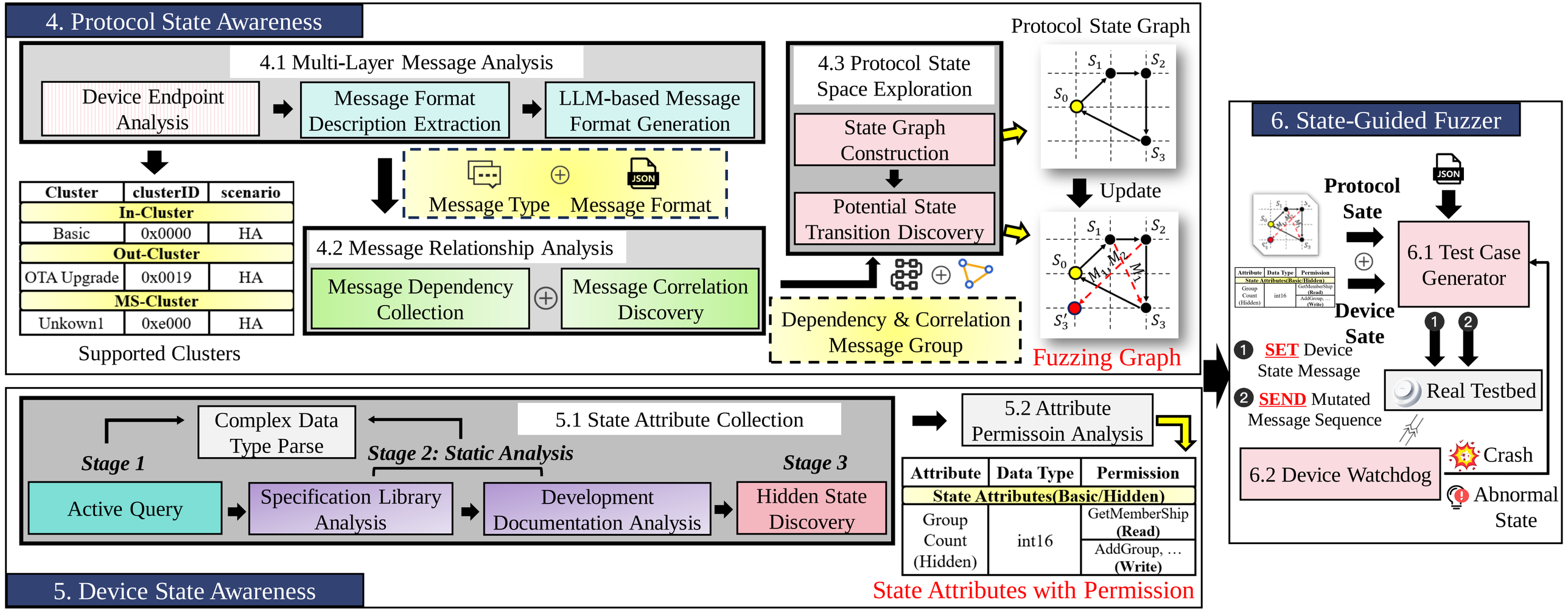
4. Protocol State Awareness
4.1 Multi-Layer Message Analysis
Device Endpoint Analysis
Message Format Description Extraction
LLM-based Message Format Generation
Cluster
clusterID
scenario
In-Cluster
Basic
0x0000
HA
Out-Cluster
OTA Upgrade
0x0019
HA
MS-Cluster
Unkown1
0xe000
HA
Supported Clusters
Message Type
Message Format
4.2 Message Relationship Analysis
Message Dependency Collection
Message Correlation Discovery
4.3 Protocol State Space Exploration
State Graph Construction
Potential State Transition Discovery
Dependency & Correlation Message Group
Protocol State Graph
Update
Fuzzing Graph
5. Device State Awareness
5.1 State Attribute Collection
Stage 1
Complex Data Type Parse
Stage 2: Static Analysis
Active Query
Specification Library Analysis
Development Documentation Analysis
Stage 3
Hidden State Discovery
5.2 Attribute Permissoin Analysis
Attribute
Data Type
Permission
State Attributes(Basic/Hidden)
Group Count (Hidden)
int16
GetMemberShip (Read)
AddGroup, … (Write)
State Attributes with Permission
6. State-Guided Fuzzer
Protocol Sate
Device Sate
6.1 Test Case Generator
1 SET Device State Message
2 SEND Mutated Message Sequence
Real Testbed
6.2 Device Watchdog
Crash
Abnormal State