Methods and means of assuring the fault tolerance of the computer network supporting the operation of critical infrastructure

Author: Andrzej Paszkiewicz, Marek Bolanowski
Affiliation: Department of Complex Systems, Rzeszow University of Technology

Science for Peace and Security (2024)
Energy infrastructure resilience in response to war and other hazards
Advanced Research Workshop (ARW) supported by NATO

POLAND, Rzeszów, 23.09.2024

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Presentation plan

- The importance of network infrastructure as a component of critical infrastructure
- Key elements of the network infrastructure
- Methods and means of ensuring resilience to failures of a computer network
- Introduction to Software Defined Networking
- Island Architecture
- The concept of a cognitive network
- Redundancy in SDN
- Cascaded Anomaly Detection
- Examples of experiments and simulations we have conducted.

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

The importance of network infrastructure as a component of critical infrastructure

- Communication and connectivity
- Multi-sectoral operation
- National security
- Digital economy
- Crisis management
- Automation and Internet of Things

The provision of a reliable, efficient ICT infrastructure is therefore one of the key aspects of a network of critical infrastructure systems

Key elements of the network infrastructure

- End Devices
- Network Devices (Switches, Routers)
- Servers and Computing Centers
- Network Cabling and Other Transmission Media
- Connections and Broadband Internet
- Backup Power Systems
- Network Management Systems
- IoT elements
- Technical Personnel and Human Resources

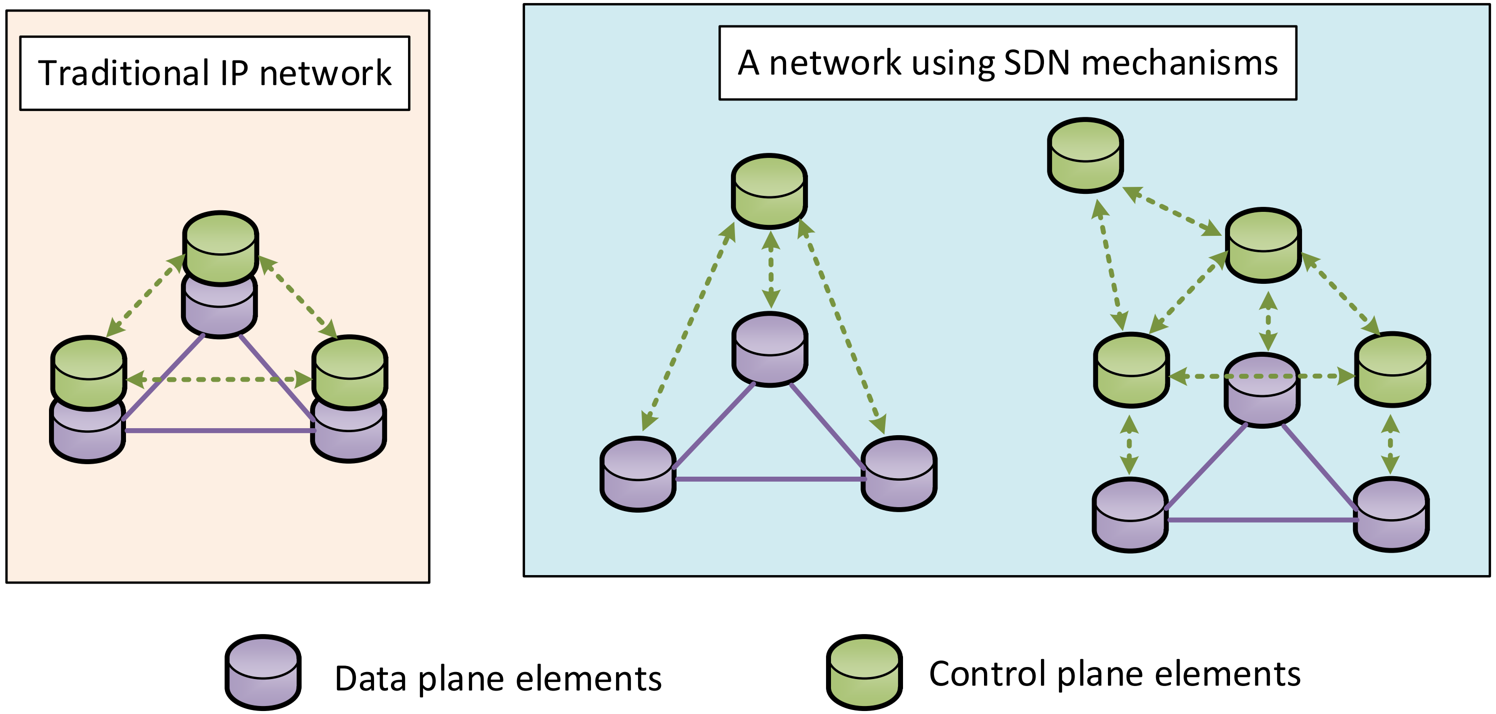
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Methods and means of ensuring resilience to failures of a computer network supporting the operation of critical infrastructure.

- Connection, device and power redundancy
- Failover Mechanisms
- Load Balncing
- Network Segmentation
- Monitoring and Network Management
- Network Security
- Backup Systems and Data Recovery
- Robustness tests and failure simulations
- Power stability

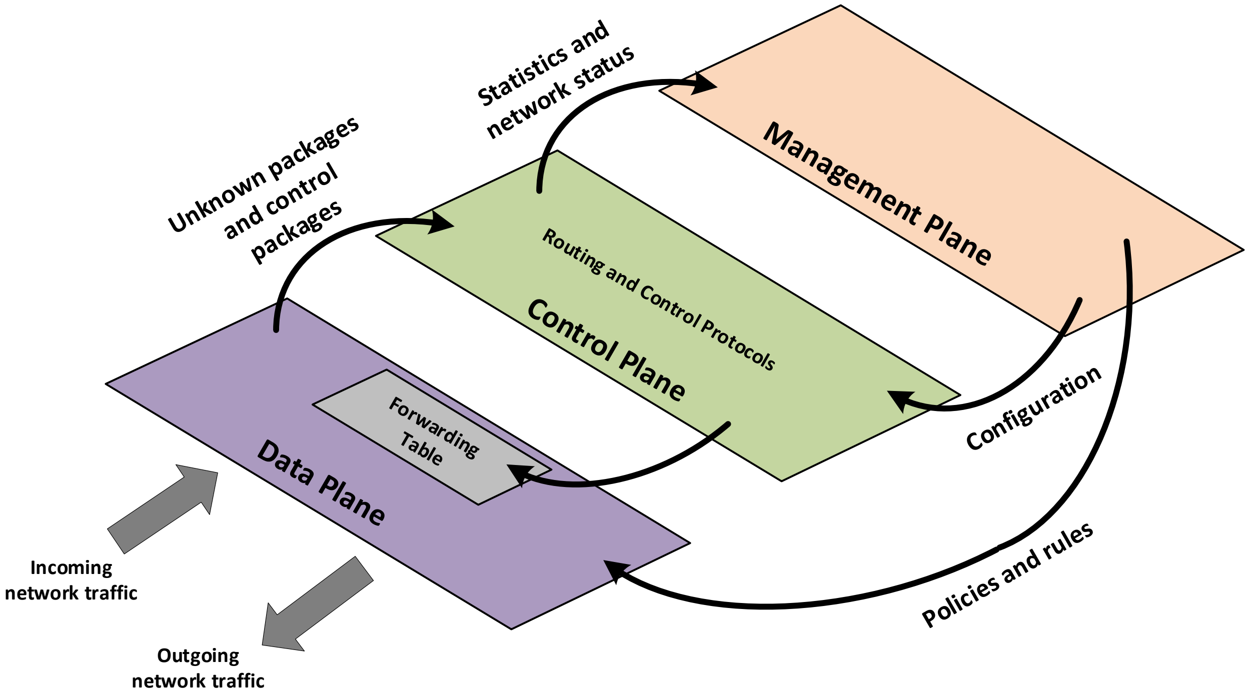
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

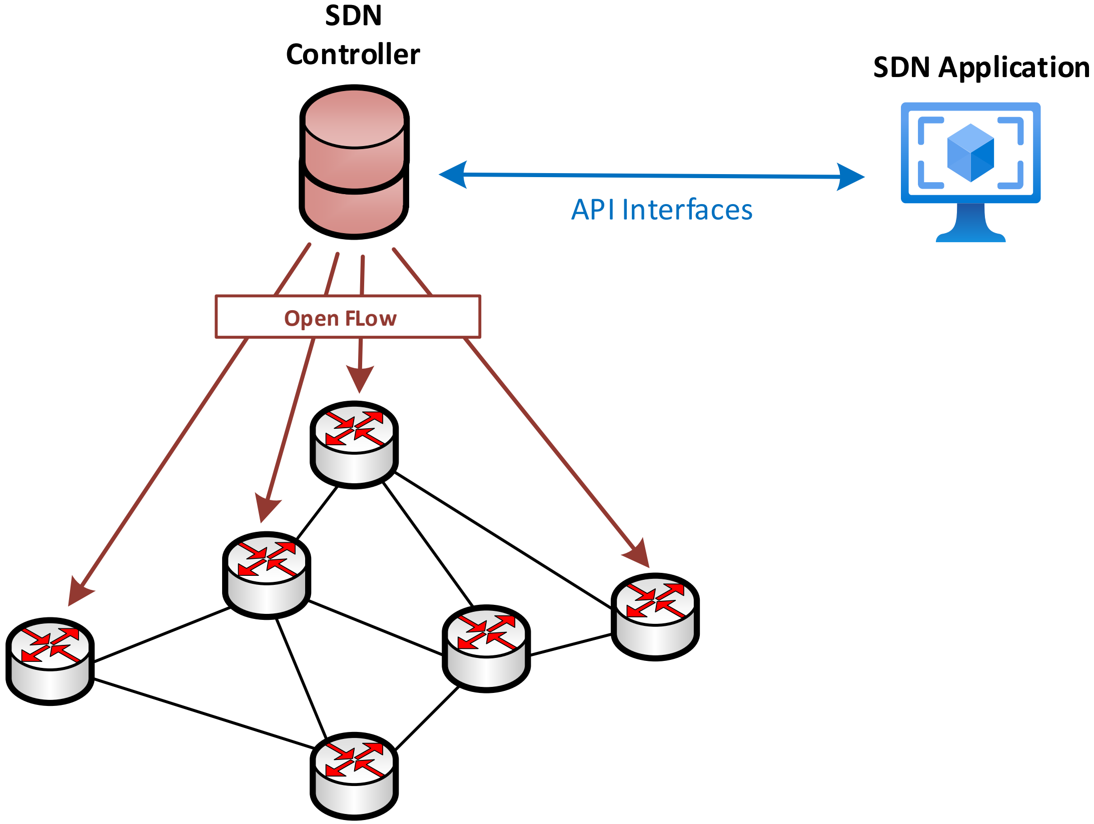
Classic Network Management vs. Software Defined Networking



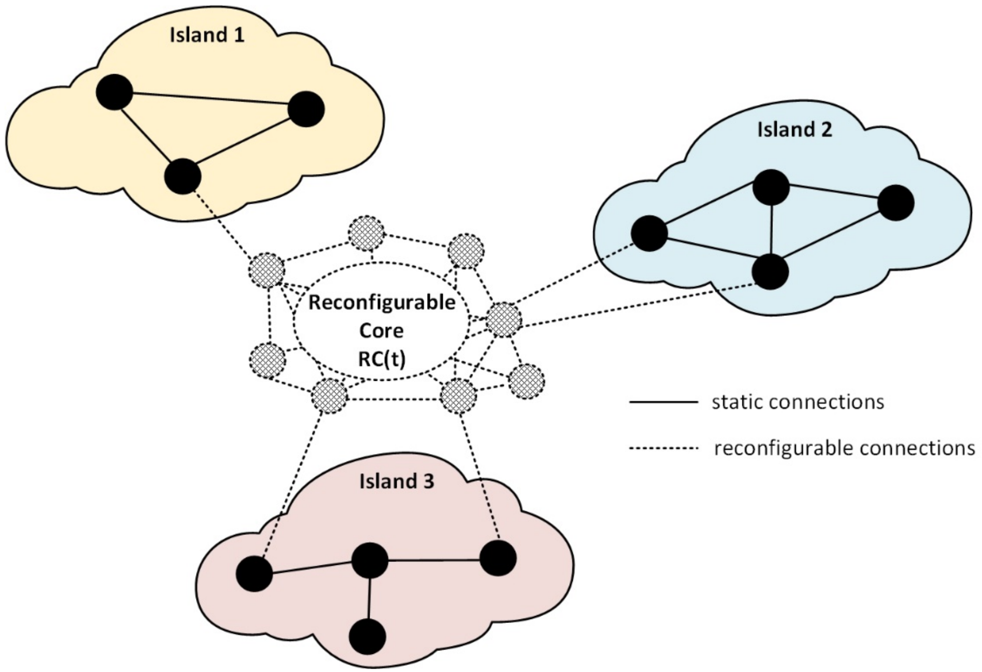
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

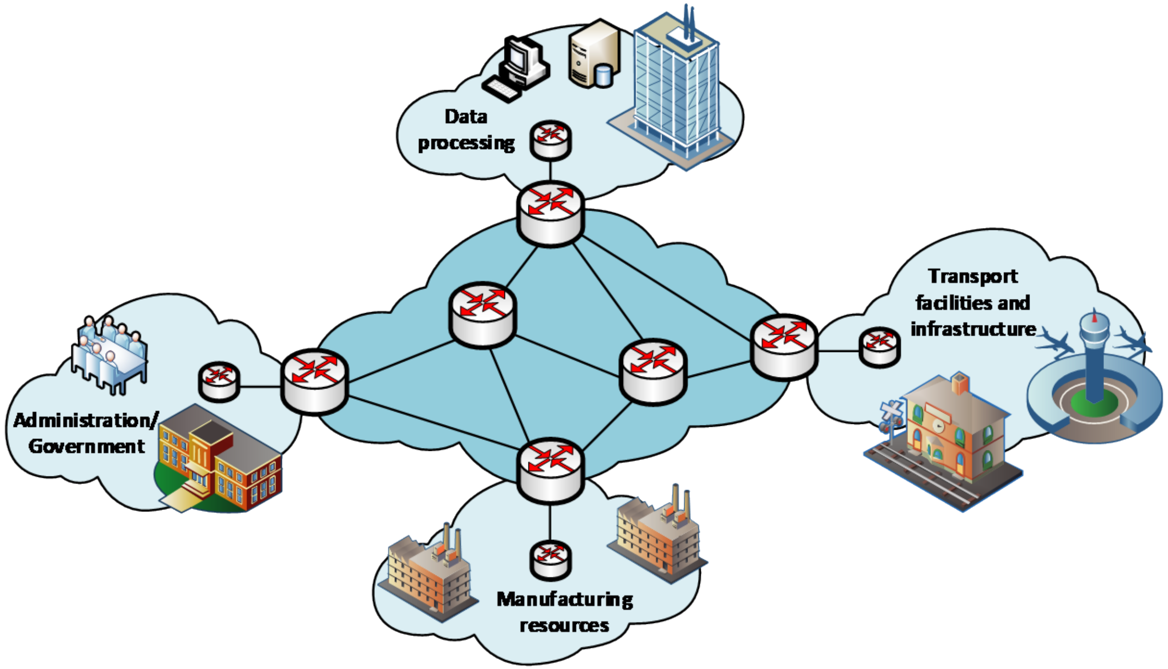
Software Defined Networking



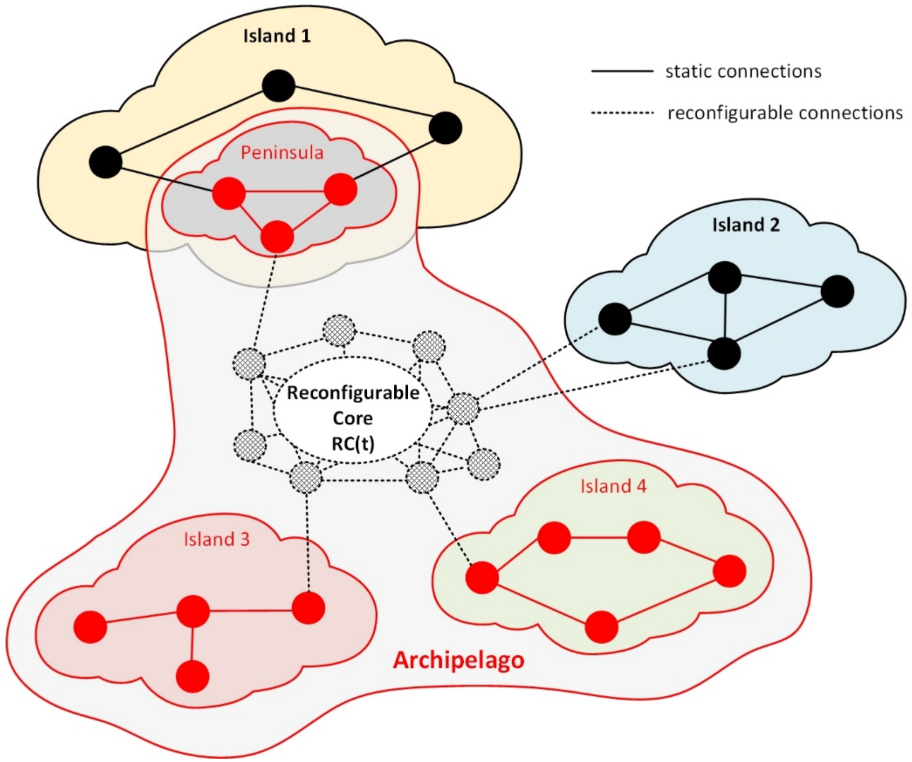


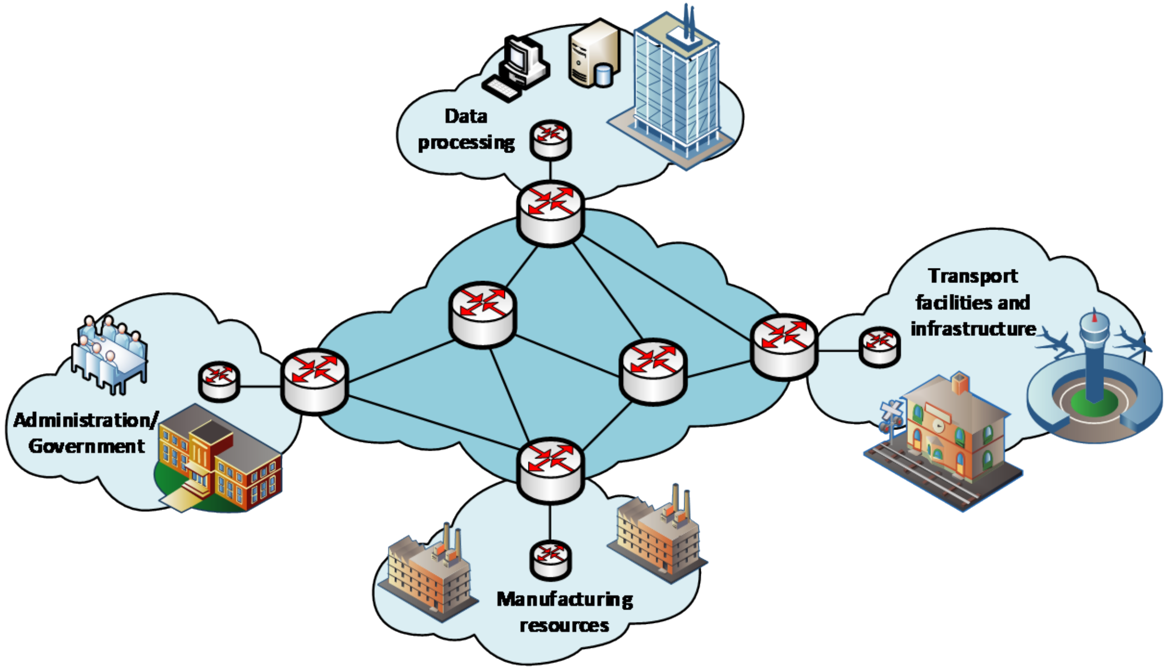
Island Architecture





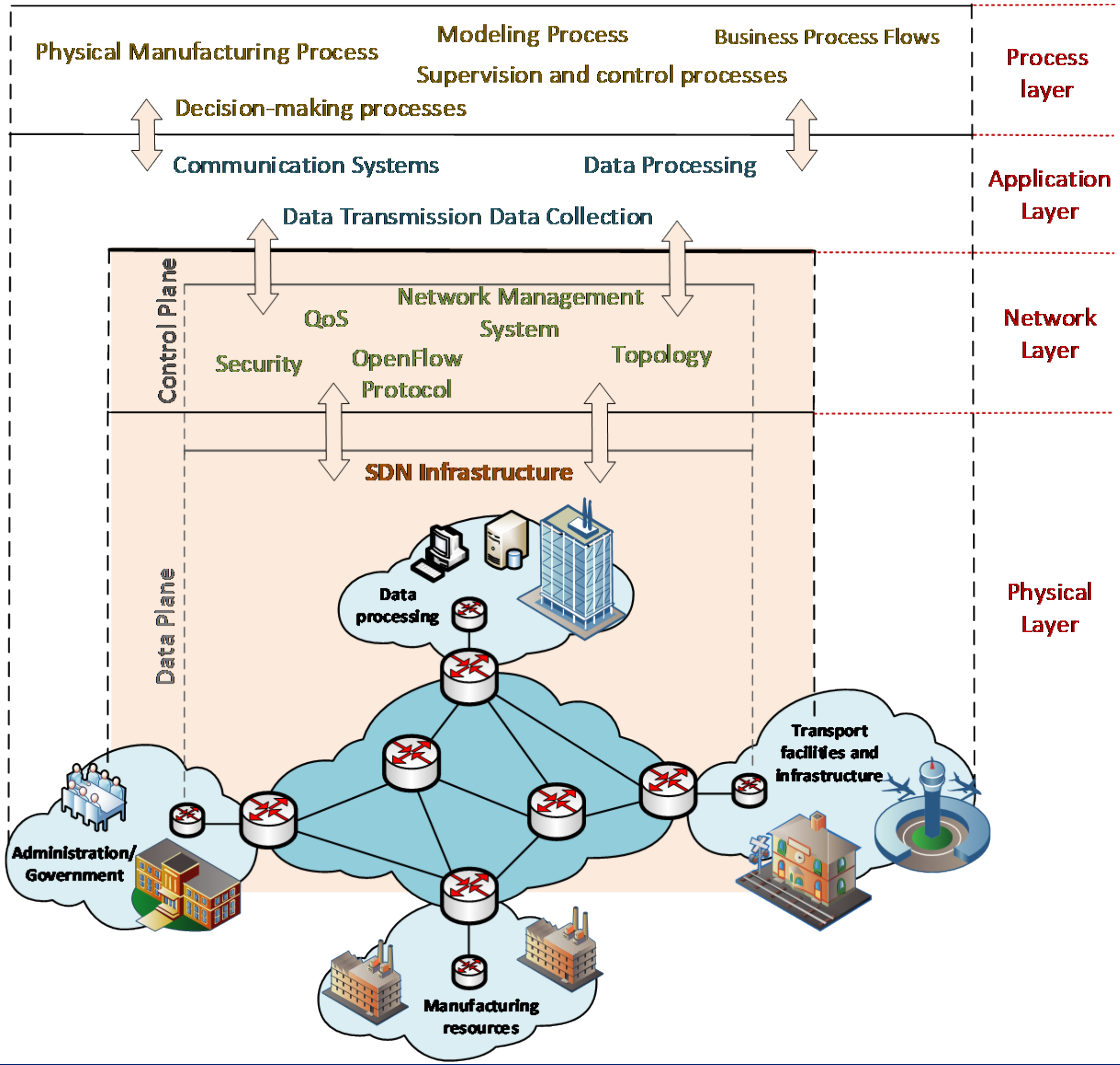
Island Architecture - Archipelago





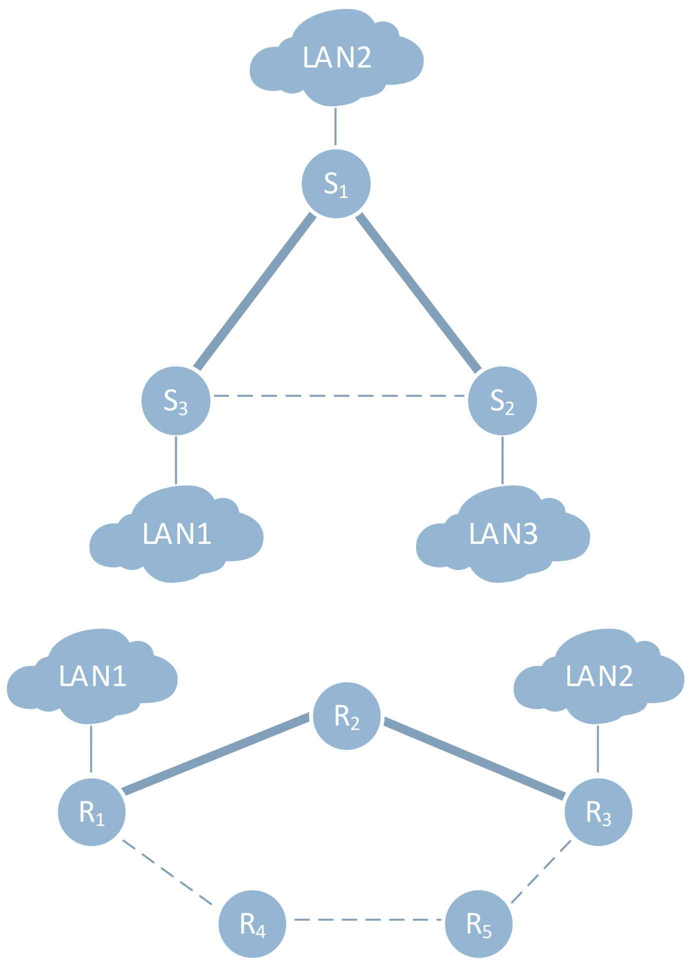
Island Architecture in the Context of SDN

- Open System
- Virtualization
- Scalability
- Independence of layers



NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

- **Lack of network engineers who understand the nature of the problems and not just focus on implementing deployment scenarios.**
- **Need for rapid reconfiguration changes for distributed and industrial systems.**
- **Strong pressure from AI**
- **Strong pressure from industry and IoT systems**
- **The idea of hyperconverged networks**
- **Static, archaic but still proven and working structure of network systems**



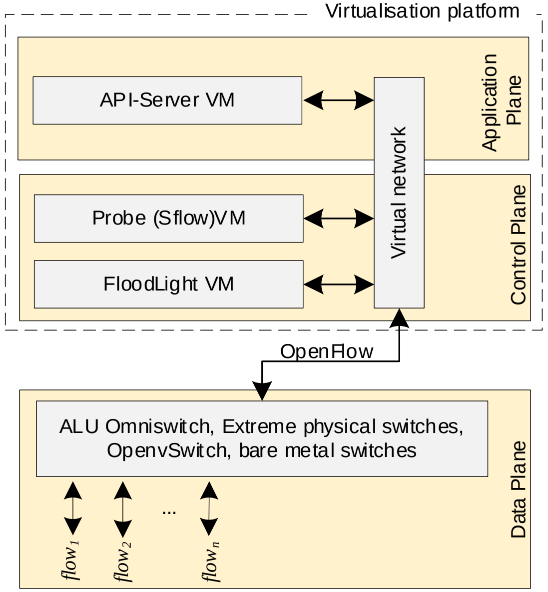
NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

In communication networks, cognitive network (CN) is a new type of data network that makes use of cutting edge technology from several research areas (i.e. machine learning, knowledge representation, computer network, network management) to solve some problems current networks are faced with.

- **Adaptability,**
- **Learning Ability,**
- **Autonomy,**
- **Sensing Capabilities,**
- **Reasoning and Decision Making,**
- **Self-Organization,**
- **Resource Awareness,**
- **Security and Privacy Considerations,**
- **Interoperability.**

Research paper

Reality




```
X460G2-24t-G4.3 # enable openflow
The current access-list width is single
* X460G2-24t-G4.4 # show openflow flows
Total number of OpenFlow flows : 1
Total number of default flows  : 1

Flow name          Type      Duration (secs)   Prio
---------------- ---- ------------------ ----- ------------
of_0               ACL                    4      0
    Match   :
    Actions:   CONTROLLER:65535
ofFDB_0            ACL                 4640      0
    Match   :  FDB Entry
    Actions:   forward

Packets:  (*) Cumulative packet count for all FDB flows
* X460G2-24t-G4.5 # openflow: Process openflow pid 1945 died
../ovs/lib/ovs-atomic.h:618: assertion old_refcount > 0 faile
Code:
n ovs_refcount_unref_relaxed()
777324c4  24070010 addiu  a3,zero,16
777324c8  24021063 addiu  v0,zero,4195
777324cc  0000000c syscall 0
```

```
Process openflow pid 1945 died
assertion old_refcount > 0 faile
```

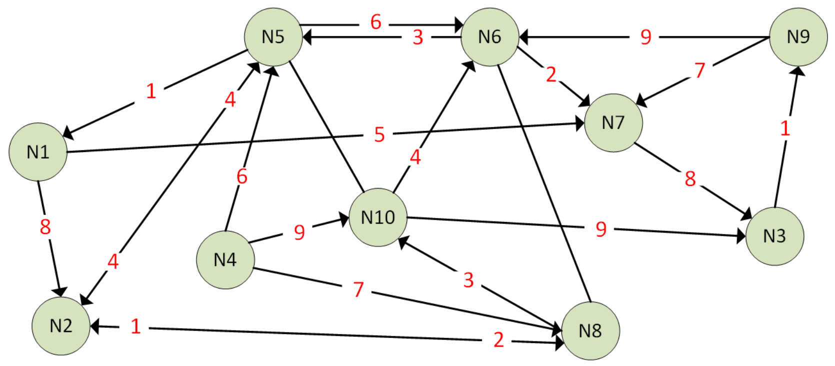
Use of metaheuristics-based approaches, to solve the load balancing problem in computer networks, remains an active (and promising) research area.

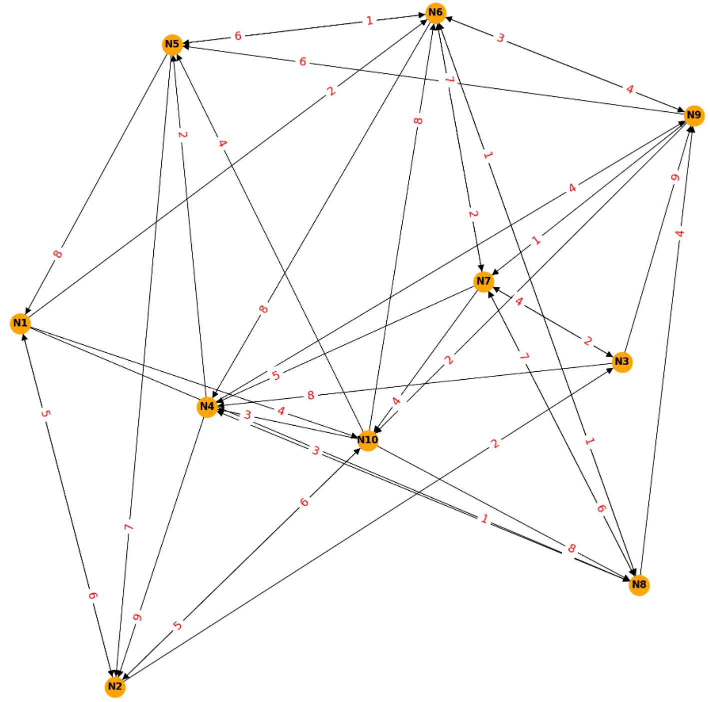
The value for lij is determined as the sum of flows psd passing through the edge eij.

The problem can be formulated as:

$$\min\left(\max\left(l_{ij}\right)\right)$$

$$M_W = M \bullet W = \begin{pmatrix} w_{11}\cdot e_{11} & \dots & w_{1N}\cdot e_{1N} \\ \vdots & \ddots & \vdots \\ w_{N1}\cdot e_{N1} & \cdots & w_{NN}\cdot e_{NN} \end{pmatrix} \qquad F_{sd} = \begin{pmatrix} p_{11} & \dots & p_{1N} \\ \vdots & \ddots & \vdots \\ p_{N1} & \cdots & p_{NN} \end{pmatrix}$$

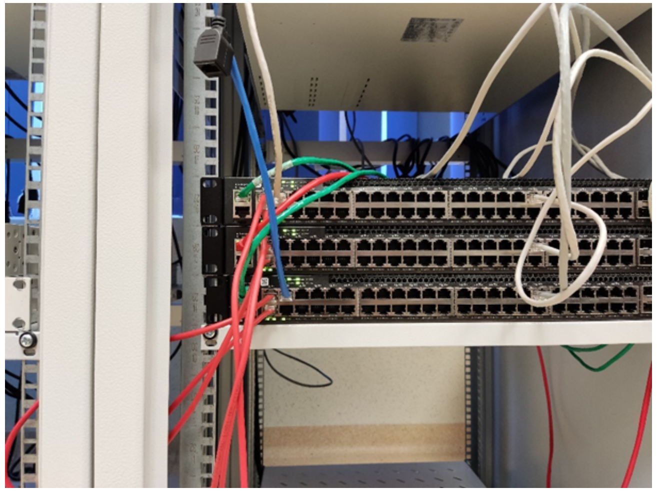
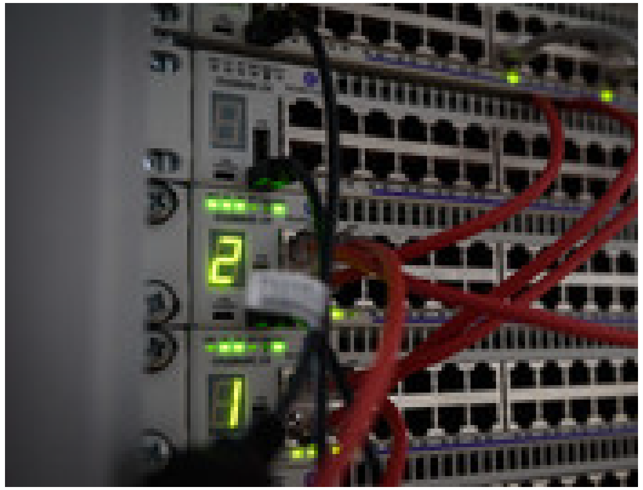




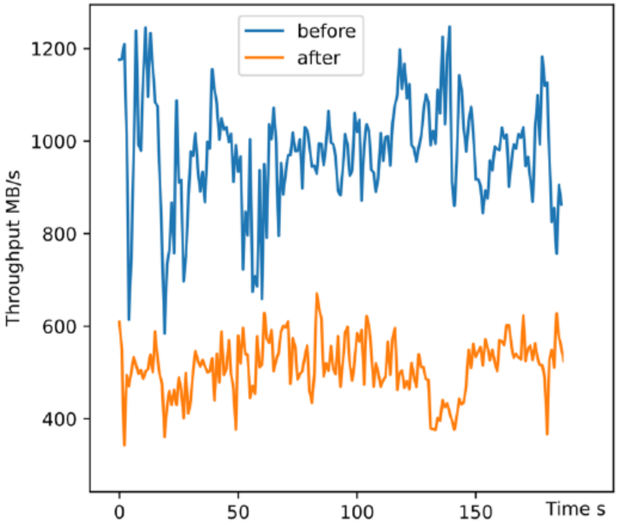
This workshop is supported by: The NATO Science for Peace and Security Programme

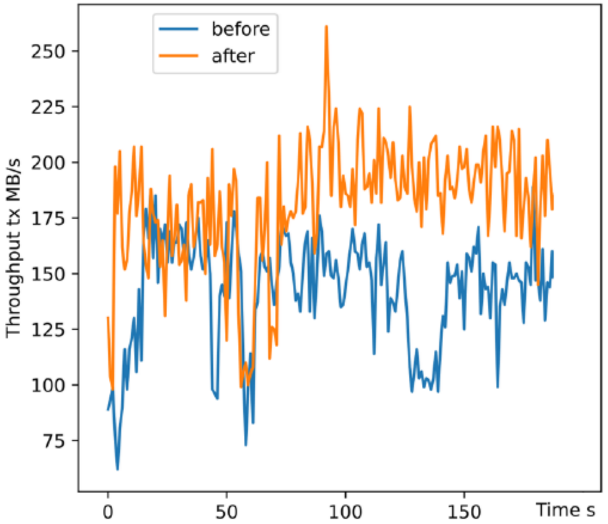
- The code of the algorithm was implemented in Python, during the implementation, apart from the standard Python library modules, also numpy and matplotlib libraries and the networkx package were used. All experiments were carried in a simulation environment with the following parameters: Debian GNU/Linux 10 4.19.0-8-amd64; 8 CPUs Intel® Xeon® CPU E5-2620 v3 @ 2.40GHz; RAM: 39,3 GB.

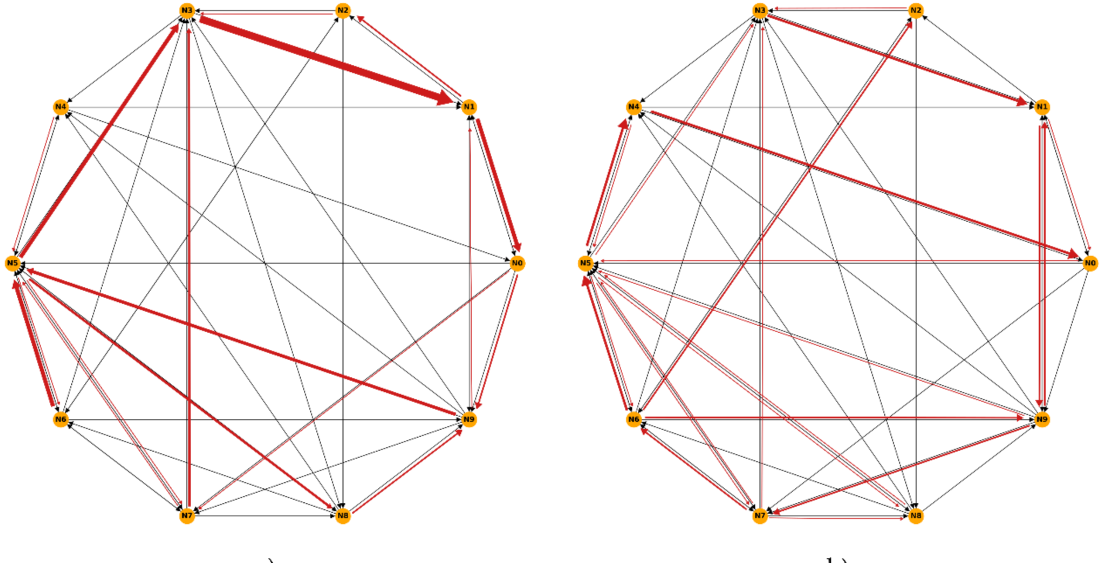
- SDN architecture in the environment of real enterprise class network devices (Extreme and OmniSwitch Alcatel-Lucent), “bare metal” switches (Edge Core), and OpenvSwitches. During experiments, a special stand configured for research of phenomena in the “Internet of Everything”

The first set of tests was focused on the effectiveness of optimization. For flows in the network represented by graph G(N,E), where |N| = 10 and |E| = 39, the values of the function (2) were compared before and after using the SDNGALB algorithm. Table 1 shows the mean value of max (lij), before and after optimization, calculated as the arithmetic mean of 10 executions of the SDNGALB algorithm for the defined network, for |Fsd| = 20; 30; 40; 50; 100; 200.





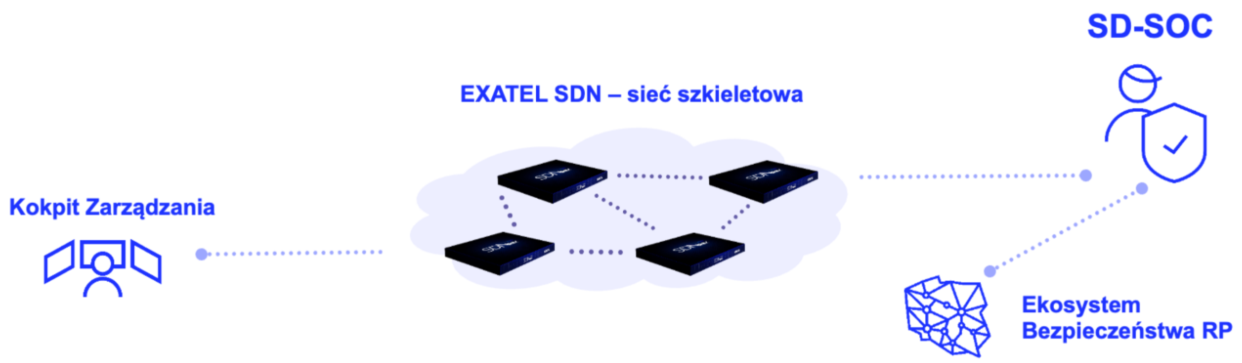


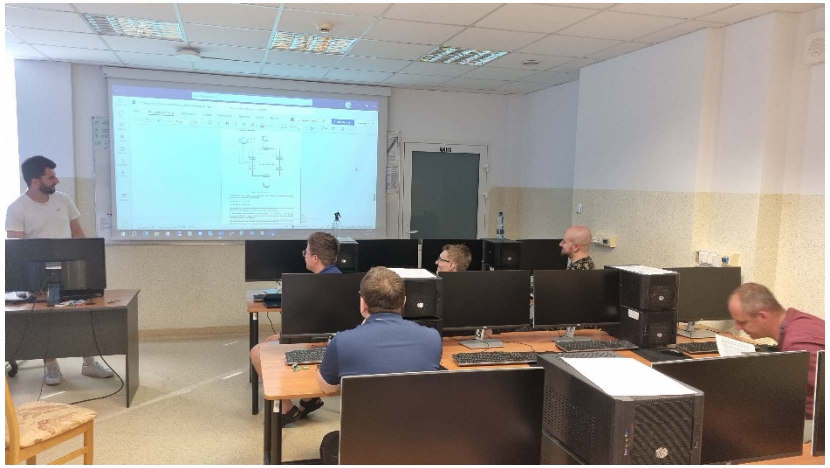
a) b)

Arithmetic mean of 10 executions	$\lvert F_{sd} \rvert$					
	20	*30*	*40*	*50*	*100*	*200*
$\overline{\max}\,(l_{ij})$ before optimisation	5,6	8,6	8.8	11,6	21,8	41,6
$\overline{\max}\,(l_{ij})$ after optimisation	2,8	4	4,8	5,8	11,6	22,4
Effectiveness of optimisation	50%	53%	45%	50%	47%	56%

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

CriNet, Critical Network SDN Security System - SDN network security system for critical infrastructure





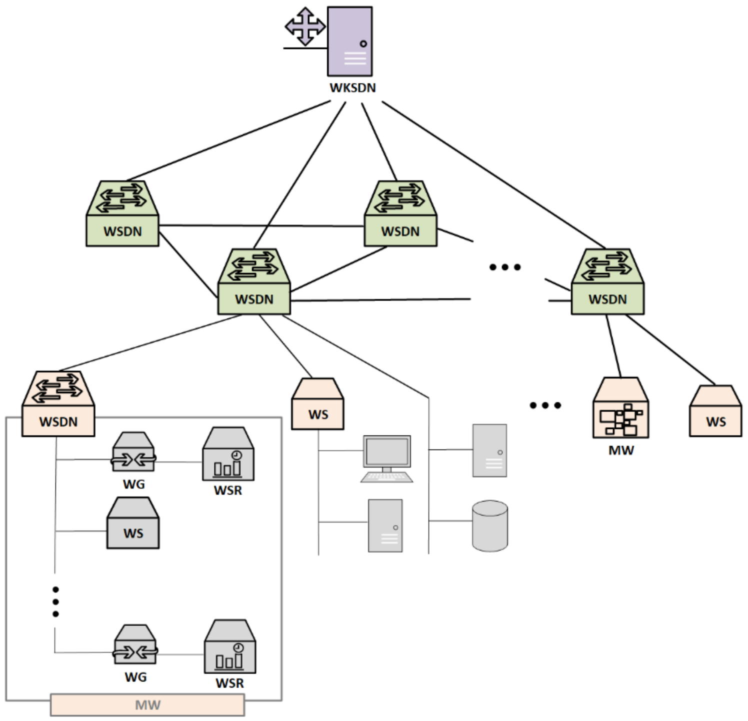
EXATEL's partners in this project are Rzeszow University of Technology and GAZ-SYSTEM, which is the operator of one of the most important elements of critical infrastructure in Poland - the natural gas transmission system.

RZESZOW UNIVERSITY OF TECHNOLOGY · EXATEL · GAZ system · NCBR Narodowe Centrum Badań i Rozwoju

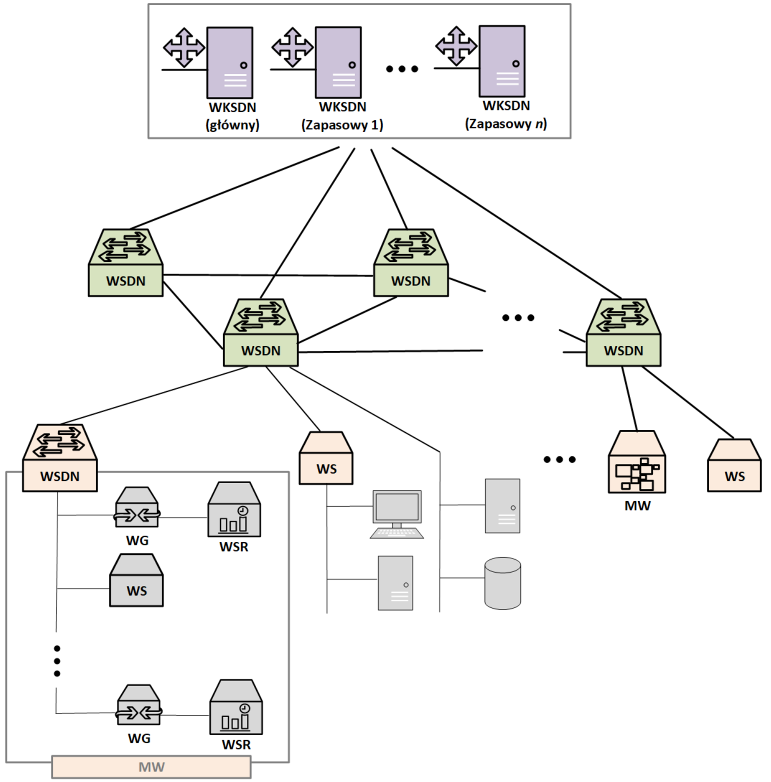
NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

Redundancy in SDN - controllers

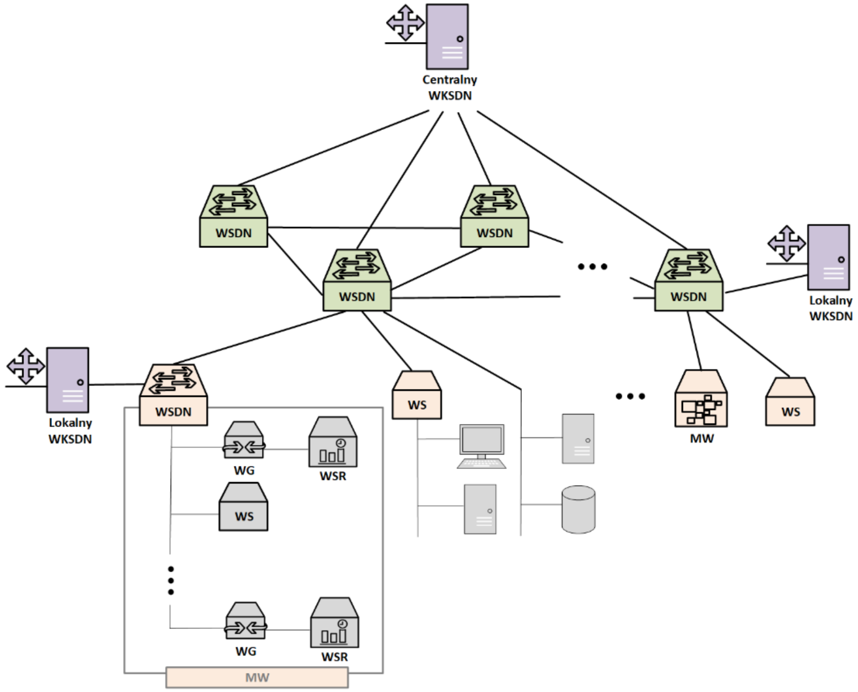
The classic approach



Topological structure with local SDN controllers

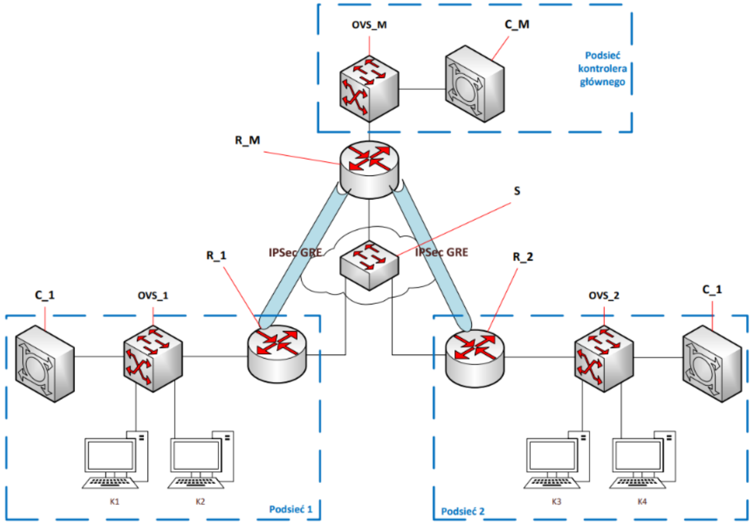


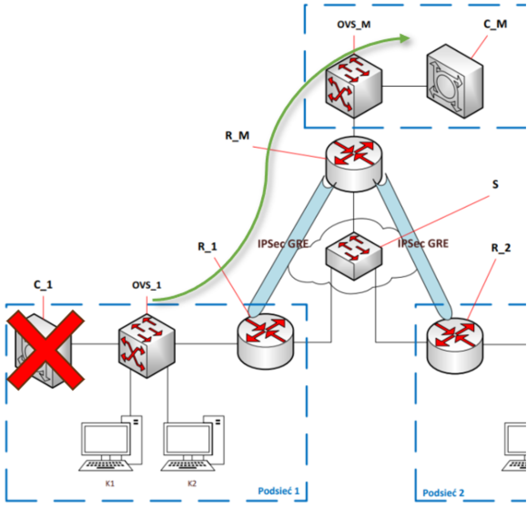
Topological structure with backup SDN controllers



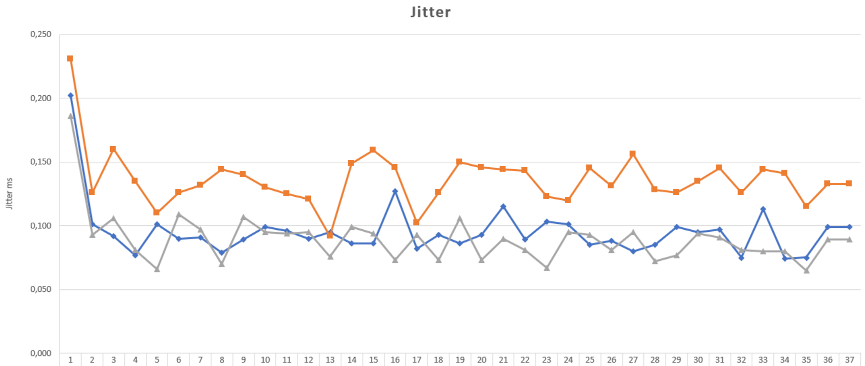
Redundancy in SDN - controllers

Controller redundancy based on Docker and Atomix






```
k2@K2:~$ ping 172.16.1.20
PING 172.16.1.20 (172.16.1.20) 56(84) bytes of data.
64 bytes from 172.16.1.20: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 172.16.1.20: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 172.16.1.20: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 172.16.1.20: icmp_seq=4 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=5 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=6 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=7 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=8 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=9 ttl=64 time=0.021 ms
64 bytes from 172.16.1.20: icmp_seq=10 ttl=64 time=0.021 ms
64 bytes from 172.16.1.20: icmp_seq=11 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=12 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=13 ttl=64 time=0.021 ms
64 bytes from 172.16.1.20: icmp_seq=14 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=15 ttl=64 time=0.022 ms
64 bytes from 172.16.1.20: icmp_seq=16 ttl=64 time=0.020 ms
64 bytes from 172.16.1.20: icmp_seq=17 ttl=64 time=0.021 ms
64 bytes from 172.16.1.20: icmp_seq=18 ttl=64 time=0.023 ms
64 bytes from 172.16.1.20: icmp_seq=19 ttl=64 time=0.021 ms
64 bytes from 172.16.1.20: icmp_seq=20 ttl=64 time=0.024 ms
^C
--- 172.16.1.20 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19252ms
rtt min/avg/max/mdev = 0.013/0.020/0.024/0.002 ms
```



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Test I	0,20	0,10	0,09	0,07	0,10	0,09	0,09	0,07	0,08	0,09	0,09	0,09	0,09	0,08	0,08	0,12	0,08	0,09	0,08
Test II	0,23	0,12	0,16	0,13	0,11	0,12	0,13	0,14	0,14	0,13	0,12	0,12	0,09	0,14	0,15	0,14	0,10	0,12	0,15
Test III	0,18	0,09	0,10	0,08	0,06	0,10	0,09	0,07	0,10	0,09	0,09	0,09	0,07	0,09	0,09	0,07	0,09	0,07	0,10

	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
Test I	0,09	0,11	0,08	0,10	0,10	0,08	0,08	0,08	0,08	0,09	0,09	0,09	0,07	0,11	0,07	0,07	0,09	0,09
Test II	0,14	0,14	0,14	0,12	0,12	0,14	0,13	0,15	0,12	0,12	0,13	0,14	0,12	0,14	0,14	0,11	0,13	0,13
Test III	0,07	0,09	0,08	0,06	0,09	0,09	0,08	0,09	0,07	0,07	0,09	0,09	0,08	0,08	0,08	0,06	0,08	0,08

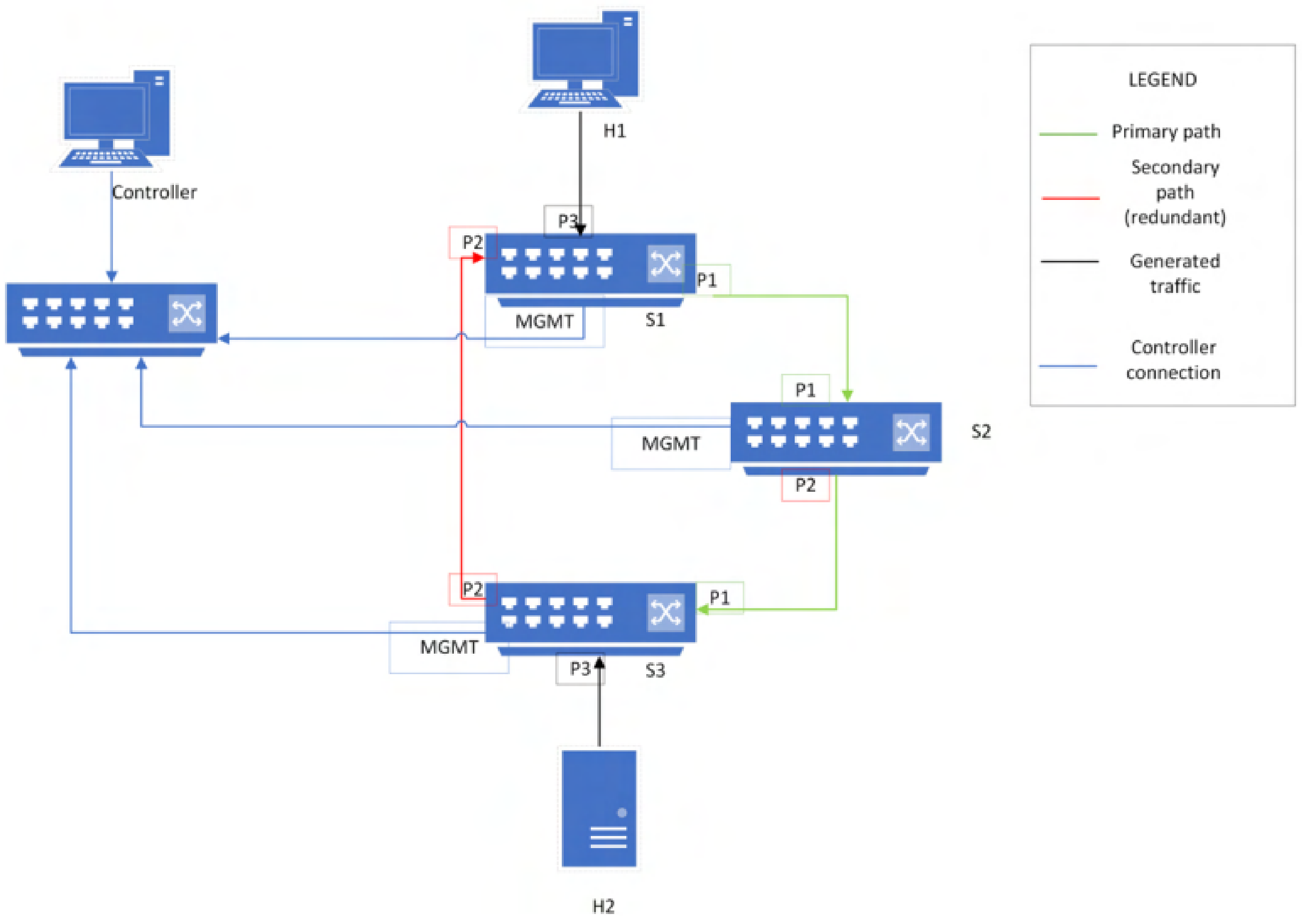
Indeksy pomiarowe wraz z wynikami

```
[ ID] Interval           Transfer     Bandwidth         Jitter    Lost/Total Datagrams
[  3] 0.0000-30.0046 sec  3.75 MBytes  1.05 Mbits/sec   0.077 ms    0/ 2678 (0%)
```

Methods and means of assuring the fault tolerance of the computer network supporting the operation of critical infrastructure

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

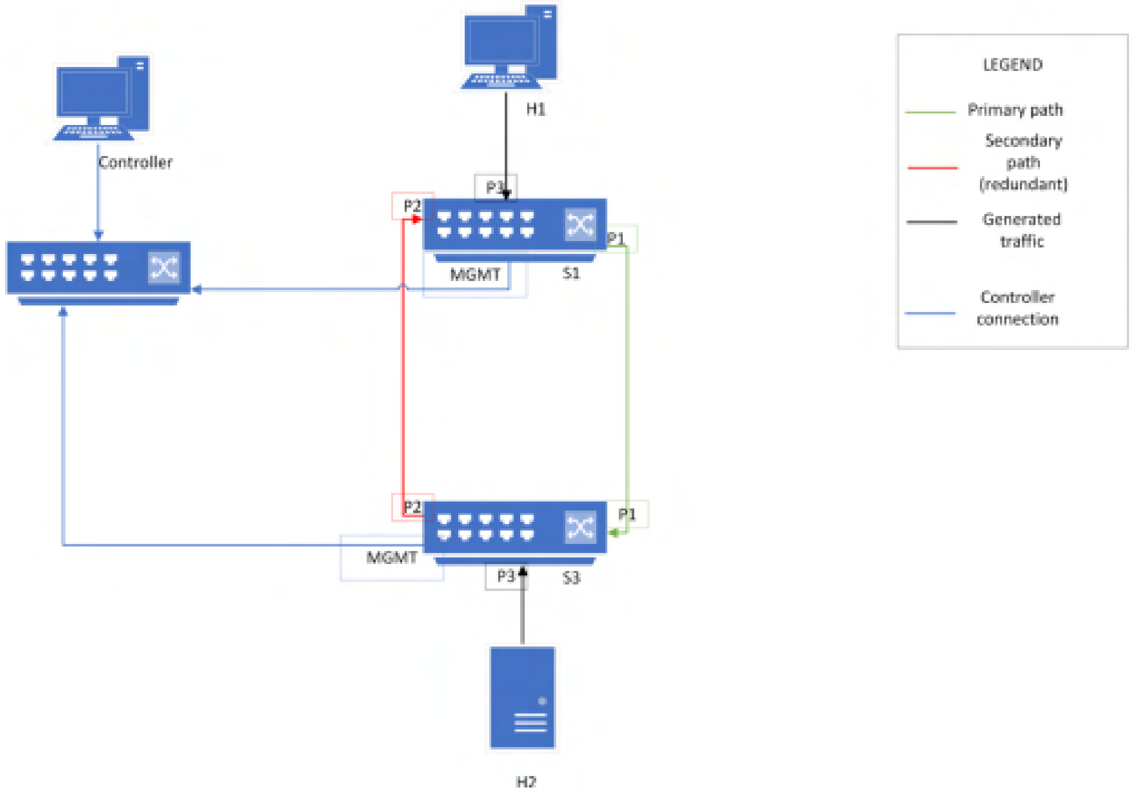
Link redundancy in software-defined networks



Methods and means of assuring the fault tolerance of the computer network supporting the operation of critical infrastructure

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Link redundancy in software-defined networks

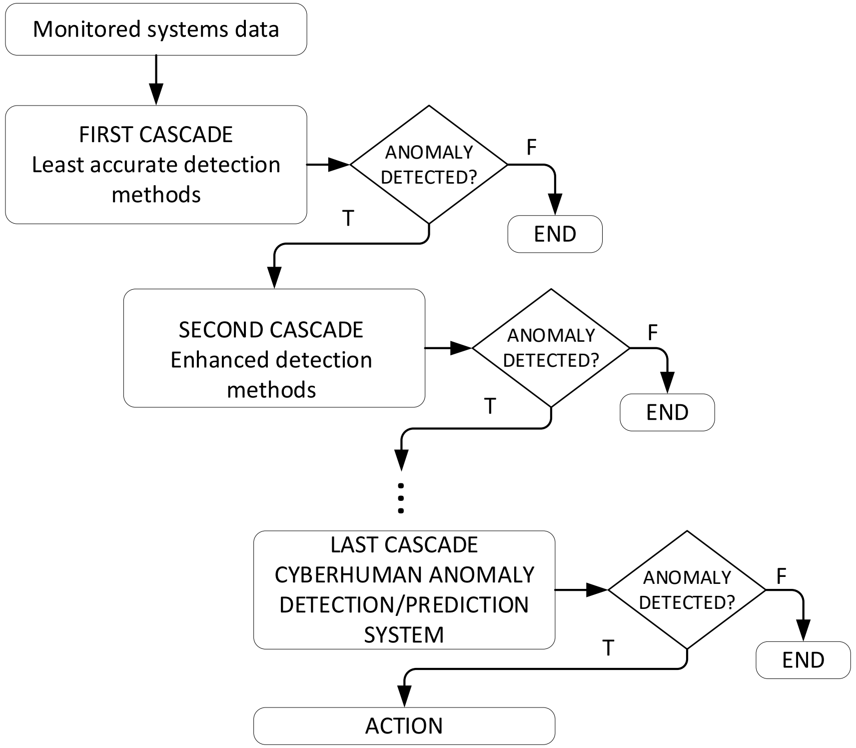


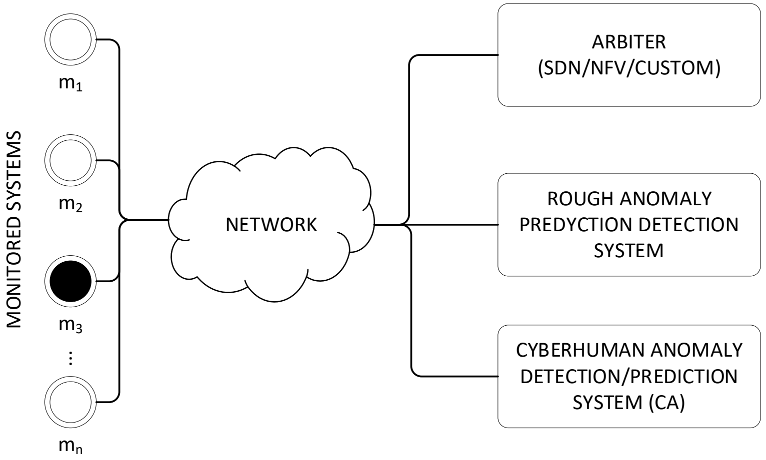
Measurements for path change using POX controller with automatic port shutdown (800 Mbits/sec)

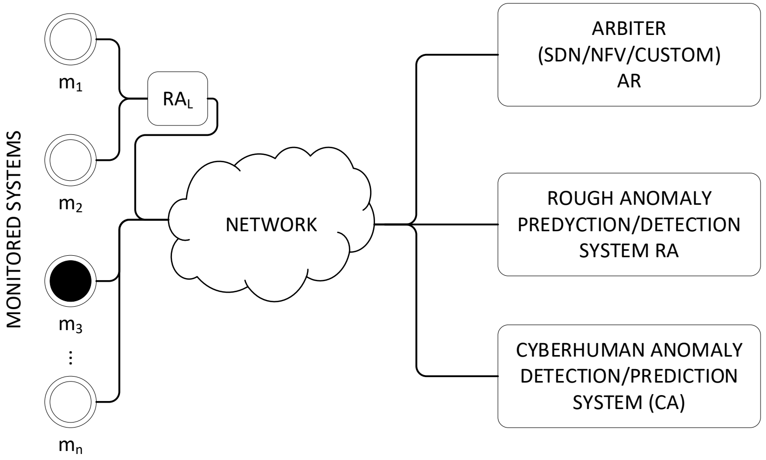
No.	Bitrate (Mbits/sec)	Jitter (ms)	Lost Datagrams	Sent Datagrams	Loss Ratio (%)
1	791	0.001	7490	1035878	0.72
2	790	0	10378	1035921	1
3	791	0.001	8720	1036518	0.84
4	791	0	8698	1036473	0.84
5	789	0	10928	1036585	1.1
6	794	0	4164	1036120	0.4
7	792	0.001	5630	1035361	0.54
8	795	0	2810	1036657	0.27
9	787	0.001	12099	1035800	1.2
10	782	0	20055	1036484	1.9
Avg.	790.2	0.0004	9097.2	1036179.7	0.881

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

Cascaded Anomaly Detection with Coarse Sampling in Distributed Systems - as a reconfiguration trigger





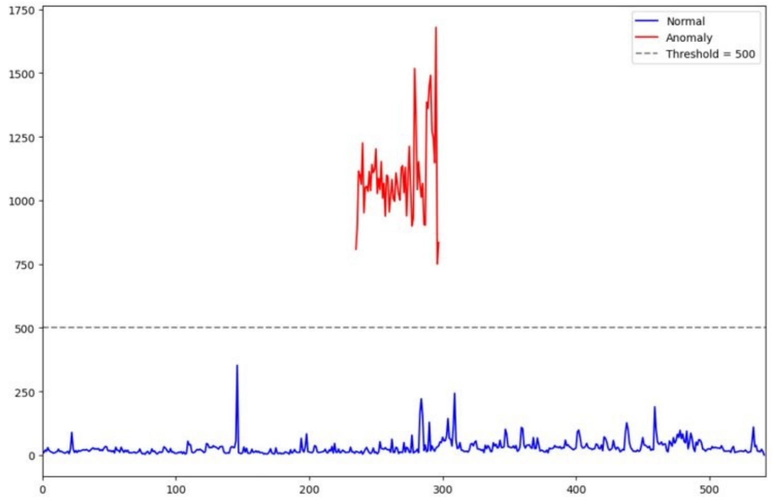


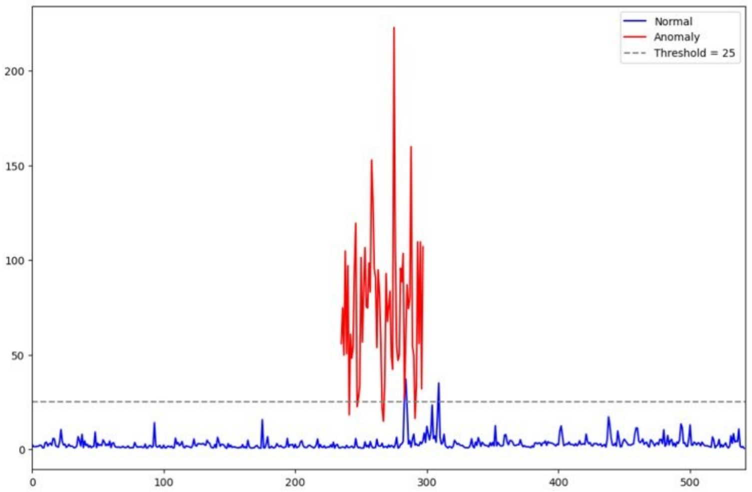
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

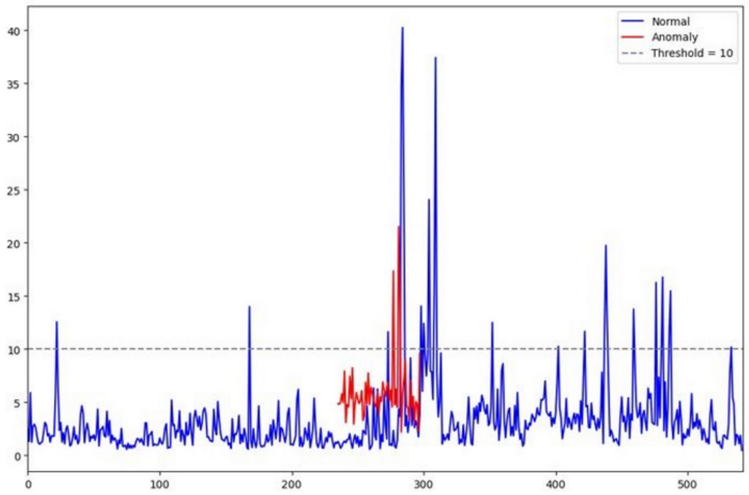
Sequential packet selection with a fixed period between consecutive samples was used in the sampling process.

RESULTS OF MODEL EVALUATION ON THE TEST SET

Sampling frequency (s)	Window size in seconds	Detection accuracy
1	5	100.0%
2	5	100.0%
5	5	100.0%
10	5	100.0%
25	5	99.8%
50	5	87.6%







NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

Thank you for your attention

https://bolanowski.v.prz.edu.pl/
marekb@prz.edu.pl

https://paszkiewicz.v.prz.edu.pl/
andrzejp@prz.edu.pl

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme