Peoples' Friendship University of Russia (RUDN University)

Federal Research Center "Computer Science and Control" RAS

Institute for Information Transmission Problems RAS

EXTRACTION OF TRAFFIC FEATURES IN SOFTWARE DEFINED NETWORKS USING AN SDN CONTROLLER

Volkov Sergey

volkserg1@gmail.com

Kurochkin I. I.

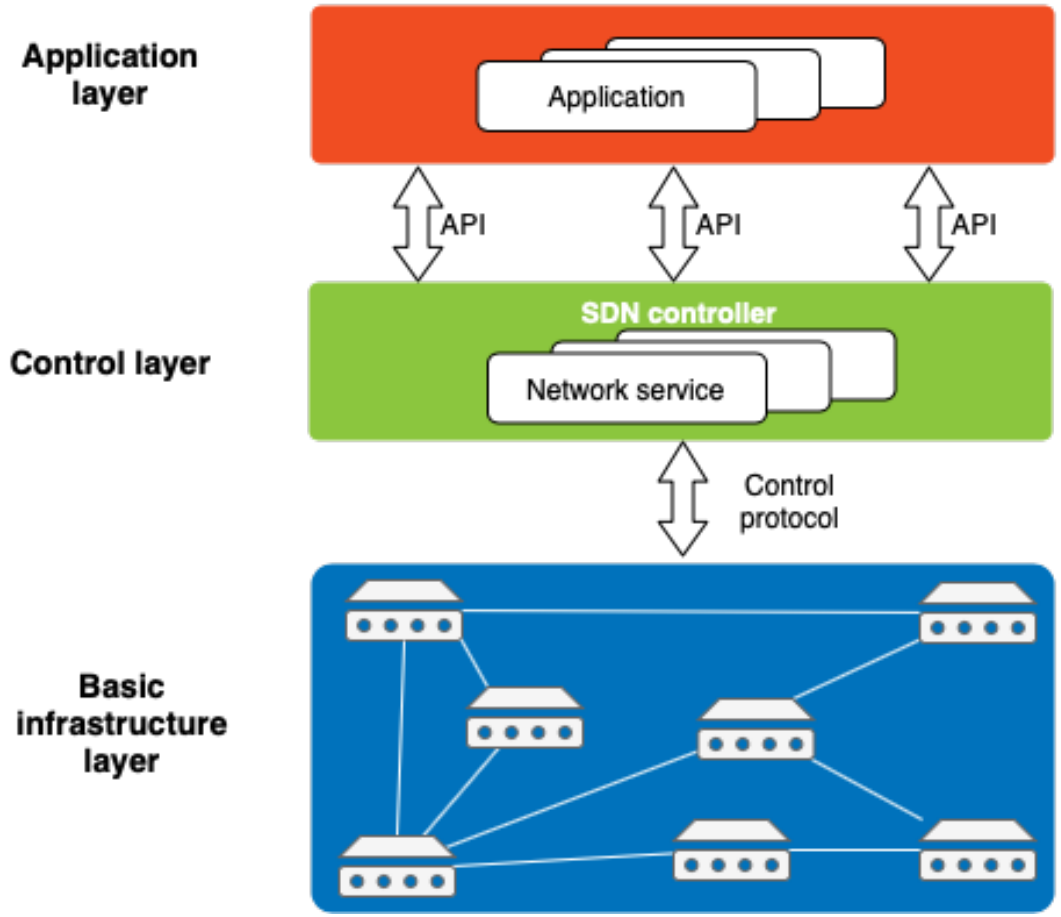
qurochkin@gmail.com

This work was funded by RFBR according to the research project No. 18-29-03264

Определение

- ***Software-Defined network, SDN*** – network in which the control plane functionality is separated from the packet forwarding layer (data plane).

- **SDN** enables network programming and allows you to dynamically change the traffic flow policy.



The main advantages of SDN

- *Simplification of network deployment.*
- *Moving from distributed to centralized management.*
- *Opportunity to design and develop network software modules.*
- *Global view and planning.*
- *Convenience of administration and debugging*.

Applications of the SDN

- Data processing centers
- Cloud services
- Corporate networks

Purpose and stages of modeling

- Designing a software-defined network topology.
- Configuring the SDN for communication (for example, setting specific hosts to receive specific signals).
- Generation of mixed traffic in the network.
- Study of traffic behavior within the network, as well as the capabilities of the SDN controller.
- Data collection for network attack detection tasks in software-defined networks.
- Modeling of a distributed network of several data centers

Tools

Software-defined network emulator

Open source SDN management platform (controller).

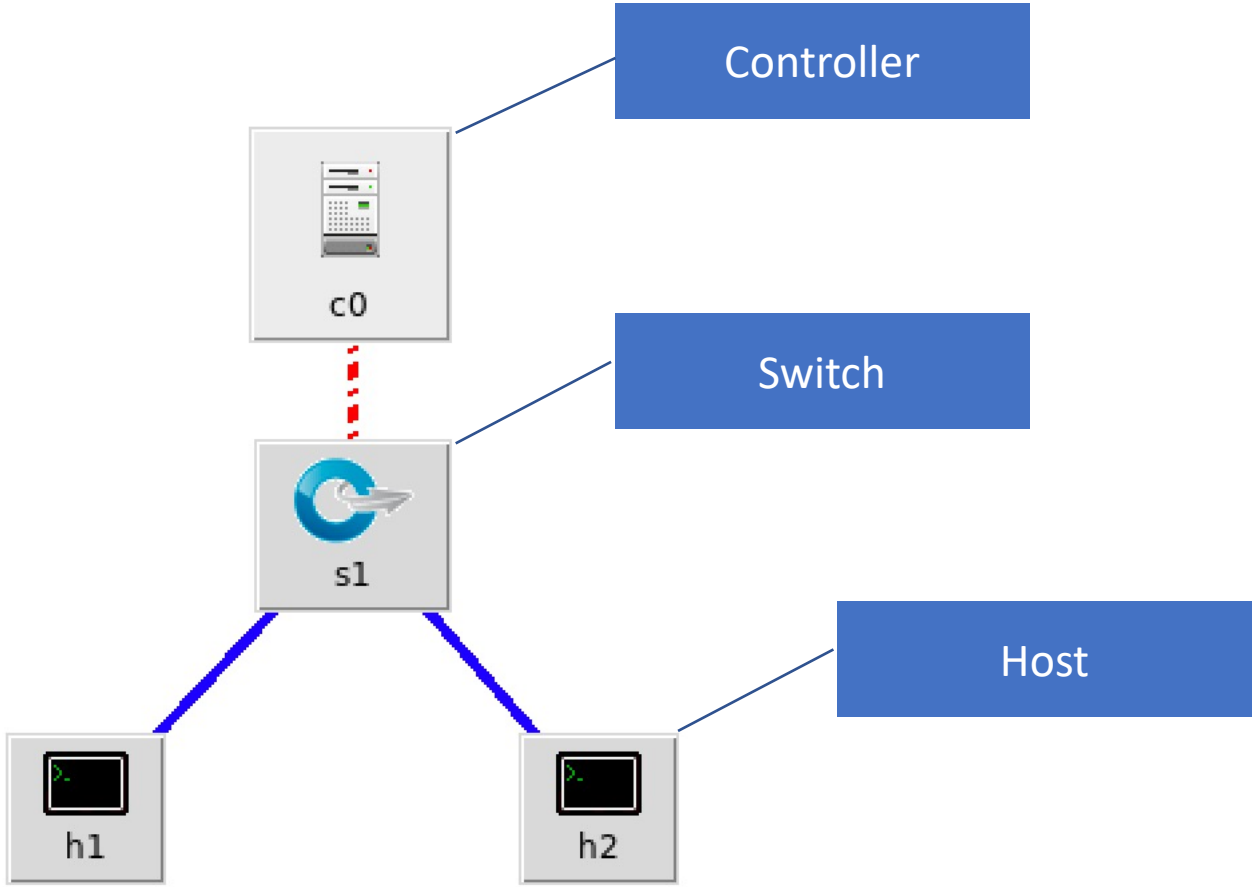
Mininet

- **Mininet** – computer network emulator.

- A computer network means simple systems that consist of:
  - Hosts
  - Switches
  - OpenFlow-controllers

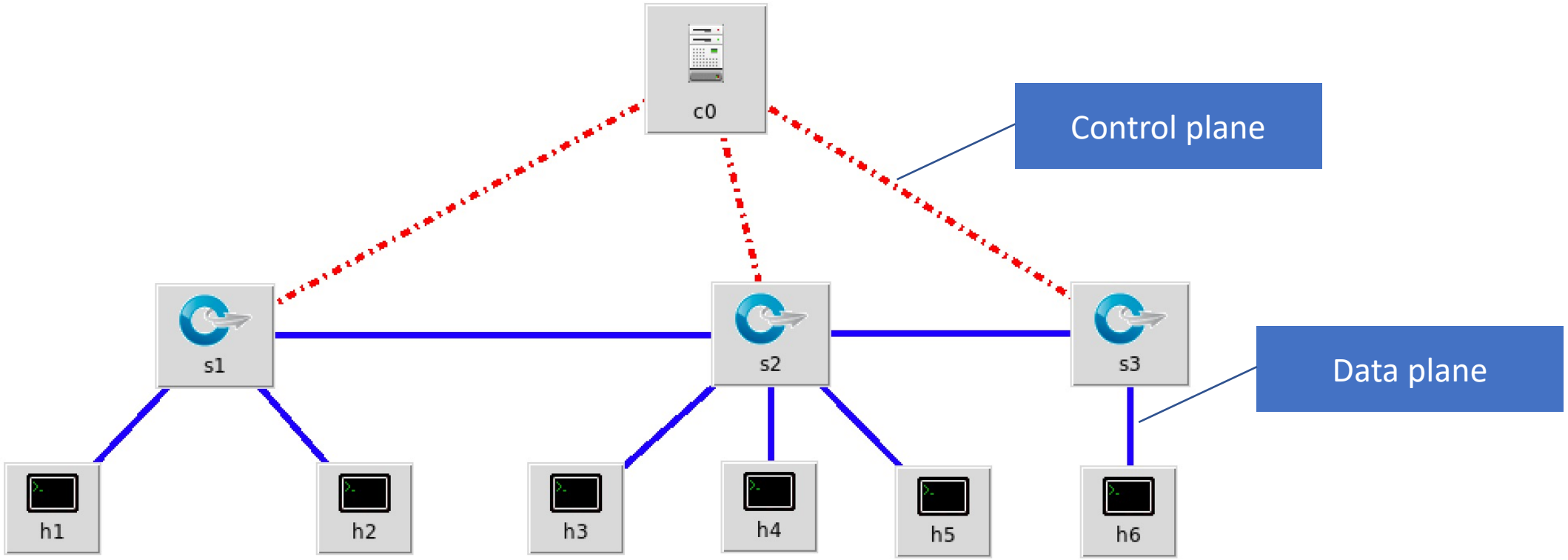
- The computer network in Mininet is deployed within one virtual machine

Mininet – simple topology



Miniedit interface

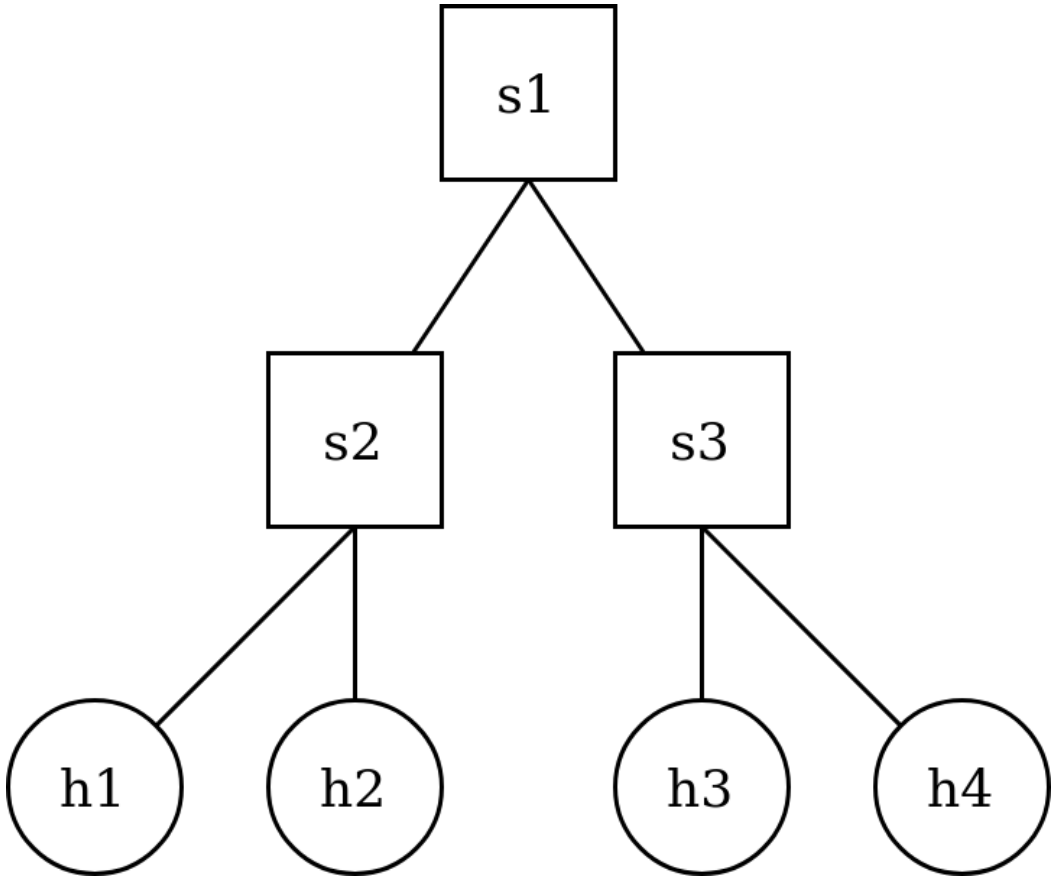
Mininet – Linear topology



Considered topologies

- **Tree**.

  Topology of a computer network, in which each higher-level node is connected to lower-level nodes.

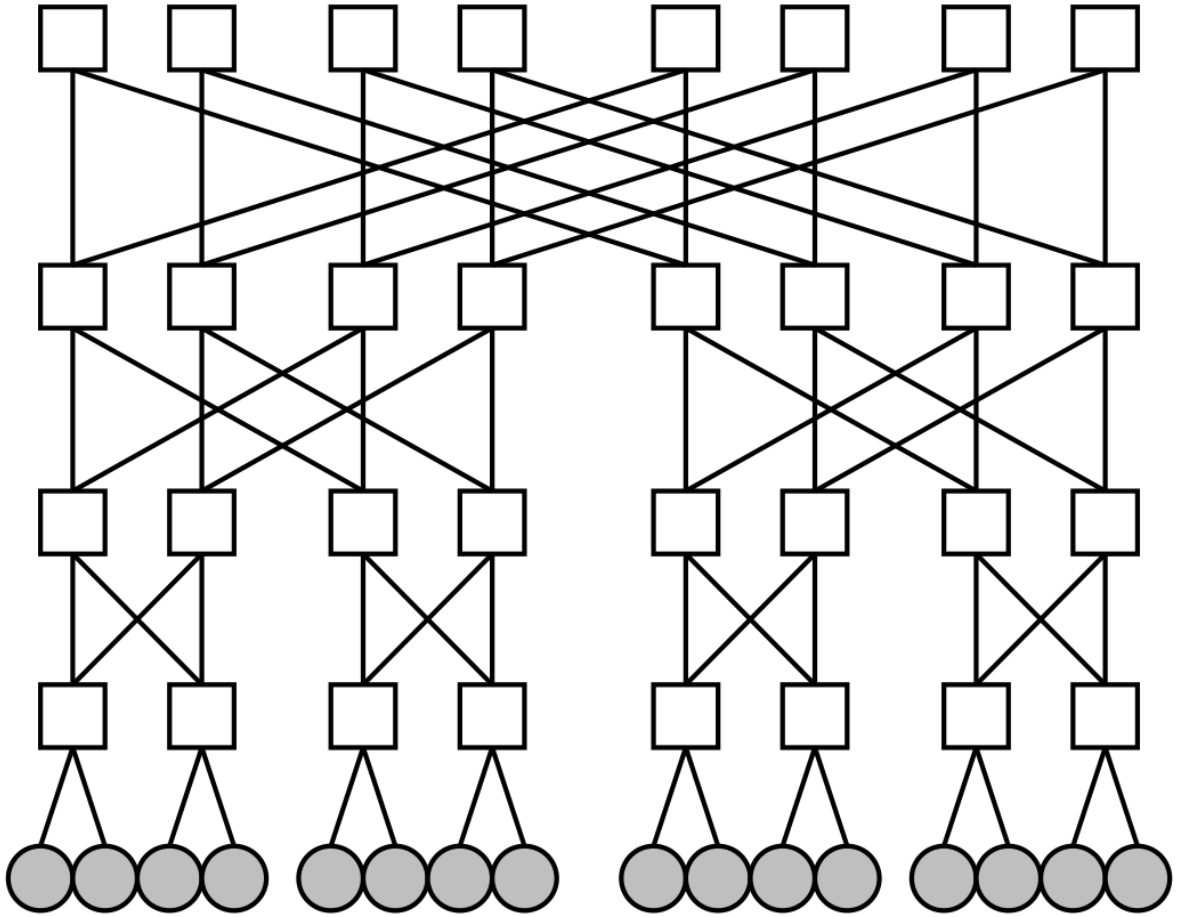


Considered topologies

- **Fat tree**.

  In a fat tree, branches nearer the top of the hierarchy are "fatter" (thicker) than branches further down the hierarchy.

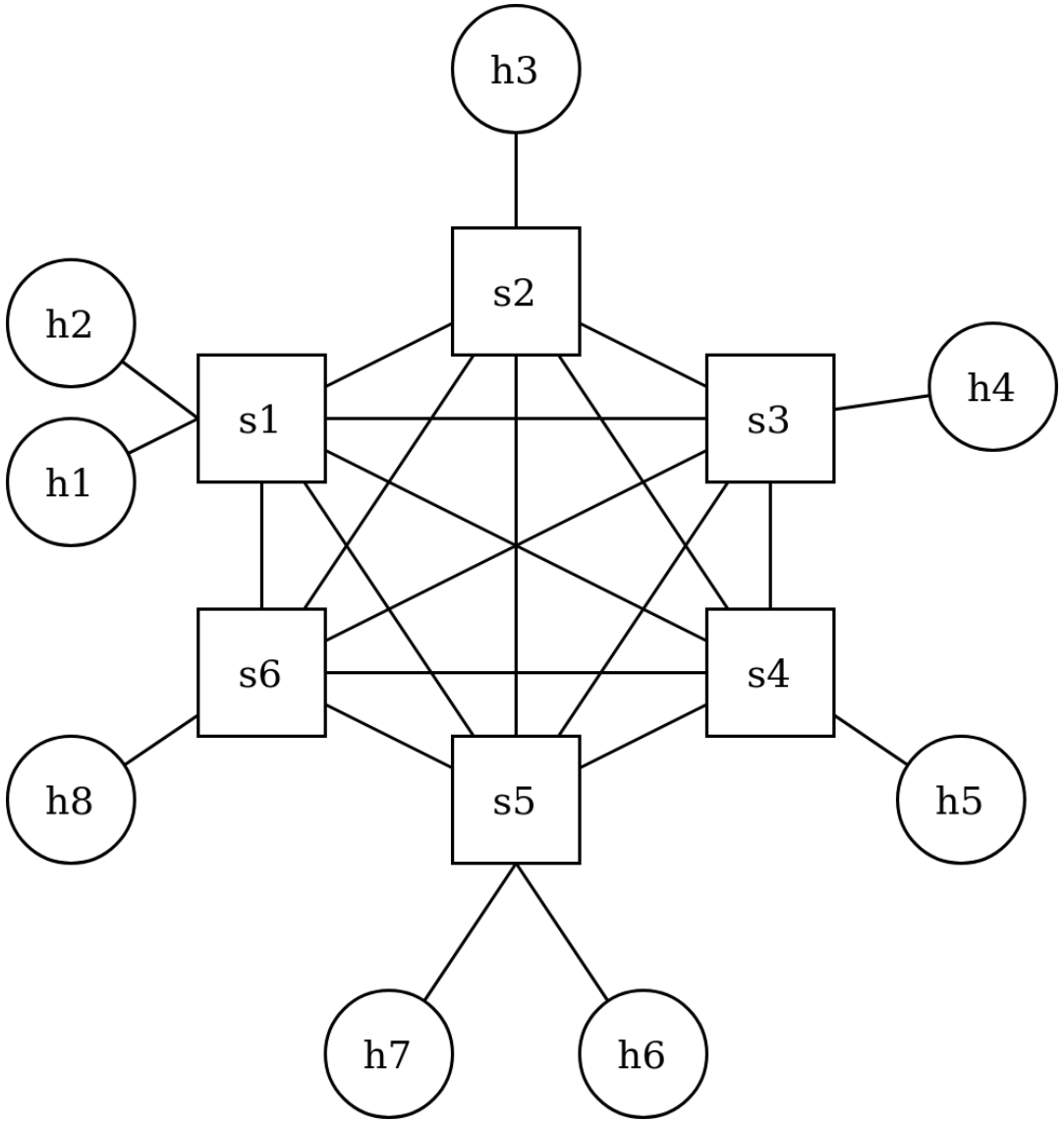
  Unlike classical tree topology, in which all connections between nodes are the same.



Considered topologies

- **Dragonfly**.

  Every router accommodates a set of terminal connections leading to end-points, and a set of topological connections leading to other routers.



SDN-controllers

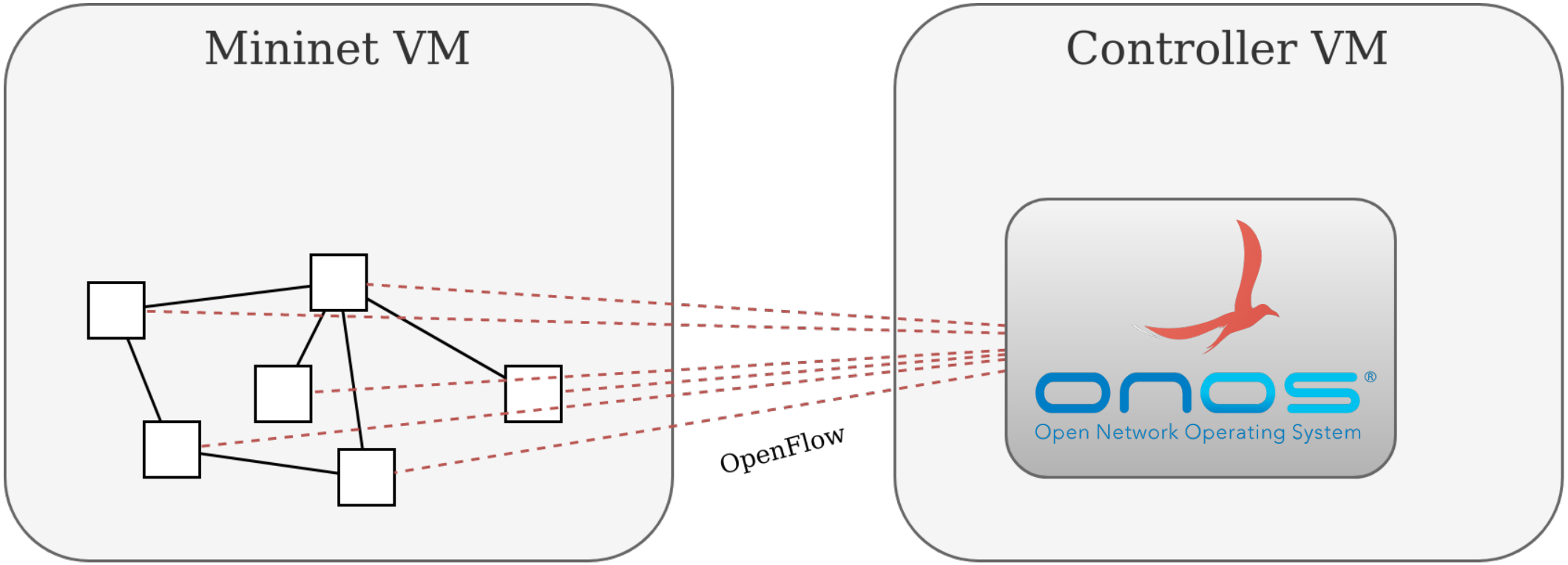
- Release: 0.4.4-Beryllium-SR4 (2016)
- Topology Loop Support
- Availability of a web interface

- Later versions lack the web interface
- Later versions do not support topology loops

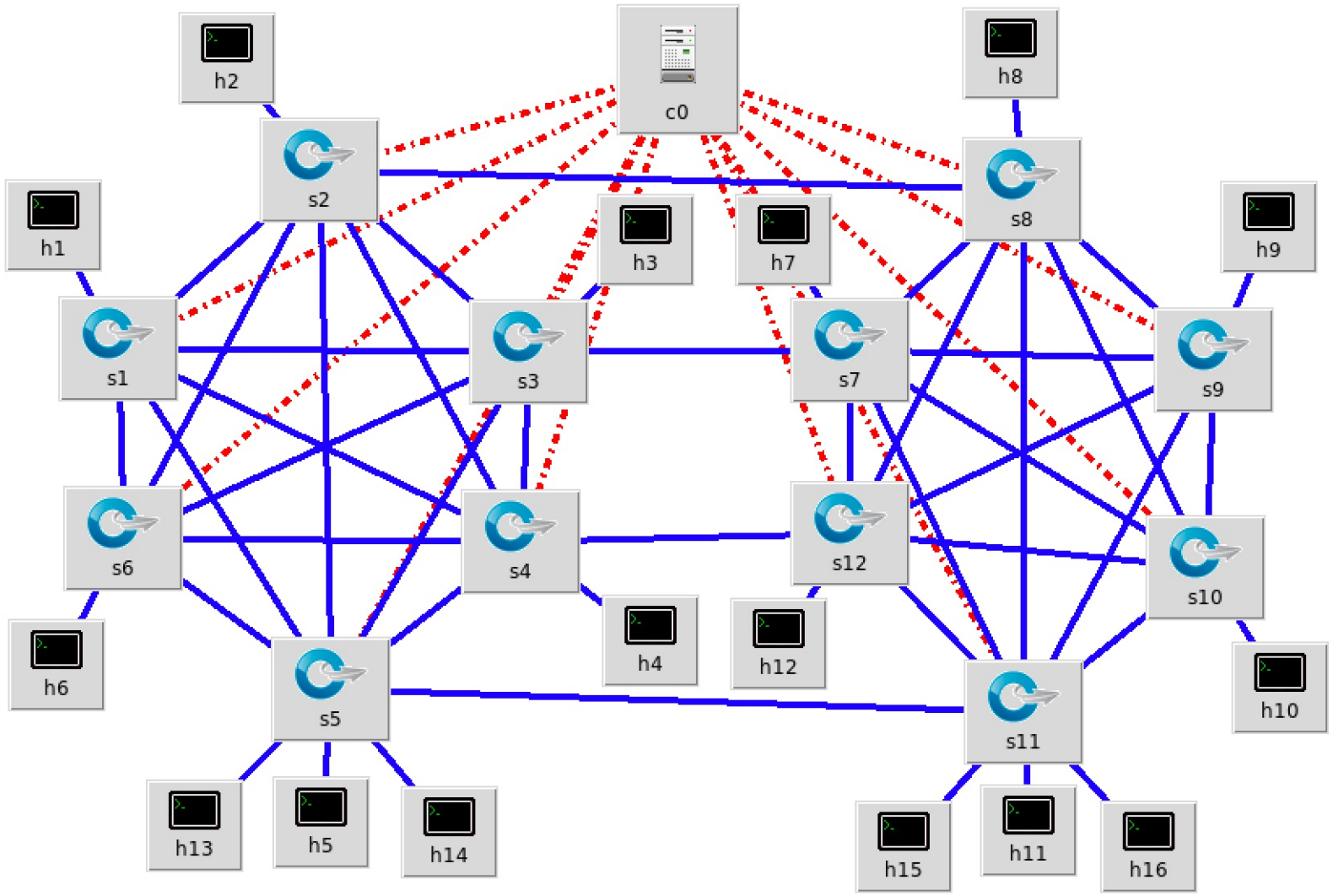
- Release: 2.4.0 Uguisu (2020)
- Topology Loop Support
- Availability of a web interface
  - Ability to view data flow and connection load in real time
- Traffic analysis services
- Services for viewing statistics

The SDN-controller is a **program**. Since in the SDN the control functionality is separated from the lower level of packet forwarding, the SDN controller can be located in a separate system.

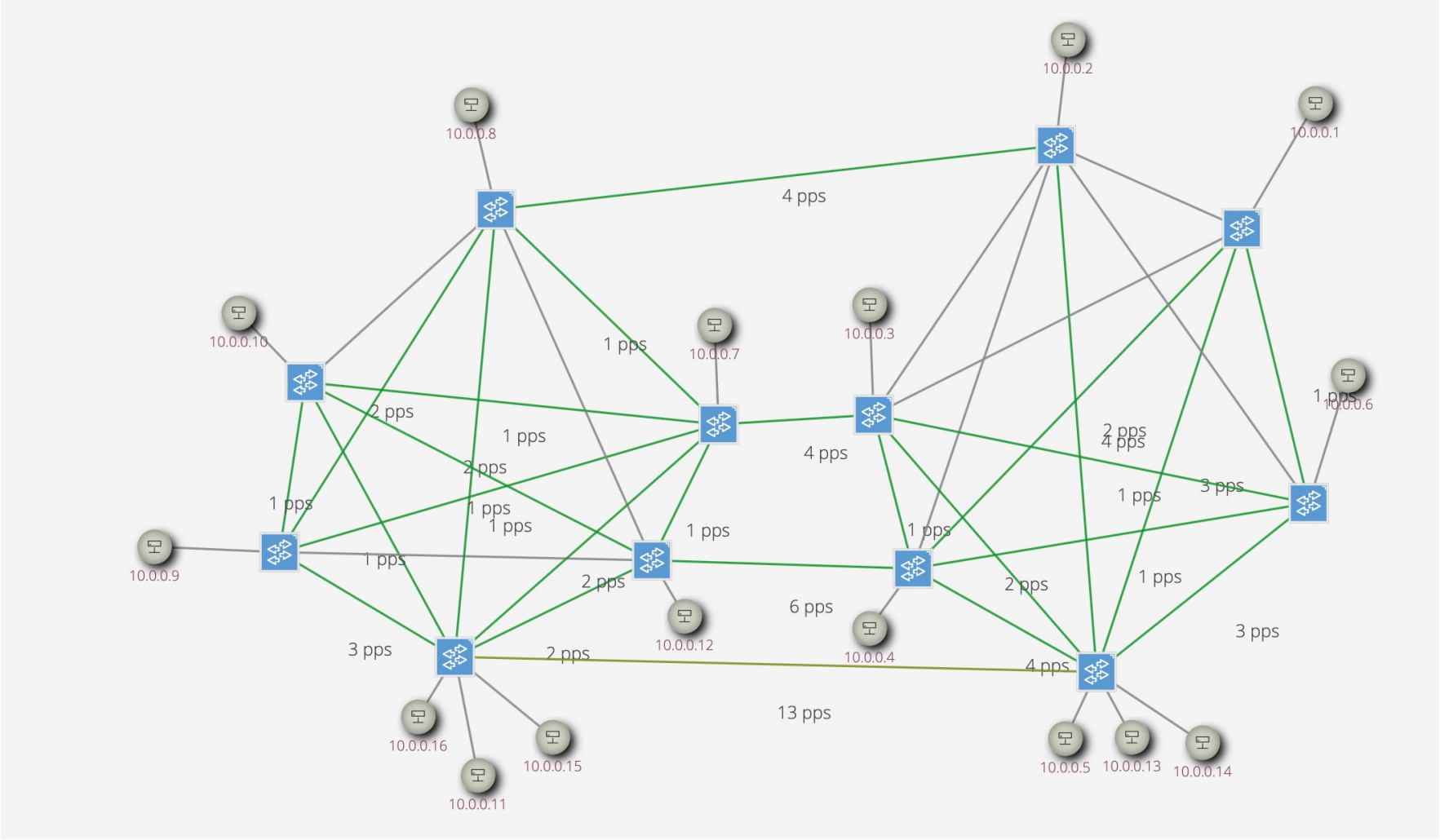
System structure



Mininet – testing topology



ONOS interface. Testing topology



Topology settings

5 different scenarios developed.

Common:

- Number of switches: 40
- Number of links: 100
- Number of traffic flows: 200 000

Various:

- Links between switches
- Switches throughput
- Start time, end time and direction of each flow

Traffic generation in mininet

- Common console commands (ping, wget, curl …)
- Ability to use scripts from each host
- All hosts have shared access to files, which is very convenient for running scripts
- Traffic generator D-ITG.

Traffic generator D-ITG

- Single-flow, Multi-flow, Daemon modes
- Detailed setting (generation time, delay, size / number of packets)
- Protocols (UDP, TCP, ICMP, SCTP, DCCP)
- Traffic emulation
  - Telnet - Telnet traffic emulator
  - DNS - DNS traffic emulator
  - Quake3 – Quake 3 traffic emulator
  - Csa – Counter strike traffic emulator of active player
  - Csi – Counter strike traffic emulator of inactive player
  - VoIP – Voice-over-IP traffic emulator

Traffic data collection

– traffic analyzer for computer networks

- Data collection should be performed on a virtual machine in which the SDN controller is running.
- Data received via the OpenFlow protocol is analyzed.

Traffic features extraction

flow_removed.byte_count	flow_removed.cookie	flow_removed.duration_nsec	flow_removed.duration_sec
flow_removed.idle_timeout	flow_removed.packet_count	flow_removed.priority	flow_removed.reason
length	match.length	match.pad	match.type
oxm.field	oxm.hm	oxm.length	oxm.value_etheraddr
oxm.value_uint32	type	version	xid
flow_removed.hard_timeout	flow_removed.table_id	oxm.class	oxm.value_ethertype

- OpenFlow 1.3 is considered
- 24 features were selected.
- https://www.wireshark.org/docs/dfref/o/openflow_v4.html - a list of all possible extracted features. Total 569 features.

Conclusion

- Using the mininet computer network emulator, several software-defined networks with different topologies were simulated.
- The tools presented as SDN controller software applications were analyzed.
- Tools for generating network traffic.
- Traffic capture tools on the controller side.
- Basic signs of traffic in the network were selected.

Future works

- Modeling larger distributed software-defined networks.
- Emulation of normal and malicious traffic within the network.
- Creating the dataset of SDN traffic with few types of network attacks.

Thanks for attention!

Volkov Sergey
volkserg1@gmail.com
Kurochkin I. I.
qurochkin@gmail.com