EasyChair Preprint

№ 11305

Leveraging SDN for Real World Windfarm Process Automation Architectures

soufiane hamadache, Elhadj Benkhelifa, Hisham kholidy, Pradeeban Kathiravelu and Brij B Gupta

November 16, 2023

Leveraging SDN for Real World Windfarm Process Automation Architectures

Soufiane Hamadache[1] , Elhadj Benkhelifa[2], Hisham Kholidy[3], Pradeeban Kathiravelu[4] and Brij B. Gupta[5]
[1] General Electric. Staffordshire, UK,
[2]Smart Systems, AI and Cybersecurity Research Centre, Staffordshire University, Stoke on Trent, UK
[3]ACRL lab, College of Engineering, State University of New York Polytechnic Institue, USA
[4] University of Alaska Anchorage, Anchorage, AK, 99508, USA
[5]Asia University, Taiwan, Taichung, Taiwan
soufiane.hamadache@ge.com, e.benkhelifa@staffs.ac.uk, kholidh@sunypoly.edu, pkathiravelu@alaska.edu, bbgupta@asia.edu.tw

***Abstract*—SCADA systems are the main part of automated controls and supervision in industrial control systems (ICS). Current SCADA systems are installed in sophisticated, complex architectures involving many third-party sub systems connected to the Internet for remote access/control and system updates. The existing architectures used in windfarms are based on classical switches where everything is enabled by default with plug and play ports, and where the administrator is required to interact with the physical infrastructure to decide what to disable such as unused ports and insecure services (Telnet, http). The classical switches have limited functions and logics. Software-Defined Networking (SDN) is an eminent technology, it decouples the control and data planes, centralizes logically the network devices and abstract the network infrastructure from the application layers. Therefore, it can interact with upstream Application to allow the extending of the functionality of a programmable network by users. Protocol like IEC61850+(60870-5-104) or (60870-5-101) are commonly used in SCADA networks to operate critical infrastructures (CI), such as power plants and substations. It is the protocol used to collect data and operate the wind turbines' interfaces; however, these protocols have never been tested in SDN. Emulation environments, such as Mininet, which is the closest work reported in literature, does not reflect the real world with real devices. Therefore, the aim of this paper is to leverage SDN technology in SCADA architecture for real world Windfarm projects. Two SDN controllers were implemented and compared, namely OpenDaylight and Ryu**

Keywords— SDN, SCADA, OpenDaylight, Ryu, windfarm. Automation

I. Introduction

Classical computer networks can be difficult to manage. Dealing with different distributed topologies using different vendors to connect different switches, routers, and firewalls to maintain them operational and functional is not easy, especially when an update in configuration in one or more devices are required and might affect other devices. It requires time, resources, and testing such as a regression test to make sure the system is still functional as expected. Each router/switch has its control plane and needs to coordinate with other routers/switches to manage the global routing table, and these controls need to be performed in a distributed way because of its architectural limitation.

The routing decisions in legacy switches and routers use the addressing information in each packet. However, in SDN, the packet in the first instance is sent to the controller for processing then returned to the OpenFlow switch with routing table control that is reprocessed by the following packets in the flow. SDN controller has full access and capability to implement and apply network 7 controls and security policies in all data plane switches. Therefore, it can interact with upstream Application to allow the extension of the functionality of a programmable network by users.

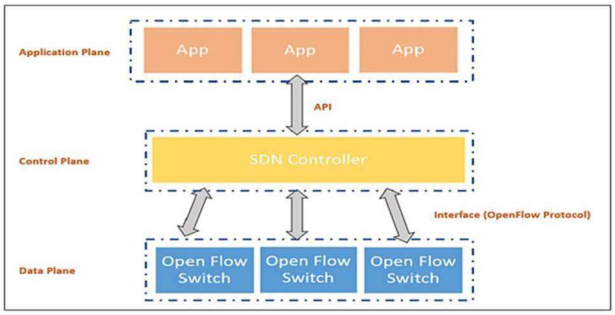

Fig 1. Layers used in SDN architecture [1]

Software defined Network (SDN) decouples the control and data planes, centralize logically the network devices and abstract the network infrastructure from the application layers [2] [3]. Therefore, the network administrators have the flexibility and capability to configure and manage the physical network through a software interfaces.

The protocol used to ensure the communication between the OpenFlow switches and SDN control is Open flow protocol [4]. A secure channel between the controller and switch should be done using either SSL (Secure Sockets Layers) or TLS (Transport Layer Security) followed by exchange of "Hello" messages [1].

SCADA systems required a networking layer underneath to work properly. Researchers have used SDN to improve the network's performance [5] SDN decouples the control and data planes, centralize logically the network devices and abstract the network infrastructure from the application layers [2]. The SDN architecture (Fig 1) and approach facilitate network evolution [6]. The devices send data in flows that are made of many individual packets. SDN is based on protocols such as OpenFlow [7].

The UK government has significantly increased the capacity of the offshore windfarm power plants in the last 10 years where a quarter of the UK's electricity is produced by offshore wind turbines with a plan to grow the size and number of power plants to meet the clean resources plan by
2035 [8]

SCADA systems are used in every wind turbine power plant to control and monitor the power and devices. Different networks and devices with different vendors are connected to transmit and receive data using different protocols. The Generic Object-Oriented Substation Event (GOOSE) uses the approach publisher/subscriber communication between the Intelligent Electronic Devices (IEDs) where the concept is based on publisher to send periodically messages to the subscriber. Failure in sending/receiving the goose between the IEDs on time (<2sec) might trip the wind turbines or generate an audible alarm which triggers the klaxon.

Section 2 presents an overview of related work, Section 3 describes in details the design of the proposed SDN based architecture for real world windfarm automation environment followed by the implementation and functional testing in section 4 and then finally finishes with the conclusions and the potential benefits of SDN for the application.

II. RELATED WORK

Authors of [9] claim in their paper that traditional network devices are not easy to manage especially in complex topologies. Cloud and virtualization solutions might be adopted to fix some of the challenges seen in traditional network. However, these two technologies and solutions require more resources, high availability, and bandwidth. To overcome the legacy network topology restrictions, the SDN technology is used to decouple the control and data plane from the network to provide more agility, scalability, and programmability. An SDN has a complete overview of network topology with ability to configure and manage the network devices through a centralized configurable controller.

The SCADA system is a core component of wind farm process automation. It consists of heterogeneous smart devices, such as intelligent electronic devices (IED), programmable logic controllers (PLC), remote terminal units (RTU), master terminal units (MTU), control servers and security devices.

Research efforts investigating the use of SDN in Smart Grid communication networks are still scarce [10]. To the best of the authors knowledge, the SDN technology has never been tested in windfarm process automation architectures and topologies nor to similar topology which cover the industrial protocols used in the wind farm projects. Furthermore, the protocol IEC-60870-5-104 (IEC-104) is not yet tested in SDN which is commonly used in (SCADA) networks to operate critical infrastructures (CI), such as power plants and substations. It is the protocol used to collect data and operate the wind turbines interfaces.

Moreover, The SDN technology is not yet tested in SCADA systems in a fundamental architecture with fundamental protocols which has the combination of the protocols (Goose or/and IEC61850+(60870-5-104) or (60870-5-101) +NTP) which are the minimum protocols in windfarm process automations to ensure the functionalities of the SCADA system with different IEDs (Intelligence electronic devices) and Wind turbine interfaces. Finally, none of existing works tested the performance of the SCADA HMIs, PLC and time synchronization in SDN architecture in real world environment.

The SDN technology, has been tested in SCADA systems in emulation environments and below is provides a summary of the very limited reported work, which can be related to windfarm architectures and protocols. Authors of [11], have tested SDN in a basis topology using Mininet to create virtual SDN/OpenFlow networks, including virtual hosts, switches, controllers, and links. The protocol MODBUS TCP/IP was used to simulate the packets from the different substation hosts.

Authors of [12] have simulated an SDN topology using Mininet to simulate an IEEE 37-buses smart grid network, a virtual host that runs as DNP3 server and a virtual sensors/actuator that runs DNP3 clients to collect the data from the server through the OpenFlow switches/Controller. Authors of [13] have simulated the SCADA networks of different IEEE test bus systems with both legacy and SDNenabled switches using Mininet. It consists of 26 IEDs, 13 RTUs, and 1 MTU (Master Terminal Units) IN a small network of a 14-bus SCADA system.

There are different SDN Controllers and each controller has its advantages and disadvantages in term of flexibility and rapidity to communicate, and to discover the OpenFlow switches. The Table2. Illustrates an overview of some SDN controllers. In this project, the Ryu and Open Daylight Controllers will be configured and analyzed in our prototype architecture.

Table 1. SDN Controllers overview

Controller	Programming language	Developer	Summary
Open Daylight (Varga and Medved, 2014)	Java	The Linux Foundation	It is very flexible which allows the users to build a customized controller according to their requirements. It implements the OpenFlow protocol
Ryu (Irawati and Hariyani, 2016)	Python	NIT	It provides logically centralized control and application programming interface to allow the innovation of network management and control applications. It works with OpenFlow
POX (Dalal and Bholebawa, 2018)	C++, Python	Niciria	It is a transparent SDN controller which functions with OpenFlow.

III. SDN-BASED ARCHITECTURE

The choice of our prototype architecture is based on fundamental protocols and devices used in windfarm process automation, which include the flowing devices PLC, SCADA Server and Wind Turbine Server, and protocols such as IEC61850 and IEC 104. These devices will be communicating through the OpenFlow Switch/OpenFlow Controller, which will be discussed in details in the next sections. Fig 2. Depicts the proposed prototype architecture, the components of which are described below.

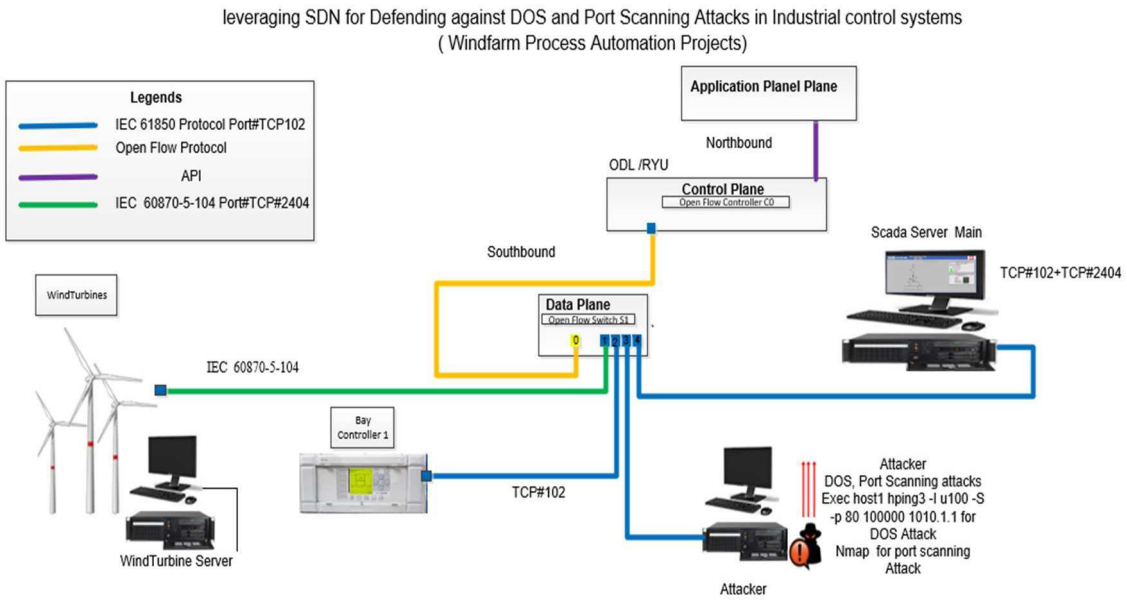

Fig 2. SDN based Arch for wind farm process automation

A. SDN controllers

There are several SDN controllers such as Open Daylight, POX, Ryu, Beacon, and Floodlight. The Ryu controller which means in Japanese the flow is a software-based software defined networking framework that permits users to create applications via an API. It supports many protocols such as OpenFlow and Netconf. Ryu is a python-based controller and includes, Ryu manager, application manager, OpenFlow controller, protocol and libraries.

The Open Daylight controller is a modular open source managed and developed by the Linux foundation. It is a java program; hence, Java needs to be installed on the machine which runs the Open Daylight controller. It is packaged in a karaf container to allow the programmers and developers to put all the software into a unique and single folder [14]. The Open Daylight has desktop GUI Dlux which allows the visualization of the connected devices along with their MAC addresses.

B. OpenFlow Protocol

In 2008, the university of Stanford developed the OpenFlow protocol for research purpose, Several OpenFlow versions are released such as versions 1.0, 1.1, 1.2, 1.3, 1.4 and 1.5.
The Open daylight controller only supports the version 1.0 and 1.3. However, the Ryu controller supports almost all OpenFlow versions (1.0,1.2, 1.3,1.4 and 1.5). In this project the OpenFlow version 1.3 will be used because it is supported by both controllers (ODL/Ryu) to provide the communication with OpenFlow switches and network devices. The Open Networking Foundation creates various standards for implementing SDN in network devices. The OpenFlow switch consists of an OpenFlow channel which represents the interface that allow the controller to configure and manage the OpenFlow switch, flow and group tables to perform the packet lookup and forwarding. Fig 3 depicts OpenFlow switch flowchart.

The main exchanged messages between the controllers and OpenFlow switches to form an OpenFlow channel connection are as follows:

- The “HELLO” message which is used to start and establish the communication between the controller and OpenFlow switches to share the OpenFlow version.

- The “FEATURE_REQUEST” message will be sent by the controller to the OpenFlow switch which has to answer by “FEATURE_REPLY” followed by a unique identified ID.

The match field in OpenFlow switch is based on source/destination MAC or/and IP addresses, logical ports, ingress ports and VLAN. The action Drop/Forward/flood the packets will be selected based on match parameters in the flow table. The default entry
“TABLE_MISS entry” will be selected as last resort with least priority in case of there in no entry match in the flow table.

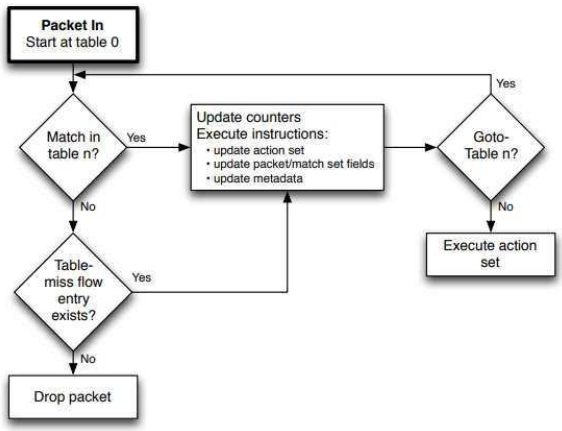

Fig 3. OpenFlow switch flowchart

C. OpenFlow Manager

In this project, the open flow manager app will be used to interact with our Open Daylight controller using the RESTCONF protocol. in the southbound the Open Daylight

controller interact with open flow switches using the open flow protocol. The open flow protocol version used in this project is 1.3. The OpenFlow manager is the application which manages the open flow network. Fig 4 depicts the OFM components.

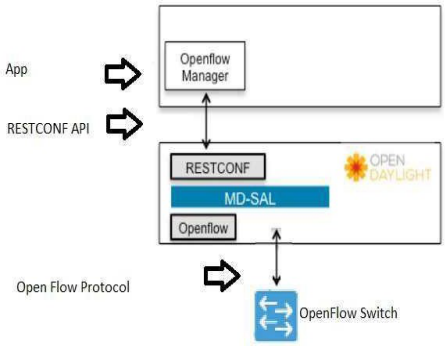

Fig 4. OpenFlow Manager components

D. SCADA HMI Server

SCADA Viewer HMI is runtime server used to visualize the devices (Wind turbine Server, SCADA HMI Server, PLC and Cyber Attacker Machine). It monitors the speed of the turbines as well as the status of the critical signals (Over Current, Temperature, over speed). It operates also the dummy breaker 1 which is used to confirm the bi-directional communication between the SCADA Server and PLC. The driver of the SCADA Viewer HMI supports many protocols such as SNMP, IEC61850 edition1 and edition2, IEC104, NTP, IEC101. etc. which are the most common protocols used in windfarm projects. This dynamic mimic will be monitored during the injection of our focus attacks (Ports scanning and DoS attacks) to check that stability and performances of our SCADA system. The Wireshark is installed in this SCADA HMI machine to collect the traces before and after the attacks. The results will be discussed in the next chapters. The Fig 5 illustrates the overview of the SCADA HMI to monitor our devices.

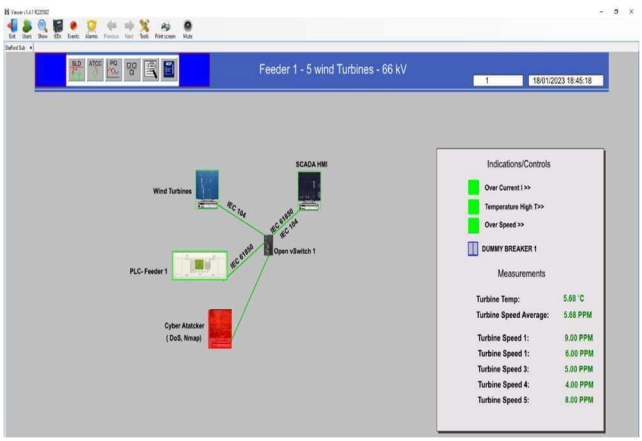

Fig 5. SCADA Viewer HMI

IV. Implementation and Testing

For the implementation of the proposed SDN based architecture for windfarm process automation, the below hardware and software are used to demonstrate a real world environment.

- VMware 16.2.1
- Laptop 1 (Wind Turbine Server) under Windows 11 with 8GB of RAM and 200 GB of free disk space
- Laptop 2 Windows 10 Pro with 32 GB of RAM and 500GB of free disk to install the following guests (VM1: SCADA HMI under windows 10 with 8GB of RAM and 60 GB of free disk, VM2: ODL/Ryu Controllers under Ubuntu 20.04.5 LTS with 8GB and 30 GB of free disk, VM3: Attacker Machine under Ubuntu 20.04.5 LTS with 4GB and 30 GB
- Raspberry PI 3 Model B with 1GB RAM and 32 GB of free disk, it is configured as open vSwitch (OpenFlow Sitch) with 4 USB/Ethernet Ports
- 4-20 ma Injector to inject the analogues into the PLC
- Wireshark to collect and analyses the traces
- Python3

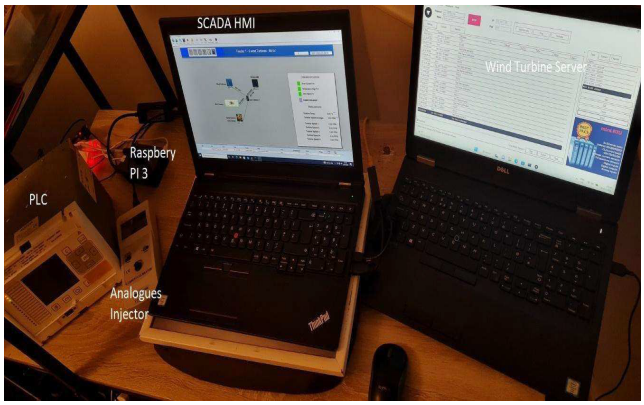

Fig 6. SDN experimentation environment

Fig 6. Depicts the experimentation environment used in this project which includes the PLC, Analogue's injector, Wind Turbine laptop and SCADA HMI VM. The Attacker machine and ODL/Ryu controller are running in the same machine as SCADA HMI in different VM guests.

A. Configuration of Raspberry PI as open vSwitch

In this project the Raspberry PI 3 is used and configured as OpenFlow switch. We have installed the version 2.7.0 which is stable and supported by both Ryu and Open Daylight controllers.

Installation of the OpenFlow switch

```
apt-get update
wget--no-check-certificate
https://www.openvswitch.org/releases/openvswitch-2.7.0.tar.gz
sudo apt-get install python-simplejson python-qt4 libssl-dev python-
twistedconch automake autoconf gcc uml-utilities libtool build-essential
pkg-config sudo su tar -xvf openvswitch-2.7.0.tar.gz cd openvswitch-2.7.0
apt-cache search linux-headers
apt-get install -y linux-headers-4.9.0-6-rpi
./configure --with-linux=/lib/modules/4.9.0-6-
rpi/build make && make install cd datapath/linux
modprobe openvswitch cat /etc/modules echo
"openvswitch" >> /etc/modules
cat /etc/modules
cd ../..
touch /usr/local/etc/ovs-vswitchd.conf mkdir
-p /usr/local/etc/openvswitch
ovsdb-tool create /usr/local/etc/openvswitch/conf.db
vswitchd/vswitch.ovsschema
nano script ovsdb-server --
remote=punix:/usr/local/var/run/openvswitch/db.sock \
        --remote=db:Open_vSwitch,Open_vSwitch,manager_options \
        --private-key=db:Open_vSwitch,SSL,private_key \
        --certificate=db:Open_vSwitch,SSL,certificate \
        --bootstrap-ca-cert=db:Open_vSwitch,SSL,ca_cert \
        --pidfile --detach
ovs-vswitchd --pidfile --detach ovs-vsctl
--no-wait init
ovs-vsctl show Ctrl+o
Ctrl+x
chmod +x script
./script
 ovs-vsctl add-br br0  ovs-vsctl add-port br0 eth0
ovs-vsctl add-port br0 eth1  ovs-vsctl add-port br0
eth2  ovs-vsctl add-port br0 eth3  ovs-vsctl add-
port br0 eth4  ovs-vsctl set-controller br0
tcp:192.168.45.32:6633  ip link set br0 up  ovs-
vsctl set bridge br0 stp_enable=true  ovs-ofctl add-
flow br0 action=normal
```

Four USB to ethernet adapters are plugged to connect the Machine attacker, SCADA HMI Server, Windturbine Server, PLC and SDN Controller (ODL / Ryu). The listening port is 6633 and the IP address of the controller is 192.168.45.32. The command “ovs-vsctl show”, allow the user to display the controller status (connected / disconnected) and IP address along with all port interfaces including the bridge port. This command is useful for troubleshooting to check the status of the controller and ports.

The command “ovs-vsctl list controller”, allow the user to display the controller status (connected/disconnected) and its role (Master/Slave) along with connection time our/last connection/last disconnection. This command is useful for troubleshooting to verify the communication between the OpenFlow switch and OpenFlow controller.

```
root@sw1:/home/pi/openvswitch-2.7.0# ovs-vsctl show
bfa5d45c-09b5-4ad3-87a1-53d14a8d4f5b
    Bridge "br0"
        Controller "tcp:192.168.45.32:6633"
            is_connected: true
        Port "eth1"
            Interface "eth1"
        Port "eth3"
            Interface "eth3"
        Port "br0"
            Interface "br0"
                type: internal
        Port "eth2"
            Interface "eth2"
        Port "eth4"
            Interface "eth4"
        Port "eth0"
            Interface "eth0"
```

OpenFlow Database Configuration

```
root@sw1:/home/pi/openvswitch-2.7.0# ovs-vsctl list controller
_uuid               : 9c8f8e02-53f2-44b4-a459-fcdd77228abe
connection_mode     : []
controller_burst_limit: []
controller_rate_limit: []
enable_async_messages: []
external_ids        : {}
inactivity_probe    : []
is_connected        : true
local_gateway       : []
local_ip            : []
local_netmask       : []
max_backoff         : []
other_config        : {}
role                : master
status              : {last_error="Connection timed out",
sec_since_connect="724", sec_since_disconnect="726", state=ACTIVE}
target              : "tcp:192.168.45.32:6633"
```

OpenFlow Controllers status

B. SDN Controller/Switch

In this part of the project, we have configured the OpenFlow switch to behave as traditional switch by adding this command “ovs-ofctl add-flow br0 action=normal”, thus, all traffics, MAC addresses, IP addresses and protocols are allowed. The below Table 2. Depicts the IP and MAC addresses of our devices (Wind Turbine Server, SCADA HMI, PLC and attacker).

The SCADA HMI is talking to all devices (Wind Turbine, PLC and attacker). Wireshark traces show the communication between the different interfaces along with associated protocols (Ports#2404 for Wind Turbine communication with SCADA HMI on protocol IEC104 and port#102 for the communication between the PLC and HMI on IEC61850 protocol). The ICMP in enabled from/to all devices including the attacker machine. Fig 7 shows the functional SDN based Architecture for wind farm process automation, which demonstrates that the system is operational with an optimal performance through the SDN controller/ switch for our focus protocols (iec61850, iec104...etc)

Table 2. MAC and IP addresses

Machine Name	MAC Address	IP Address
Wind Turbine Server	28 : f1 : 0e : 07 : e4 : 79	192.168.1.200
SCADA HMI Server	18 : db : f2 :52 : f4 : ca	192.168.1.10
PLC Device	80 : b3 : 2a : 00 : 1c : 38	192.168.1.2
Attacker Machine	00 : 0c : 29 : 57 : 5a : 1a	192.168.1.230

loss nor impacting the SCADA system.

Fig 7. IO Graphs for Functional SDN based Architecture for wind farm process automation, where it show how the packet flows captured from the windsurfing server, which are around 17.5 packet/sec, all the packets are forwarded / received without any

V. Conclusions

In this paper, for the first time, we have designed and implemented a centralized software-defined network for Windfarm automation process. Advantages of leveraging SDN for this industrial application can create a mind shift in the relevant industry moving more towards SDN solutions. Some of these advantages are highlighted below including enhanced security, flexibility, and manageability, in addition to performance.

Traditional networks and switches in windfarm automation lack cybersecurity measures, prioritizing productivity over security. They have limited functions and lack support for scripts, logics, and programming languages, making it difficult to detect and prevent sophisticated attacks. SDN controllers can quickly detect and drop abnormal traffic and patterns and can also handle advanced attacks, allowing configuration as layer 2 and layer 3 switches with specified protocols, IP/MAC addresses, and secured ports.

Legacy networks require separate configuration of numerous switches, risking failures. SDN decouples control and data planes, centralizing devices and allowing centralized management with a programmable data plane. OpenDaylight offers user-friendly GUI for administration. Traditional switches lack easy monitoring, while SDN offers real-time visibility and optimization of network performance through centralized control and flow path management. SDN's programmability and decoupling of control and data planes enable the blocking of abnormal network traffic. The Ryu controller with Python applications allows customization for optimized detection and defense against sophisticated attacks. For future work, we will extend the current work with the cybersecurity solutions introduced in [15-89].

References

[1] J. McCauley, P. c.-0.-2. (2008). OpenFlow: enabling innovation in campus networks. SIGCOM. Rev. 38 (2), 69–74.

[2] al, S. S. (2013). Are we ready for SDN? Implementation challenges. EEE Commun, EEE Commun. Mag., vol. 51, no. 7

[3] A. Sallam, A. Refaey and A. Shami, "On the Security of SDN: A Completed Secure and Scalable Framework Using the SoftwareDefined Perimeter," in IEEE Access, vol. 7, pp. 146577-146587, 2019, doi: 10.1109/ACCESS.2019.2939780.

[4] B. Xiong, K. Yang, J. Zhao , W. Li, and K. Li (2016). Performance evaluation of OpenFlow-based software-defined networks based on queueing model. Computer Networks. Volume 102, 19 June 2016, Pages 172-185

[5] C. P. Yoon, (2015). Enabling security functions with SDN: a feasibility study. Comput. Network. IEEE, 85, 19–35. Retrieved from https://doi.org/10.1016/j.comnet.2015.05.005.

[6] E. R. Celyn Birkinshaw, (2019). Celyn Birkinshaw, Elpida Rouka, Vassilios G. Vassilakis, 2019. Implementing an intrusion detection and prevention system using software-defined networking . IEEE.

[7] W. M. Li, W. Meng and L. For Kwok (2016). A survey on OpenFlowbased software defined. Journal of Network and Computer Applications V.68,126–139.

[8] BBC, How many more wind turbines will the UK build? Retrieved frm https://www.bbc.com/news/explainers-60945298

[9] Masoudi, R., Ghaffari, A., 2016. Software defined networks: A survey. Journal of Network and computer Applications 67, 1–25.

[10] Y. Jararweh, M. Al-Ayyoub, A. Bousselham, E. Benkhelifa. 2015. Software Defined based smart grid architecture. 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Morocco.

[11] E. G. da Silva; L. A. Dias Knob; J. A.Wickboldt; L. P. Gaspary; L. Z. Granville and A. Schaeffer-Filho (2015). SDN based has secured the communication flow between devices in SCADA systems.

[12] U. Ghosh, P. Chatterjee, S. Shetty (2017). A Security Framework for SDN-enabled Smart Power Grids. 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)

[13] A H M Jakaria, M. A. Rahman, A. Gokhale (2021). Resiliency-Aware Deployment of SDN in Smart Grid SCADA: A Formal Synthesis Model. IEEE Transactions on Network and Service Management. Volume: 18, Issue: 2, June 2021

[14] A. Eftimie, & E. Borcoci, (2020). SDN controller implementation using OpenDaylight: experiments. 2020 13th International Conference on Communications (COMM2020)

[15] A. A. Khalil, M. A. Rahman and H. A. Kholidy, "FAKEY: Fake Hashed Key Attack on Payment Channel Networks," 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, 2023, pp. 1-9, doi: 10.1109/CNS59707.2023.10288911.

[16] Hisham A. Kholidy, Fabrizio Baiardi, A. Azab, "A Data-Driven Semi-Global Alignment Technique for Masquerade Detection in Stand-Alone and Cloud Computing Systems", is Submitted in ", granted on January 2019, US 20170019419 A1.

[17] Hisham A. Kholidy, “Accelerating Stream Cipher Operations using Single and Grid Systems”, US Patent and Trademark Office (USPTO), April 2012, US 20120089829 A1.

[18] Hisham Kholidy, “Multi-Layer Attack Graph Analysis in the 5G Edge Network Using a Dynamic Hexagonal Fuzzy Method”, Sensors 2022, 22, 9. https://doi.org/10.3390/s22010009. (IF: 3.576).

[19] Hisham Kholidy, “Detecting impersonation attacks in cloud computing environments using a centric user profiling approach”, Future Generation Computer Systems, Volume 117, issue 17, Pages 299-320, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12.009, (IF: 7.307). April 2021, https://www.sciencedirect.com/science/article/pii/S0167739X20330715

[20] Hisham Kholidy, “Autonomous Mitigation of Cyber Risks in Cyber-Physical Systems”, Future Generation Computer Systems, Volume 115, February 2021, Pages 171-187, ISSN 0167-739X, (IF: 7.307) DOI: https://doi.org/10.1016/j.future.2020.09.002 https://www.sciencedirect.com/science/article/pii/S0167739X19320680

[21] Hisham A. Kholidy, “An Intelligent Swarm based Prediction Approach for Predicting Cloud Computing User Resource Needs”, the Computer Communications Journal, Feb 2020 (IF: 5.047). https://authors.elsevier.com/tracking/article/details.do?aid=6085&jid=COMCOM&surname=Kholidy

[22] Hisham A. Kholidy, “Correlation Based Sequence Alignment Models for Detecting Masquerades in Cloud Computing”, IET Information Security Journal, DOI: 10.1049/iet-ifs.2019.0409, Sept. 2019 (IF: 1.51) https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2019.0409

[23] I. Elgarhy, M. M. Badr, M. Mahmoud, M. M. Fouda, M. Alsabaan and Hisham A. Kholidy, "Clustering and Ensemble Based Approach For Securing Electricity Theft Detectors Against Evasion Attacks", in IEEE Access, January 2023, doi: 10.1109/ACCESS.2023.3318111. (IF: 3.55).

[24] Mustafa, F.M., Hisham A. Kholidy, Sayed, A.F. et al. “Backward pumped distributed Raman amplifier: enhanced gain”, Optical Quantum Electron 55, 772 (2023). https://doi.org/10.1007/s11082-023-05066-3 (IF: 3.0).

[25] Alahmadi TJ, Rahman AU, Alkahtani HK, Hisham A. Kholidy “Enhancing Object Detection for VIPs Using YOLOv4_Resnet101 and Text-to-Speech Conversion Model”, Multimodal Technologies and Interaction. 2023; 7(8):77. https://doi.org/10.3390/mti7080077 (IF: 3.17).

[26] Alkhowaiter, M.; Hisham A. Kholidy.; Alyami, M.A.; Alghamdi, A.; Zou, C, “Adversarial-Aware Deep Learning System Based on a Secondary Classical Machine Learning Verification Approach”. Sensors 2023, 23, 6287. https://doi.org/10.3390/s23146287 (IF: 3.9).

[27] Badr, Mahmoud M., Mohamed I. Ibrahem, Hisham A. Kholidy, Mostafa M. Fouda, and Muhammad Ismail. 2023. "Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems" Energies 16, no. 6: 2852. 2023 (IF: 3.25). https://doi.org/10.3390/en16062852

[28] A Jakaria, M. Rahman, M. Asif, A. Khalil, Hisham Kholidy, M. Anderson, S. Drager, "Trajectory Synthesis for a UAV Swarm Based on Resilient Data Collection Objectives," in IEEE Transactions on Network and Service Management, 2022, doi: 10.1109/TNSM.2022.3216804. (IF: 4.75). https://ieeexplore.ieee.org/document/9928375?source=authoralert

[29] Mustafa, F.M., Hisham Kholidy., Sayed, A.F. et al., “Enhanced dispersion reduction using apodized uniform fiber Bragg grating for optical MTDM transmission systems”. Optical and Quantum Electronics 55, 55 (December 2022). https://doi.org/10.1007/s11082-022-04339-7 . (IF: 2.79).

[30] Hisham A. Kholidy, Abdelkarim Erradi, “VHDRA: A Vertical and Horizontal Dataset Reduction Approach for Cyber-Physical Power-Aware Intrusion Detection Systems”, SECURITY AND COMMUNICATION NETWORKS Journal (IF: 1.968), March 7, 2019. vol. 2019, 15 pages. https://doi.org/10.1155/2019/6816943.

[31] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607-016-0495-8, June 2016. (IF: 2.42).

[32] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, “DDSGA: A Data-Driven Semi- Global Alignment Approach for Detecting Masquerade Attacks”, in IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/TDSC.2014.2327966, May 2014. (ISI Impact factor: 6.791).

[33] Hisham A. Kholidy, Hala Hassan, Amany Sarhan, Abdelkarim Erradi, Sherif Abdelwahed, "QoS Optimization for Cloud Service Composition Based on Economic Model", Book Chapter on the Internet of Things. User-Centric IoT, 2015, Volume 150 ISBN : 978- 3-319-19655-8

[34] Atta-ur Rahman, Maqsood Mahmud, Tahir Iqbal, Hisham Kholidy, Linah Saraireh, et al “Network anomaly detection in 5G networks”, The Mathematical Modelling of Engineering Problems journal, April 2022, Volume 9, Issue 2, Pages 397-404. DOI 10.18280/mmep.090213

[35] Hisham A Kholidy., et al. “A Survey Study For the 5G Emerging Technologies", Acta Scientific Computer Sciences 5.4 (2023): 63-70, DOI: 10.13140/RG.2.2.22308.04485.

[36] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. ElHariri, Ahmed M. Youssouf, and Sahar A. Shehata, “A Hierarchical Cloud Intrusion Detection System: Design and Evaluation”, in International Journal on Cloud Computing: Services and Architecture (IJCCSA), November 2012. DOI 10.5121/ijccsa.2012.2601

[37] Hisham A. Kholidy, Alghathbar Khaled s., “Adapting and accelerating the Stream Cipher Algorithm RC4 using Ultra Gridsec and HIMAN and use it to secure HIMAN Data”, Journal of Information Assurance and Security (JIAS), vol. 4 (2009)/ issue 4,pp 274,tot.pag 283, 2009. http://www.mirlabs.org/jias/vol4-issue6.html

[38] Hisham A. Kholidy, “A Smart Network Slicing Provisioning Framework for 5Gbased IoT Networks”, The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.

[39] Hisham A. Kholidy, “Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis”, IEEE International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, May 1-3, 2019. https://ieeexplore.ieee.org/document/8769482.

[40] Hisham A. Kholidy, "A Study for Access Control Flow Analysis With a Proposed Job Analyzer Component based on Stack Inspection Methodology", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 1442-1447, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.

[41] Hisham A. Kholidy, "HIMAN-GP: A Grid Engine Portal for controlling access to HIMAN Grid Middleware with performance evaluation using processes algebra", The 2nd International Conference on Computer Technology and Development ICCTD, pp 163-168, Cairo, 2010.

[42] R. Bohn, A. Battou, B. Choi, R. Chaparadza, S. Song, T. Zhang, T. Choi, Hisham A. Kholidy, M. Park, S. Go, “NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking”, in the IEEE Future Networks World Forum (FNWF), 13–15 November 2023 // Baltimore, MD, USA.

[43] I. Elgarhy, A. El-toukhy, M. Badr, M. Mahmoud, M. Fouda, M. Alsabaan, Hisham A. Kholidy, “Secured Cluster-Based Electricity Theft Detectors Against Blackbox Evasion Attacks”, in the IEEE 21st Consumer Communications & Networking Conference (CCNC), 6-9 January 2024.

[44] M. C. Zouzou, E. Benkhelifa, Hisham A. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 19-22 June 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510.

[45] Hisham A. Kholidy, Andrew Karam, James Sidoran, et al. “Toward Zero Trust Security in 5G Open Architecture Network Slices”, IEEE Military Conference (MILCOM), CA, USA, November 29, 2022. https://edas.info/web/milcom2022/program.html

[46] Hisham A. Kholidy, Andrew Karam, Jeffrey H. Reed, Yusuf Elazzazi, "An Experimental 5G Testbed for Secure Network Slicing Evaluation", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf

[47] Hisham A. Kholidy, Riaad Kamaludeen “An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection”, the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf

[48] Hisham A. Kholidy, Salim Hariri, “Toward an Experimental Federated 6G Testbed: A Federated leaning Approach”, the 19th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2022), Abu Dhabi, UAE December 5th - December 7th, 2022

[49] Hisham Kholidy, Andrew Karam, James L. Sidoran, Mohammad A. Rahman, "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", the 26th IEEE Symposium on Computers and Communications (The 26th IEEE ISCC), Athens, Greece, September 5-8, 2021. https://ieeexplore.ieee.org/document/9631531

[50] N. I. Haque, M. Ashiqur Rahman, D. Chen, Hisham Kholidy, "BIoTA: Control-Aware Attack Analytics for Building Internet of Things," 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (IEEE SECON), 2021, pp. 1-9, doi: 10.1109/SECON52354.2021.9491621.

[51] Samar SH. Haytamy, Hisham A. Kholidy, Fatma A. Omara, “Integrated Cloud Services Dataset”, Springer, Lecture Note in Computer Science, ISBN 978-3-319-94471-5, https://doi.org/10.1007/978-3-319-94472-2. 14th World Congress on Services, 18-30. Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA.

[52] Hisham A. Kholidy, Ali Tekeoglu, Stefano Lannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, “Attacks Detection in SCADA Systems Using an Improved Non- Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), published in February 2018.

[53] Stefano Iannucci, Hisham A. Kholidy Amrita Dhakar Ghimire, Rui Jia, Sherif Abdelwahed, Ioana Banicescu, “A Comparison of Graph-Based Synthetic Data Generators for Benchmarking Next-Generation Intrusion Detection Systems”, IEEE Cluster, Sept 5 2017, Hawaii, USA.

[54] Qian Chen, Hisham A. Kholidy, Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017.

[55] Hisham A. Kholidy, Abdelkarim Erradi, “A Cost-Aware Model for Risk Mitigation in Cloud Computing Systems”, 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[56] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, “Attack Prediction Models for Cloud Intrusion Detection Systems”, in the International Conference on Artificial Intelligence, Modelling and Simulation (AIMS2014), Madrid, Spain, November 2014.

[57] Hisham A. Kholidy, Ahmed M. Yousouf, Abdelkarim Erradi, Hisham A. Ali, Sherif Abdelwahed, "A Finite Context Intrusion Prediction Model for Cloud Systems with a Probabilistic Suffix Tree", in the 8th European Modelling Symposium on Mathematical Modelling and Computer Simulation, Pisa, Italy, October 2014.

[58] Hisham A. Kholidy, A. Erradi, S. Abdelwahed, “Online Risk Assessment and Prediction Models For Autonomic Cloud Intrusion Prevention Systems”, in the “11th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, November 2014.

[59] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, “A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.

[60] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, “A Hierarchical, Autonomous, and Forecasting Cloud IDS”, the 5th Int. Conference on Modeling, Identification and Control (ICMIC2013), Cairo, Aug31-Sept 1-2, 2013.

[61] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, “HA- CIDS: A Hierarchical and Autonomous IDS for Cloud Environments”, Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN) Madrid, Spain, June 2013.

[62] Hisham A. Kholidy, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", the 9th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[63] Hisham A. Kholidy, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[64] Hisham A. Kholidy, Chatterjee N., "Towards Developing an Arabic Word Alignment Annotation Tool with Some Arabic Alignment Guidelines", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 778-783, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.

[65] Hisham A. Kholidy, Khaled S. Algathber, "A New Accelerated RC4 Scheme using "Ultra Gridsec" and "HIMAN", 5th Int. Conference on Information Assurance and Security, Aug 2009, China.

[66] Hisham A Kholidy, A. Azab, S. Deif, "Enhanced ULTRA GRIDSEC: Enhancing High- Performance Symmetric Key Cryptography Schema Using Pure Peer-to-Peer Computational Grid Middleware (HIMAN)", IEEE-ICPCA (the 3rd Int. Conf. on Pervasive Computing and Applications, 06-08 Oct 2008.

[67] A. Azab, Hisham A Kholidy, "An Adaptive Decentralized Scheduling Mechanism for Peer-to-Peer Desktop Grids", International Conference on Computer Engineering & Systems Nov 2008.

[68] Mostafa-Sami M., Safia H D., Hisham A Kholidy, "ULTRAGRIDSEC: Peer-to-Peer Computational Grid Middleware Security Using High-Performance Symmetric Key Cryptography" in IEEE-ITNG (5th Int. Conf. On Information Technology-New Generations), LasVegas, Nevada, USA, 7-9 April 2008.

[69] Mohammed Arshad, Patel Tirth, Hisham Kholidy, “Deception Technology: A Method to Reduce the Attack Exposure Time of a SCADA System”, https://dspace.sunyconnect.suny.edu/handle/1951/70148,

[70] Akshay Bhoite, Diwash Basnet, Hisham Kholidy, “Risk Evaluation for Campus Area Network”, https://dspace.sunyconnect.suny.edu/handle/1951/70162

[71] Malkoc, M., & Kholidy, H. A. (2023). 5G Network Slicing: Analysis of Multiple Machine Learning Classifiers. ArXiv. /abs/2310.01747.

[72] Fathy M. Mustafa, Hisham A. Kholidy, Ahmed F. Sayed et al. Distributed Backward Pumped Raman Amplifier Gain Enhancement: New Approaches, 06 April 2023, available at Research Square [https://doi.org/10.21203/rs.3.rs-2770728/v1]

[73] Grippo, T., & Kholidy, H. A. (2022). Detecting Forged Kerberos Tickets in an Active Directory Environment. arXiv. https://doi.org/10.48550/arXiv.2301.00044

[74] Zielinski, D., & Kholidy, H. A. (2022). An Analysis of Honeypots and their Impact as a Cyber Deception Tactic. arXiv. https://doi.org/10.48550/arXiv.2301.00045

[75] Kholidy, H. A., & Abuzamak, M. (2022). 5G Network Management, Orchestration, and Architecture: A Practical

Study of the MonB5G project. arXiv. https://doi.org/10.48550/arXiv.2212.13747
[76] Abuzamak, M., & Kholidy, H. (2022). UAV Based 5G Network: A Practical Survey Study. arXiv. https://doi.org/10.48550/arXiv.2212.13329
[77] Kholidy, H. A., Rahman, M. A., Karam, A., & Akhtar, Z. (2022). Secure Spectrum and Resource Sharing for 5G Networks using a Blockchain-based Decentralized Trusted Computing Platform. arXiv. https://doi.org/10.48550/arXiv.2201.00484
[78] Kholidy, H. A. (2021). State Compression and Quantitative Assessment Model for Assessing Security Risks in the Oil and Gas Transmission Systems. arXiv. https://doi.org/10.48550/arXiv.2112.14137
[79] Kholidy, H. A. (2021). A Triangular Fuzzy based Multicriteria Decision Making Approach for Assessing Security Risks in 5G Networks. arXiv. https://doi.org/10.48550/arXiv.2112.13072
[80] Haque, N. I., Rahman, M. A., Chen, D., & Kholidy, H. (2021). BIoTA Control-Aware Attack Analytics for Building Internet of Things. arXiv. https://doi.org/10.48550/arXiv.2107.14136
[81] Kholidy, H. A. (2020). Cloud-SCADA Penetrate: Practical Implementation for Hacking Cloud Computing and Critical SCADA Systems. Department of Computer and Network Security, College of Engineering, SUNY Polytechnic Institute. http://hdl.handle.net/20.500.12648/1605
[82] Hisham A. Kholidy, Abdelkader Berrouachedi, Elhadj Benkhelifa and Rakia Jaziri, "Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification", the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.
[83] Soufiane Hamadache, Elhadj Benkhelifa, Hisham kholidy,Pradeeban Kathiravelu, Brij B Gupta, "Leveraging SDN for Real World Windfarm Process Automation Architectures", The 10th International Conference on Software Defined Systems (SDS-2023) San Antonio, Texas , USA. October 23-25.
[84] Adda Boulem, Abdelkader Berrouachedi, Marwane Ayaida, Hisham Kholidy and Elhadj Benkhelifa, "A New Hybrid Cipher based on Prime Numbers Generation Complexity: Application in Securing 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[85] Meriem Chiraz zouzou, mohamed shahawy, Elhadj Benkhelifa and Hisham Kholidy, “SIoTSim: Simulator for Social Internet of Things”, The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.
[86] Hisham A. Kholidy, Keven Disen, Andrew Karam, Elhadj Benkhelifa, Mohammad A. Rahman, Atta-Ur Rahman, Ibrahim Almazyad, Ahmed F. Sayed and Rakia Jaziri, "Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[87] Ibrahim Almazyad, Sicong Shao, Salim Hariri and Hisham Kholidy, “Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis and Evaluation”, the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.
[88] Abdulbast A Abushgra, Hisham A Kholidy, Abdelkader Berrouachedi and Rakia Jaziri, "Innovative Routing Solutions: Centralized Hypercube Routing Among Multiple Clusters in 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[89] Adda Boulem, Cyril De Runz, Hisham Kholidy, Abdelmalek Bengheni, Djahida Taib, Marwane Ayaida, “A New Classification of Target Coverage Models in WSNs, Survey and Algorithms and Future Directions”, The 7th International Conference on Information and Computer Technologies (ICICT 2024), March 15-17, Honolulu, Hawaii.