TopoSleuth Detection Performance Across Attack Types
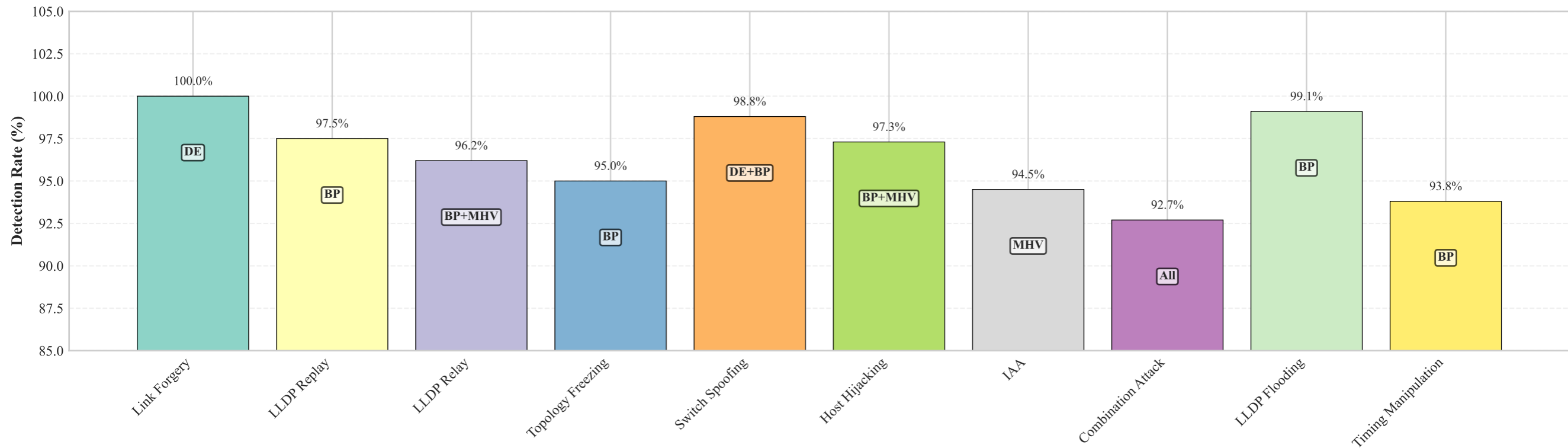
(a) Detection Rate per Attack Type

Attack Type	Detection Rate (%)	Module
Link Forgery	100.0%	DE
LLDP Replay	97.5%	BP
LLDP Relay	96.2%	BP+MHV
Topology Freezing	95.0%	BP
Switch Spoofing	98.8%	DE+BP
Host Hijacking	97.3%	BP+MHV
IAA	94.5%	MHV
Combination Attack	92.7%	All
LLDP Flooding	99.1%	BP
Timing Manipulation	93.8%	BP

(b) False Positives per Attack Type

Legend:
- Decoy Engine (DE)
- Behavior Profiler (BP)
- Multi-hop Validator (MHV)
- All Modules

Attack Type	False Positives (per 100 instances)
Link Forgery	1.2
LLDP Replay	2.3
LLDP Relay	2.1
Topology Freezing	1.8
Switch Spoofing	1.5
Host Hijacking	1.9
IAA	2.4
Combination Attack	2.7
LLDP Flooding	1.1
Timing Manipulation	2.0