Symbolic Router Execution – *Public Review*

Ennan Zhai
Alibaba Group
Hangzhou, China
ennan.zhai@alibaba-inc.com

How to ensure the correctness of network forwarding behavior—i.e., *does your network forward packets as your expectation*—is an important, fundamental problem. To this end, our community typically employs the network configuration verification technique, which uses a rigorous way (e.g., formal verification and symbolic execution) to check whether your network configuration meets your network property specification. Specifically, the network verification is required to reason about specified properties across different spaces (e.g., header space and failure space) under different failure models (e.g., deterministic failure model and probabilistic failure model). In the past ten years, while many network verification systems (e.g., Batfish, Minewsweeper, Hoyan, Plankton, Jinjing, ARC, NetDice and Tiramisu) have been proposed to reason about the network properties of interest, none of them can *efficiently* cover both spaces (i.e., header and failure spaces) while *efficiently* supporting both failure models (i.e., deterministic and probabilistic).

Symbolic Router Execution (or SRE) is proposed to fill the above gap. Specifically, SRE is a general and efficient verification system capable of supporting all above analyses. SRE proposes a new concept called *packet failure equivalence* classes (or PFECs). First, SRE symbolically executes the input network model, and generates PFECs by jointing failure scenarios and packet headers to determine a set of forwarding paths, each corresponding to an equivalence class in the product space. Then, with the PFECs in hand, SRE checks the packet-level forwarding properties (including reachability, waypointing, and isolation) by encoding PFECs and solving the entire model via BDD. SRE has been evaluated by comparing with the state of the art network verification systems (including Minesweeper, Batfish and Tiramisu) on both real and synthetic network typologies. The evaluation results show that SRE not only can run faster than the state of the art systems, but also can be used to check real property correctness of a campus backbone network.

All reviewers agree that the PFEC, the core contribution of SRE, is very interesting abstraction, and the algorithms proposed by SRE for computing this abstraction is quite useful for checking network properties under failures. By combining optimizations and the BDD usage insight, SRE has presented a general and scalable verification capability in terms of multi-space and multi-failure model reasoning. Furthermore, all reviewers appreciate the comprehensive performance evaluations conducted by SRE on both real and synthetic networks.

The future directions of SRE include (but are not limited to) the following topics: (1) incremental SRE computation for network update scenarios, (2) an optimized BDD implementation that enables SRE to run much faster and save more memory, and (3) exploring an enhanced SRE on more complex network such as production-scale backbone network with many aggregation routes and multi-protocol redistribution.