Scribes for the *Efficient Network Reachability Analysis Using a Succinct Control Plane Representation*

by: Sandeep Kumar and Pawan Rajotiya

Environment Assumptions

The possible announcements from the router (network *NOT* under consideration) can be huge. Modelling this with a **true** bit vector, provides a maximal kind of setting. This does not guarantee all possible environments as it might be possible that network has a bug which is triggered when a subset of the bit vector is set to false, or something similar.
ERA, guarantees reachability only for a given environment assumption. To satisfy that it condition that the reachability analysis always holds then we must perform iterate over all possible environment assumptions.

Router Levels

During the discussion of Bug Triggered because of link failure, it is fair to assume that the routers are situated at different *levels*. The router at a higher level is not involved in communication of the lower routers. It is analogous to routers at a department level is not involved in communications across labs in the department.

Modeling Loops in Routing

The routes from node A to node B can be serialized or in parallel. The serialized routes are just *AND* with the route and the parallel routes *OR*-ed with the routes.
The loop around loops.

Static Routes

Static routes present in the router are configured by the admin when he/she wants the traffic for a particular destination to be always forwarded to a particular machine. The static routes are not broadcasted to other routers. These are useful in security and balancing purposes.

Aggregate Routes

Aggregate routes in the router are responsible for redirecting the traffic to a set of IP addresses. These addresses can be formed automatically in the routers based on the *Route Aggregation Logic* or can be configured by an administrator. Aggregate routes are not always active. They become active when they receive announcement for the a destination which is contained within the destination for which this particular Aggregate route is configured. This is called a *contributing* *route.*

In case of automatically configured Aggregate routes, as there is already a contributing route (otherwise this route wouldn't have formed) they are activated immediately. However, in case of the manually configured Aggregate routes, they lie dormant and are activated as soon as they receive a contributing routes.

Network Convergence

The tool, ERA performs reachability analysis in a converged network and no guarantee is given when the network is in *transient* state.

Things keeps changing in the network and the network tries to stabilize itself after each change. This process of stabilizing (where announcements are sent from routers to routes) is called process of converging and when this process is done the network is said to be converged.

Rouer I/O

To perform analysis on a given network Authors model the I/O of the router and the processing logic of the routers for efficient analysis.
I/O of the router or the announcements is modelled as a 128 bit vector, representing Destination IP, Prefix, AD (Administrative Distance), Protocol Attributes.
The announcements from different routers are represented as a *predicate*.

True = Maximal set of values with zero restrictions False = Empty set, no routes. Boolean predicate = Routes broadcasted from outside with some values for Destination, AD and Protocol Attributes.

Visibility Function

THe processing logic of the router is defined as a *Visibility Function* which defines how the incoming announcements from the nearby routers and the environments is processed by this router.

Exploring the Model

Cause of data plane explosion is announcement from outside the network.
Given the model for the announcements and the processing logic of the routers, it is necessary to explore the model to find a reachability violation present in the network. In simple terms it will be, given a control plane explore all of its data plane to see if a particular reachability policy is violated in any of the data planes. This will take time and for large networks may be intractable. So, exploring here using models will be efficient.

Exploring using BDD, or Verification Technique

Choosing a representation totally depends upon the functions to be performed on the model constructed. In the paper the functions can applied easily and efficiently on the model using BDDs.
The authors uses BDD (Binary Decision Diagram) to encode the predicates and explore them efficiently. However, as discussed in the class a state of the art SMT solver, which is meant for these kind of problems can be used to explore the model much more efficiently. A related work which uses SMT solver for its analysis can be found here:
Minesweeper: https://batfish.github.io/minesweeper/
Main thing in the paper is even though the problem is very complicated and large; using a model to generalize the problem variables we can solve it not perfectly but almost perfectly.

Optimizations

To further enhance the exploring performance, author uses techniques such as:

- K Map: TO reduce the number of variables in the predicate.
- Predicate Equivalence: In a large network most of the part of networks behaves similarly. Analyzing them independently is unnecessary. Predicates are grouped into equivalence classes and the operation is performance on these classes.
- Bit - Set operations: To perform operations such as Union and Intersection authors use the bit set operations. Where Union means logical OR and Intersection means logical AND.

Beyond Reachability

Altough ERA cannot be used to find bugs related to convergence, it can find bugs which are similar in nature to reachability such as

- Valley free Routing
  - Announcements from one network should **NOT** reach another.
- Equivalence of two routers
  - Verify that the setting of two routers from different vendors are equivalent.
- Black hole freeness
  - Verify that the router are not dropping packets *unintentionally*.
- Way Pointing
  - You want the data from one address to another should take a particular route.
- Loop freeness
  - No Loops in the network.