Scalability and Resilience in SDN: an overview

Nicola Rustignoli
rnicola@student.ethz.ch
Software-Defined networking

How does Software-Defined networking perform in datacentre networks?

Traffic generated by servers in our datacenters

What about carrier-grade networks?

- End to end applications require a delay <50ms

What can go wrong?

50ms
Many things can go wrong!

- Controller is too busy to manage new flows
- Controller fails
- A link fails
- Your network is under attack
Scalability

One single controller is unable to handle requests for very large (or busy) networks

How to scale?

A. Distributed controllers: can handle more flows

B. Hierarchical controllers: only most relevant flows are managed by central control, while others are taken care by other entities

- Controllers are brought close to switches
- Each area of network is managed by one single controller
- Controllers have a global view of network. This comes with high synchronization overhead

GLOBAL LAYER

Event-based
CONTROL LAYER
Push-subscribe system
slow

SWITCH
FORWARDING
LAYER
A: Distributed controllers (2): ONIX [5]

- Switches are dynamically assigned to controller instances according to load
- Topology and link monitoring are offloaded to a dedicated control platform
- Network Information is distributed across instances thanks to an high performance system (SQL+DHT).
A: Distributed controllers (2): ONIX [5]

GLOBAL LAYER
Global optimal routing

CONTROL LAYER
Area control

- A transparent virtualization layer is introduced between switch and multiple OpenFlow controllers
- The virtualization layer offers “slices” of network to each controller
- Provides multi-tenancy, isolation, resilience

CONTROL LAYER

VIRTUALIZATION LAYER

This layer adds significant delay in flow setup

SWITCH LAYER
B: Hierarchical controllers. Managing relevant flows and congestion

- Only elephant flows need management by central controller
- Small flows are handled at switch layer or by local controllers
- Goal: route (heavy) traffic on least congested paths

CONTROL LAYER

SWITCH LAYER

Modified for small flow handling

Hard to deploy in existing networks
B: Hierarchical controllers (2): Kandoo[7]

GLOBAL CONTROL LAYER

LOCAL CONTROL LAYER
Switch-local controller performance is limiting factor

SWITCH LAYER
Conclusion: scalability

- Workload can be effectively divided

- Optimal flow management is important for bigger flows

- A compromise between performance, reliability and complexity has to be made while scaling up to large networks
Break!
Resilience

Ability to quickly respond to:

1. Controller failure
2. Link failure, path failure (including case of in-band networks)
3. Attacks on network
Controller replication (Fonseca et al. [8])

- Backup controllers are kept in sync, before flows are installed to switches (adding *latency in flow setup*)

- Recovery might fail in case of network partitioning

- Recovery takes *too long* (900ms)
Reactive link failure recovery
(Controller-based)
Sharma et al [9], Van Andrichem et al [11].

- **Restoration**
  
  a. Use a spanning tree algorithm to remove possible loops in topology [9]


- **Protection**
  
  a. Controller is manually configured with fixed alternative paths [9]
Reactive link failure recovery [9] [11] (Controller-based)

- **Restoration**
  
  Dynamic, need link discovery mechanisms with their overhead, slow response (>100ms)

- **Protection**
  
  Quite fast response (120ms), no overhead traffic, manual configuration, inflexible
Path/Link-based protection (Switch-based)
Sharma et al [10], Van Andrichem et al [11]

1:1 Protection: use backup paths preconfigured in switches, using OpenFlow group tables. BFD* used for failure detection.

a) Path based [10]: number of monitored paths grows quadratically with number of nodes

b) Link based [11]: per-link BFD guarantees fastest detection time (3.3ms recovery). Linear complexity.

*BFD=Bidirectional Forwarding Detection. Group tables are aware of BFD.
Network security

- Switch-controller connection is **not secure** in all controller implementations

- In order to respond to attacks on your network, you should:
  1. Detect malicious flows (i.e. flow statistics?...)
  2. Modify flow rules
  3. Check that new rules comply with security policy
Conclusions: resilience

- No presented scheme offers controller failure resiliency that satisfies the 50ms requirement of carrier networks
- Paths can be recovered in less than 50ms
- Detecting malicious flows remains a challenge
Thank you!

Questions?

Nicola Rustignoli
rnicola@student.ethz.ch
References


References


