Config2Spec:
Mining Network Specifications from Network Configurations

Rüdiger Birkner, Dana Drachsler-Cohen, Martin Vechev, Laurent Vanbever

nsg.ee.ethz.ch

ANRP at IETF 111
July, 26 2021

ETH zürich
Intent-based networking has been and still is one of the buzzwords in the community.
Many tools are available that allow you to check that your network behaves as intended

Standard recipe:

1. Upload configurations
2. Provide specification
3. Run the tool
4. Iterate & deploy
Definition
The specification of a network is the set of all policies that hold...

Set of policies

- reachability($r_1,p_1$)
- waypoint($r_3,r_1,p_2$)
- reachability($r_5,p_2$)
- ...
- loadbalancing($r_3,p_2$)

Topology
Definition

The specification of a network is the set of all policies that hold...

Set of policies

\[
\text{reachability}(r_1, p_1) \\
\rightarrow \text{waypoint}(r_3, r_1, p_2) \\
\rightarrow \text{reachability}(r_5, p_2) \\
\rightarrow \text{loadbalancing}(r_3, p_2)
\]

Topology
Definition
The specification of a **network** is the **set of all policies** that hold...

![Set of policies](image1)

![Topology](image2)
Definition
The specification of a network is the set of all policies that hold under a given failure model.

Set of policies
reachability(r1,p1)
waypoint(r3,r1,p2)
reachability(r5,p2)
...
loadbalancing(r3,p2)
Definition
The specification of a network is the set of all policies that hold under a given failure model.
The specification of a **network** is the **set of all policies** that hold under a given **failure model**.

**Definition**

Set of concrete environments

Symbolic environment

Failure bound

\[ k = 2 \]
The specification of a **network** is the **set of all policies** that hold under a given **failure model**.

**Definition**

Set of policies

- `reachability(r1,p1)`
- `waypoint(r3,r1,p2)`
- `reachability(r5,p2)`
- `loadbalancing(r3,p2)`

**Symbolic environment**

- `k = 2`
Writing the network’s precise specification is hard

Standard recipe:

1. Upload configurations
2. Provide specification
3. Run the tool
4. Iterate & deploy
Writing the network’s precise specification is hard

Dr Heidy Khlaaf
@HeidyKhlaaf

In the past three years of working on large safety critical systems, I've learned that verification isn't the real problem, but it's writing specifications. Don't @ me.

twitter.com/Conaw/status/1…

Conor White-Sullivan @Conaw
Replying to @Conaw @vgr
38. Provably correct doesn't mean it works

141 7:06 PM - Dec 15, 2019
38 people are talking about this
Writing the network’s precise specification is hard

Dr Heidy Khlaaf
@HeidyKhlaaf

In the past three years of working on large safety critical systems, I've learned that verification isn't the real problem, but it's writing specifications. Don't @ me.

twitter.com/Conaw/status/1…

Putting network verification to good use

Ryan Beckett
Microsoft Research

Ratul Mahajan
University of Washington
Intentionet

... However, outside of a handful of large cloud computing providers, the use of network verification is still sparse.
Internet2’s specification with its 10 routers consists of ~4000 policy predicates.
Config2Spec

Mining Network Specifications from Network Configurations

Rüdiger Birkner  Dana Drachsler-Cohen  Martin Vechev  Laurent Vanbever

nsg.ee.ethz.ch
Config2Spec automatically mines the network’s full specification from its configuration and the given failure model.

Input:
- Network Configuration
- Failure Model

Output:
- Network Specification
  - loadbalancing(4, p2)
  - reachability(1, p1)
  - reachability(1, p2)
  - ...
Config2Spec:
Mining Network Specifications from Network Configurations

1. Baseline approaches
   one search space at a time

2. Our approach
   the best of both worlds

3. Evaluation
   scales to realistic networks
Config2Spec: Mining Network Specifications from Network Configurations

1. Baseline approaches
   one search space at a time

2. Our approach
   the best of both worlds

3. Evaluation
   scales to realistic networks
Mining a network specification involves exploring two exponential search spaces

reachability\((r_1, p_1)\)
waypoint\((r_3, r_1, p_2)\)
... 
loadbalancing\((r_5, p_2)\)

all concrete environments
all possible policies
Mining a network specification involves exploring two exponential search spaces

data plane analysis \times control plane verification
data plane analysis

×

control plane verification
Data plane analysis tools allow to find all the policies that hold for a single concrete environment

\[ k = 2 \]
Data plane analysis tools allow to find all the policies that hold for a single concrete environment.
Data plane analysis tools allow to find all the policies that hold for a **single** concrete environment
Data plane analysis tools allow to find all the policies that hold for a single concrete environment.
Data plane analysis tools allow to find all the policies that hold for a single concrete environment.
The network specification is the intersection of the policies that hold for every concrete environment.
The network specification is the intersection of the policies that hold for every concrete environment
The network specification is the intersection of the policies that hold for every concrete environment.
The network specification is the intersection of the policies that hold for every concrete environment.
The network specification is the intersection of the policies that hold for every concrete environment.

\[ \bigcap \]
The network specification is the intersection of the policies that hold for every concrete environment.
data plane analysis \times control plane verification
Control plane verification tools determine whether a policy holds for the entire failure model
Control plane verification tools determine whether a policy holds for the entire failure model

\[
reachability(r_1, p_1) \quad \text{Single policy}
\]

\[k = 2\]
Control plane verification tools determine whether a policy holds for the entire failure model.
Control plane verification tools determine whether a policy holds for the entire failure model.

\[
\text{reachability}(r_1, p_1)
\]

Single policy

Control plane verification

Verification result
The network specification is the set of policies that the verifier determined to hold for the failure model

\[
reachability(r_1, p_1)
\]
The network specification is the set of policies that the verifier determined to hold for the failure model.

$reachability(r_1, p_1)$ $reachability(r_2, p_1)$ $\cdots$

$k = 2$

$\square$ $\times$ $\square$ $\square$

$\rightarrow$ $\rightarrow$

$\rightarrow$

$\rightarrow$ $\rightarrow$ $\rightarrow$

$\rightarrow$

$\rightarrow$ $\rightarrow$ $\rightarrow$

$\rightarrow$ $\rightarrow$ $\rightarrow$ $\rightarrow$
The network specification is the set of policies that the verifier determined to hold for the failure model.
The network specification is the set of policies that the verifier determined to hold for the failure model.
The network specification is the set of policies that the verifier determined to hold for the failure model.
The network specification is the set of policies that the verifier determined to hold for the failure model.
Both techniques have pros and cons

<table>
<thead>
<tr>
<th>approach</th>
<th>data plane analysis</th>
<th>control plane verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>all policies for</td>
<td>one policy for the</td>
<td></td>
</tr>
<tr>
<td>one concrete env.</td>
<td>entire failure model</td>
<td></td>
</tr>
</tbody>
</table>

What about combining them?
Config2Spec:
Mining Network Specifications from Network Configurations

1. Baseline approaches
   one search space at a time

2. Our approach
   the best of both worlds

3. Evaluation
   scales to realistic networks
**Config2Spec** mines the network’s full specification from its configuration and the required failure tolerance.
Step-by-step from all existing policies to the network’s specification
By performing data plane analysis on a topology, Config2Spec refines the space of candidate policies.
By performing data plane analysis on a topology, Config2Spec refines the space of candidate policies.
By performing data plane analysis on a topology, Config2Spec refines the space of candidate policies.
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.

Policy #1
reachability(1, p1)
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.

Policy #2

reachability(3, p2)
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.

Policy #3

reachability(1,p2)
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.
With control plane verification, Config2Spec checks whether a candidate policy belongs to the specification.
When Config2Spec terminates, it is left with the specification.
**Config2Spec** can be improved further by two domain-specific techniques:

- **Policy-aware selection**
- **Grouping and trimming**
Config2Spec: Mining Network Specifications from Network Configurations

1. Baseline approaches
   one search space at a time

2. Our approach
   the best of both worlds

3. Evaluation
   scales to realistic networks
We fully implement Config2Spec and show its practicality.

**Implementation**
5k lines of Python and Java
relying on Batfish and Minesweeper

**Methodology**
generated configs using NetComplete
employing OSPF, BGP

for a small, medium, and large network
with 33, 70, and 158 routers
Config2Spec mines the specification for realistic networks in few hours.
For failure models with few concrete environments, data plane analysis on its own provides fastest progress.
For failure models with a high failure bound, policy trimming reduces the candidate space significantly.

run time [h]  
large topology

k = 1  2  3

OSPF  BGP

Control plane verification  Data plane analysis
Config2Spec mines the specification for realistic networks in few hours.
Config2Spec: Mining Network Specifications from Network Configurations

1. Baseline approaches
   one search space at a time

2. Our approach
   the best of both worlds

3. Evaluation
   scales to realistic networks
Config2Spec: Mining Network Specifications from Network Configurations

automatically learns a network's specification based on its configuration and failure model

the specification is useful beyond verification

what-if analysis
config streamlining
network understanding
Config2Spec: Mining Network Specifications from Network Configurations

Rüdiger Birkner¹  Dana Drachsler-Cohen²  Laurent Vanbever²  Martin Vechev³
¹ETH Zürich ²Technion ³UC Berkeley

Abstract
Network verification and configuration synthesis are promising approaches to make networks more reliable and secure by extracting a set of policies. However, these approaches require a formal and precise description of the intended network behavior, meaning a naive hartic in their adoption. Network specifications are not only difficult to write formal specifications, but also difficult to know what these specifications are.

We present Config2Spec, a system that automatically synthesizes a formal specification (set of policies) of a network given its configuration and a failure model (e.g., a tree link failure). A key technical challenge is to design a synthesis algorithm which can efficiently explore the large space of possible policies. To address this challenge, Config2Spec selects a careful combination of two well-known methods: dataplane analysis and control-plane verification.

Experimental results show that Config2Spec scales to mining specifications of large networks (N=10 routers).

1 Introduction
Consider the task of a network operator who maintains a network-wide configuration (e.g., 10,000 routers) and needs to verify network behavior. Among others, it needs to enforce load balancing for popular destinations, provide isolation between customers, drop traffic for expired sessions, and ensure business traffic via predefined rules—all these under different policies. Writing the precise

Check our NSDI’20 paper as there is much more behind Config2Spec

We are still improving Config2Spec through richer specifications and automatic bug detection

Please reach out to us at rbirkner@ethz.ch with all your inputs and feedback

nsg.ee.ethz.ch
Config2Spec

Mining Network Specifications from Network Configurations

Rüdiger Birkner  Dana Drachsler-Cohen  Martin Vechev  Laurent Vanbever

nsg.ee.ethz.ch