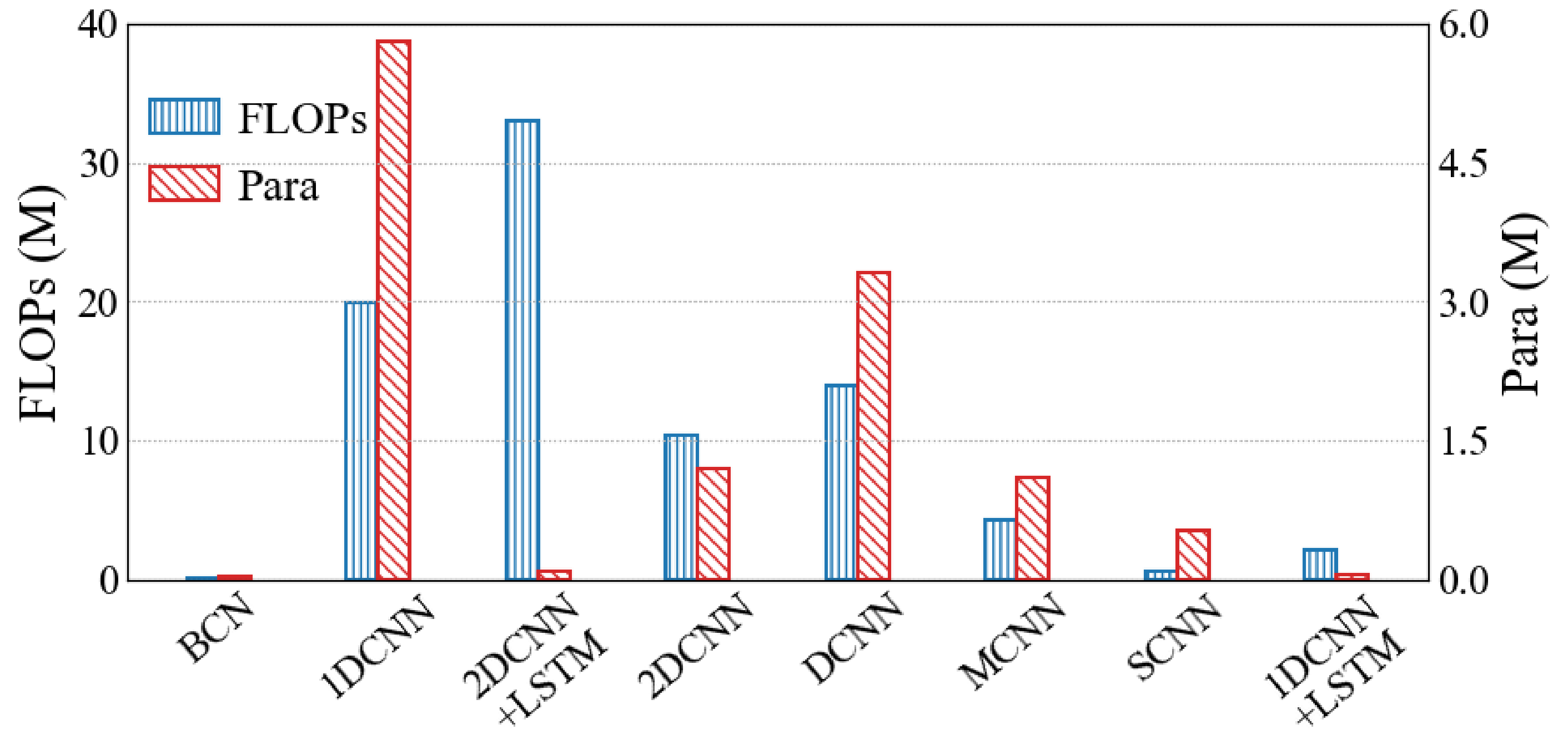
- Soter consists of two main processes: the training process and the detection process.
- Deploy the decision tree on the switch pipeline and the BCN network on the switch CPU.

BCN Structure

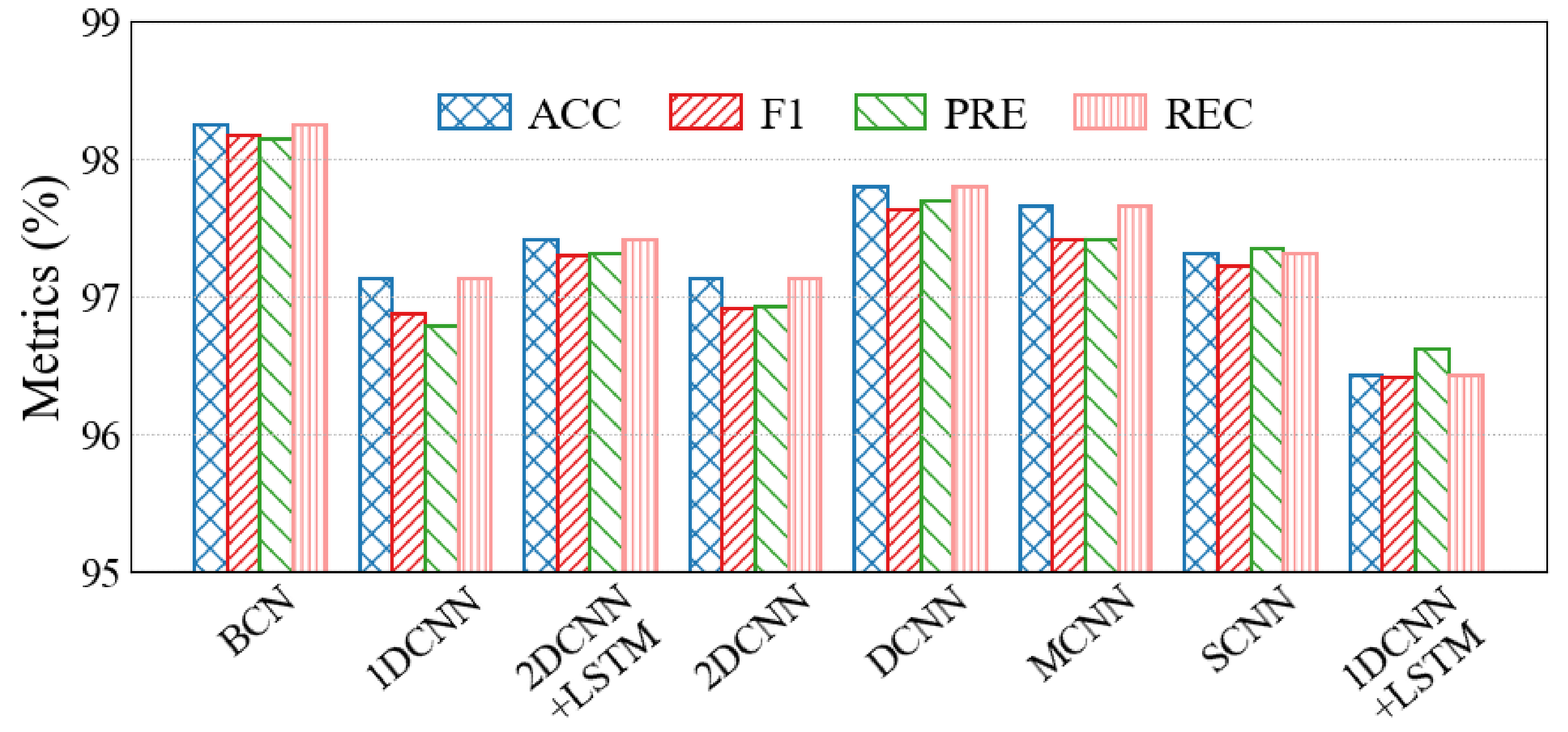


- A new branch conv module is introduced to reduce the computational complexity.
- The parameters can be reduced by C times, where C is the number of channels.
- HardSwish is used as the activation function to improve the effect.

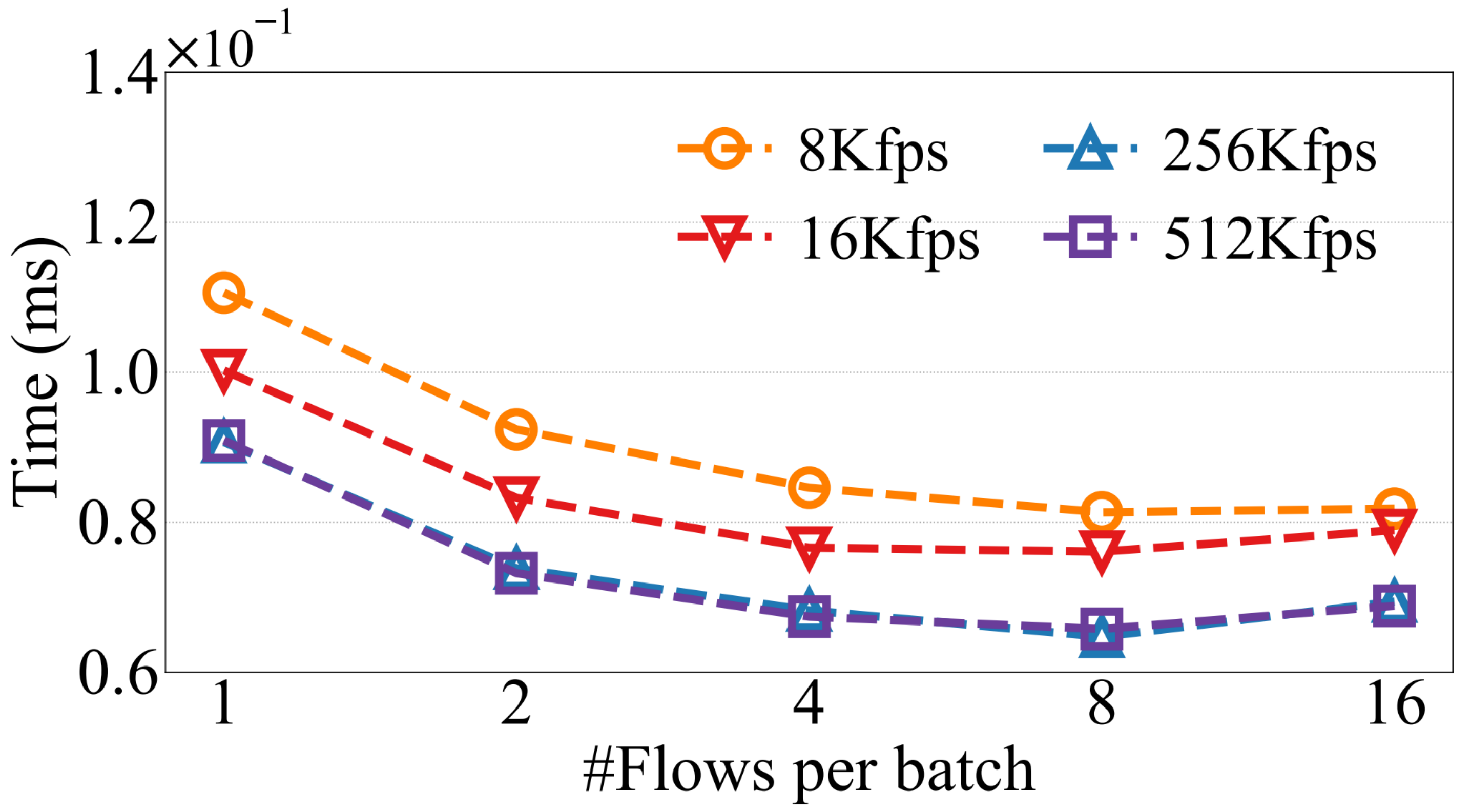
EXPERIMENTS



- BCN has few calculations and parameters. Compared with the 1DCNN, the BCN has a 193x less Para.



- Among the above four indicators, the performance of BCN is better. The ACC is 98.25%.



- Soter can complete the detection of a flow in 0.06 ms.