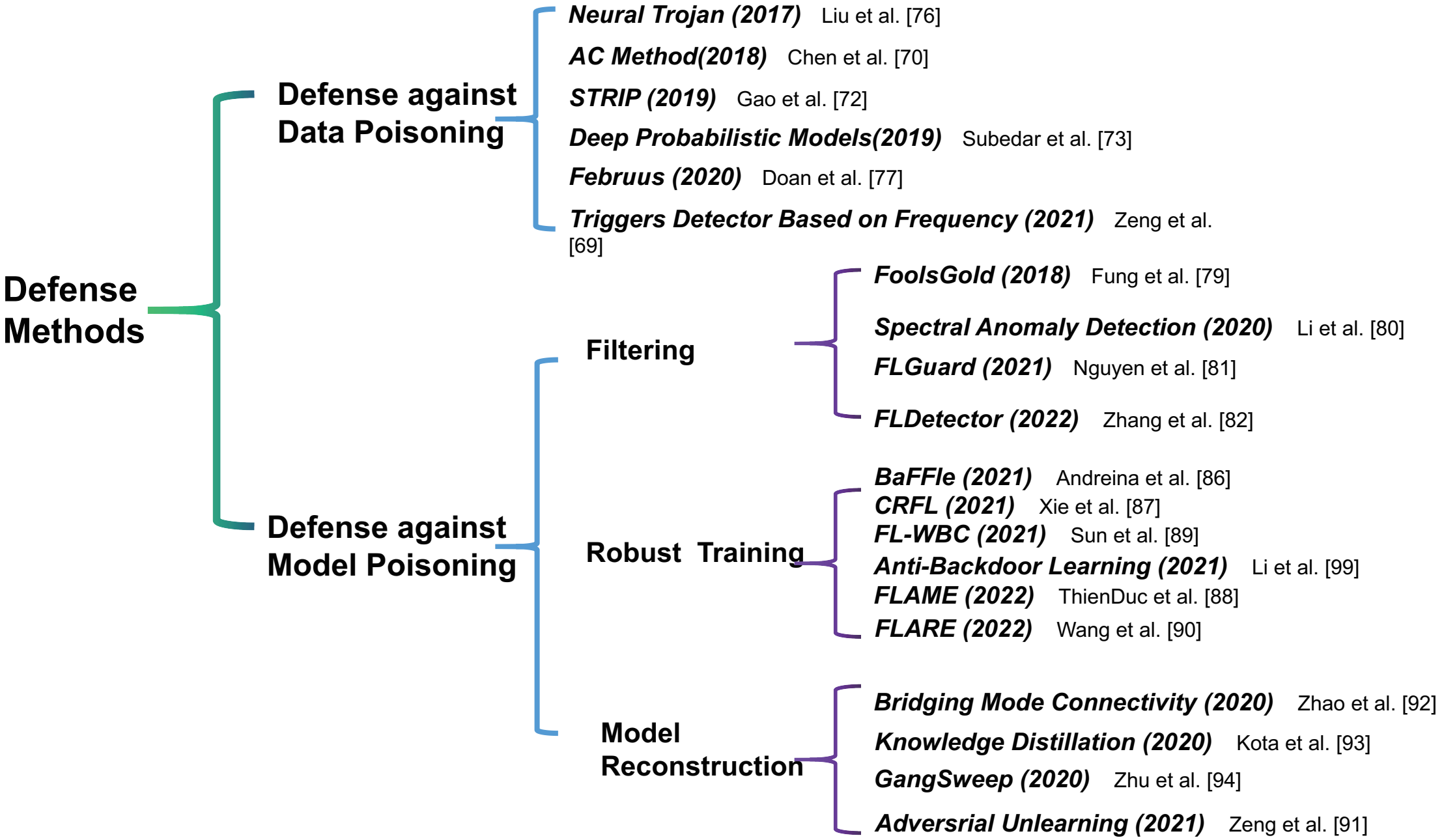
Defense Methods
Defense against Data Poisoning
Neural Trojan (2017) Liu et al. [76]
AC Method(2018) Chen et al. [70]
STRIP (2019) Gao et al. [72]
Deep Probabilistic Models(2019) Subedar et al. [73]
Februus (2020) Doan et al. [77]
Triggers Detector Based on Frequency (2021) Zeng et al. [69]
Defense against Model Poisoning
Filtering
FoolsGold (2018) Fung et al. [79]
Spectral Anomaly Detection (2020) Li et al. [80]
FLGuard (2021) Nguyen et al. [81]
FLDetector (2022) Zhang et al. [82]
Robust Training
BaFFle (2021) Andreina et al. [86]
CRFL (2021) Xie et al. [87]
FL-WBC (2021) Sun et al. [89]
Anti-Backdoor Learning (2021) Li et al. [99]
FLAME (2022) ThienDuc et al. [88]
FLARE (2022) Wang et al. [90]
Model Reconstruction
Bridging Mode Connectivity (2020) Zhao et al. [92]
Knowledge Distillation (2020) Kota et al. [93]
GangSweep (2020) Zhu et al. [94]
Adversrial Unlearning (2021) Zeng et al. [91]