MMCo: Using multimodal deep learning to detect malicious traffic with noisy labels

Qingjun YUAN, Gaopeng Gou,
Yuefei ZHU, Yongjuan WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2386-4

Problems & Ideas

- Problems of Parallel training-based LNL (Learning with noise labels):
  - Disagreement is maintained by the initial state of the network alone and is prone to self-controlled degradation
  - Multi-modal information naturally present in traffic is ignored.
- Ideas: MMCo is a Co-teaching-like method using multimodal information and parallel, heterogeneous networks to detect malicious traffic with noisy labels.

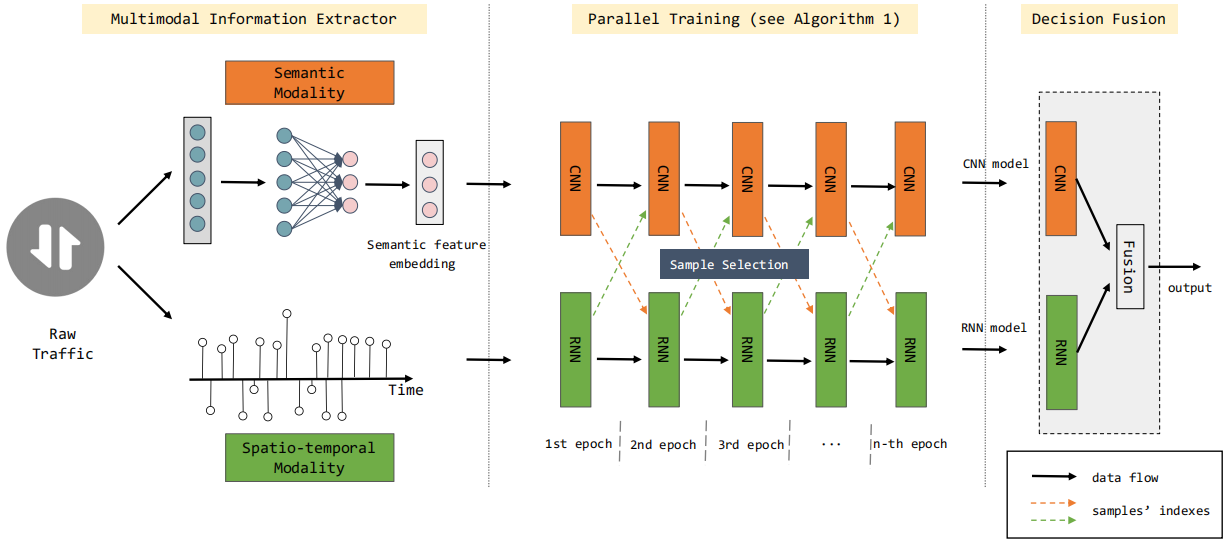

Fig. 1 Architecture of MMCo

Main Contributions

- Contributions:
  - MMCo is the first LNL method that uses multimodality to maintain disagreement;
  - the parallel networks in MMCo are heterogeneous and input different modalities of samples, which can mitigate self-control degradation and enhance robustness.

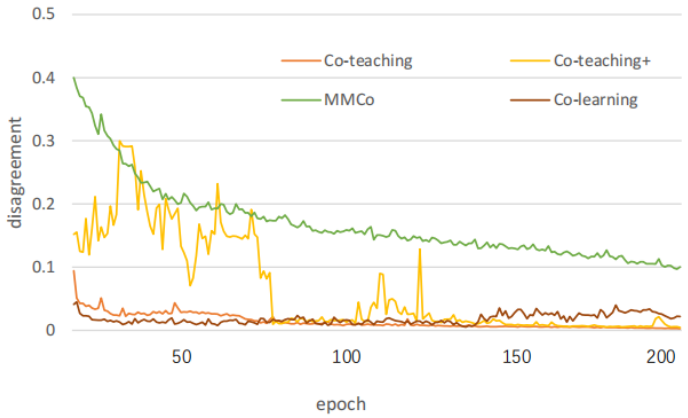

Fig. 2 Disagreement of networks (Sym-20%)

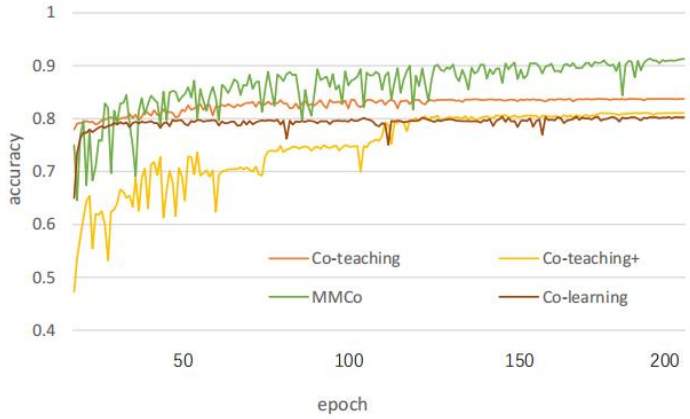

Fig. 3 Accuracy on validation set (Sym-20%)

The disagreement of the two networks is shown in Figure 2. The accuracy on the validation set is shown in Figure 3. When 200 epochs are completed, the classification networks of MMCo still maintain 10% disagreement with a final clas sification accuracy of 90%, while the disagreement of the two networks of other methods is close to zero. At this time, the two networks are in a state of self-control degradation, and it is difficult to learn more knowledge. However, MMCo can maintain a higher disagreement compared to others, thus help ing the classifiers to learn more correct knowledge, with about 10% higher accuracy.