©2022 Published in 10th International Symposium on Innovative Technologies in Engineering and Science 21-23 October 2022 (ISITES2022 Bursa - Turkey)
https://doi.org/10.33793/acperpro.05.03.5314

Web Based Health Check Application for Water Management Systems via SNMP Protocol

[1]Hilal Yıldız and [2]Musa Balta
[1-2]Faculty of Computer and Information Sciences, Department of Computer Engineering, Sakarya University, Turkey

Abstract:

The purpose of this article is to develop a system that will enable the monitoring of smart water systems over the network. In this study, firstly why this system is needed is explained and then the developed application is explained. As described in chapter I, each network must be monitored by its administrators to detect potential cyber-attacks and faults. In critical infrastructures, this is a mandatory condition. Otherwise, a possible cyber-attack or faults in the network may lead to the suffering of thousands of people. The application developed for these reasons has been designed according to user criteria, taking into account the previous applications, as explained in section II. With the developed application, the Critical Infrastructures National Testbed Center water management network can be monitored using the web-based and SNMP protocol, and possible abnormal situations can be easily detected.

Key words: SNMP, SNMP Health Check, Web

1. Introduction

Systems that enable a part or all the society to access the services they need while fulfilling their vital functions, and the infrastructures that enable these systems to work in the desired way are called critical infrastructures [1-2]. Critical infrastructures must ensure that the service they provide is uninterrupted and secure.

A "Cyber Security Board" was formed in our country in 2012 to ensure cyber security, and the "National Cyber Security Strategy and 2020-2023 Action Plan" was adopted at the first meeting of this committee [3-4]. In the 5th article of the action plan, the critical infrastructures of our country were determined as follows in the first stage within the scope of information security by the Cyber Security Board: Electronic Communication, Water Management, Energy, Banking and Finance, Critical public services, Transportation.

While some of the listed critical infrastructures use general and known information technologies, the other part is monitored or managed by special information systems called Industrial Control Systems (ICS) [5]. Among these critical infrastructures, Water Management is among the most important as it is of vital importance for humanity.

Access to healthy water is one of the fundamental rights for all people. Water plays an important role in protecting life and public health. Countries that are not water-rich have to develop, manage,

use, and protect their water resources in the best way possible. In order to ensure an effective management, the efficiency and scope of infrastructure systems should be increased, and innovative and local conditions compatible technologies should be used. As in the world, new applications related to water management are on the agenda in our country as well. With smart water management, it is aimed to save water, reduce infrastructural problems and monitor water quality [6]. It commonly includes applications such as intelligent management of water, geographic information systems-based water distribution and network management, detection of losses and leaks, drinking water management, wastewater management, asset management, subscriber accrual and collection transactions management.

Considering the economic and process significance of ICS based critical infrastructures, these systems have always been seen as an obvious target by attackers. Today, there are cyber-attacks in which some groups act together, and even states have begun to use them as wars, rather than individual attacks [7]. When these attacks are carried out on critical infrastructures, they can cause irreparable damage to the society. These critical systems and infrastructures, which are of vital importance, must operate and be protected 24/7. It is important to foresee the damage to be caused by a cyber-attack on this critical infrastructure and systems, to make a risk assessment, to identify the weaknesses that may exist on critical infrastructures and the threats that can use them, and to take precautions to prevent them in advance. This situation has led to the necessity of continuous monitoring and monitoring of smart water management systems [8-11].

SNMP (Simple Network Management Protocol) is a protocol developed for monitoring, tracing, and managing network systems. Management and monitoring of network components such as routers, switches, or network cards such as UPS are carried out with various applications based on SNMP protocol. Controlling a large network with dozens of devices is difficult. In fact, it can be said that it is impossible to track each device separately. SNMP Health Check applications, which aim to provide this monitoring easily, can be defined as a monitoring solution based on the SNMP protocol for systems created by network devices [12-16]. Thanks to these applications, the devices in the system can be monitored instantly and the system information desired to be learned (processor usage percentages of the devices, mac addresses and incoming and outgoing byte amounts to their ports, etc.) can be learned.

Today, many applications are developed as web-based due to their ease of use and advantages in the development process. For this reason, system monitoring applications are mostly web-based in order to facilitate the use of the SNMP protocol, to make it understandable and to visualize it more easily.

In this study, thanks to the web-based SNMP Health Check application developed using the SNMP protocol, the Critical infrastructures national test bed central water management network infrastructure established within Sakarya University was visualized in the web environment and instantly monitored. Thanks to the application developed using scrum, one of the agile software development methods, the network structure is embodied in the web environment, so it will be easier to follow up in a shorter time than the real system.

The next sections of the document are organized as follows: All the details of the SNMP Health

Check application developed for smart water management are presented in section II. In the same section, the SNMP protocol and the structure of the network are also discussed in detail. In the last part, the study was concluded and future developments were mentioned.

2. The Developed Web Based Snmp Health Check Application

Snmp Health Check applications are very common for both commercial and personal use. Applications are offered to the user as web-based or console applications. In this section, the web-based Snmp Health Check application developed for the Critical infrastructures national testbed central water management system will be explained.

The application has been developed using Asp.Net MVC software architecture due to its clarity and the possibilities of visualizing the data. In order to use the Snmp protocol in the application, the necessary Snmp settings of the computer on which the application will be run have been made, and the command line tool SNMPWalk has been installed in order to use the protocol. The SnmpSharpNet library is used to learn the device data in the network with the Snmp protocol. The json library was used to bring device data to the appropriate format for use in graphics, and CanvasJS structure was used for graphics.

2.1. Network Infrastructure of the Application

Figure 1. Physical representations of the water management testbed center [2]

The Critical Infrastructures National Testbed Center water management system is given in Figure 1. This system consists of drinking water process Dam/Lake, Treatment, Lift-1, Lift-2 and Storage stations, and wastewater process Elevation-1, Lift-2 and Treatment stations. Many analog or digital I/O units are used for both systems [2].

There are a total of 7 stations separated from each other by the Vlan structure. These stations are divided into two parts: the sources from which the regions receive drinking water and the sources

from which they send wastewater. These are the "drinking water process" and "wastewater process" sections.

The water management system, which is physically modelled in the test bed as it is used in real systems, is also realistically modelled in the SNMP Health Check application, as seen in Figure 2.

The number and variety of devices in the system have led to the gathering of devices that support different Snmp versions. Although the devices support different versions, there are also devices without Snmp support in the system. The lack of Snmp support of a device means that the network activities of that device cannot be monitored.

In Table 1, the types, names and supported Snmp versions of the devices in the system that support Snmp are given. Devices numbered 1-12 are located in the drinking water section, while devices numbered 13-22 are located in the wastewater section.

Table 1. Device To Monitor With SNMP

No	Device Type	Device Name	SNMPv1	SNMPv2	SNMPv3
1	Switch	MOXA (Dam_Treatment)	✓	✓	
2	Switch	MOXA (Ereservoir)	✓	✓	
3	Switch	Scalance_XB208 (Creservoir)	✓	✓	
4	Switch	Scalance_XB208 (Tank)	✓	✓	
5	HMI	Siemens HMI(KP700 Basic)	✓	✓	×
6	HMI	Siemens HMI(KTP700 Basic)	✓	✓	×
7	HMI	Siemens HMI(KTP700 Basic)	✓	✓	×
8	Firewall	Teltonica	✓	✓	
9	Firewall	Fourfaith	✓	✓	
10	PLC	S7_1200 (Promotion1)	✓	×	×
11	PLC	S7_1200 (Promotion2)	✓	×	×
12	PLC	S7_1500 (Treatment)	✓	×	×
13	Switch	Scalance_XB208 (Promotion1)	✓	✓	✓
14	Switch	Scalance_XB208 (Promotion2)	✓	✓	✓
15	Switch	Scalance_XB208 (Treatment)	✓	✓	✓
16	HMI	Siemens HMI(TP700 Basic)	✓	✓	×
17	HMI	Siemens HMI(TP700 Basic)	✓	✓	×
18	Firewall	Siemens Scalance S615	✓	✓	×

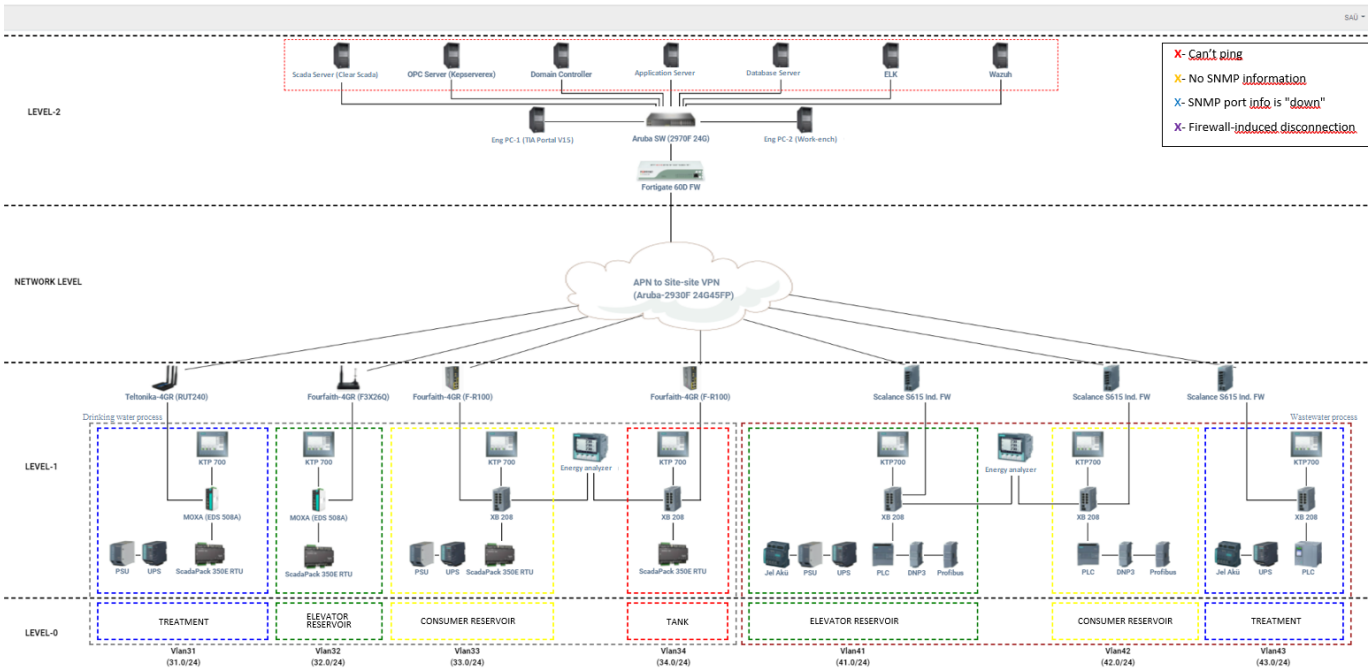

Figure 2. SNMP health check home page

2.2. Working Structure of the Application

The application consists of 3 structures: web structure, database and Snmp protocol. This structure can be explained as learning the information of the devices using the Snmp protocol, recording the information in the database, and then presenting these records to the user with the web-based SNMP Health Check application. This structure is shown in the sequence diagram given in Figure 3.

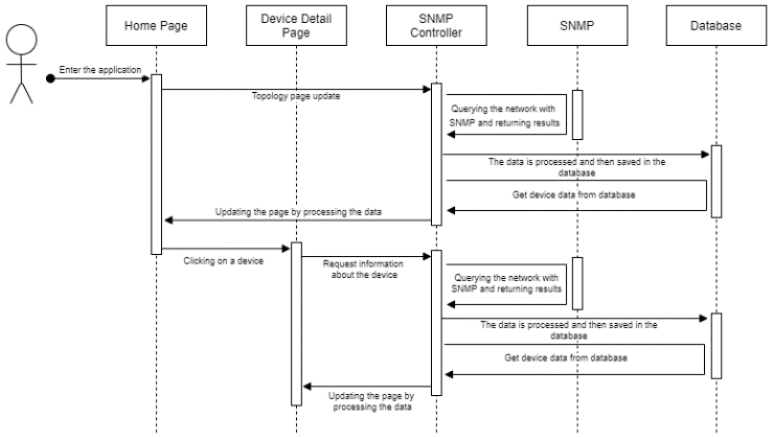

Figure 3. Sequence diagram of developed model

While showing the connection status between the devices on the topology page and displaying the data about the device on the device detail page (Figure 6), the path followed is the same. The

controller structure pulls the network data of the devices using the Snmp protocol. Since this data is not always in the desired format, it may need to be processed. After various checks are made and the data is processed, it is recorded in the database. Then, real-time data is taken from the database and presented to the user in the application.

The IP addresses of the devices on the network are recorded in the database with their device numbers. In this way, the IP addresses of the devices can be easily learned when needed.

The fact that the Snmp versions supported by the devices are different has led to differentiation in the code. Snmp versions supported by the devices are given in Table 1.

With the SnmpSharpNet library used for the Snmp protocol, data can be received from devices that support SNMPv2 and SNMPv3, while data cannot be received from devices that support SNMPv1. This situation caused data to be received from the related devices using only the command line.

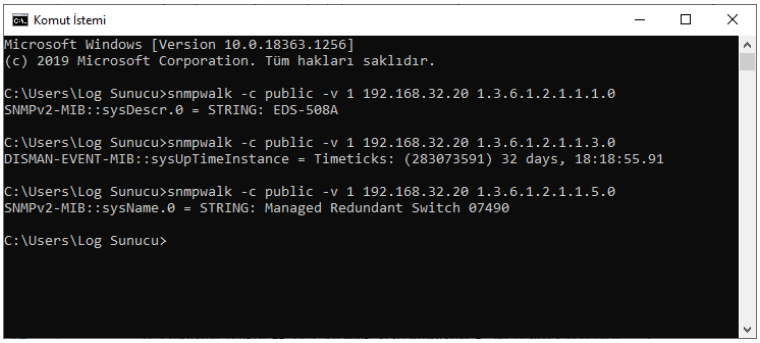

Figure 4. Using SNMPWalk on the command line

SNMPWalk is used to retrieve data from the devices that support SNMPv1 from the command line. An example command line screen is shown in Figure 4. Although the raw data from the command line poses a challenge, this data is processed in the application, made available and saved in the database.

OID values are used to retrieve data from the network with the Snmp protocol. The OID values of the data used in the application are given in Table 2.

Thanks to the recording of the information used in the application in the database, it is also possible to access retrospective information and make various evaluations when requested.

Table 2. OID Values

OID	Information
1.3.6.1.2.1.1.1.0	System Description
1.3.6.1.2.1.1.5.0	System Name
1.3.6.1.2.1.1.3.0	System Updated Time
1.3.6.1.2.1.1.6.0	System Location

1.3.6.1.2.1.1.7.0	System Service
1.3.6.1.2.1.2.2.1.6	Mac Address
1.3.6.1.2.1.2.2.1.8	Status information
1.3.6.1.2.1.2.2.1.9	Last Change
1.3.6.1.2.1.2.2.1.10	Bytes Received
1.3.6.1.2.1.2.2.1.16	Bytes Sent
1.3.6.1.2.1.5.1.0	Received ICMP Packet
1.3.6.1.2.1.5.14.0	Sent ICMP Packet
1.3.6.1.2.1.4.9.0	Received IP Datagram
1.3.6.1.2.1.4.11.0	Sent IP Datagram
1.3.6.1.2.1.6.10.0	Received TCP Segment
1.3.6.1.2.1.6.11.0	Sent TCP Segment

2.3. Application Interfaces

On the homepage, the Critical Infrastructure National Testbed Center water management system is realistically modeled. In this model, besides the names, pictures, station and vlan information of the devices, their connections with each other are also shown (Figure 2).

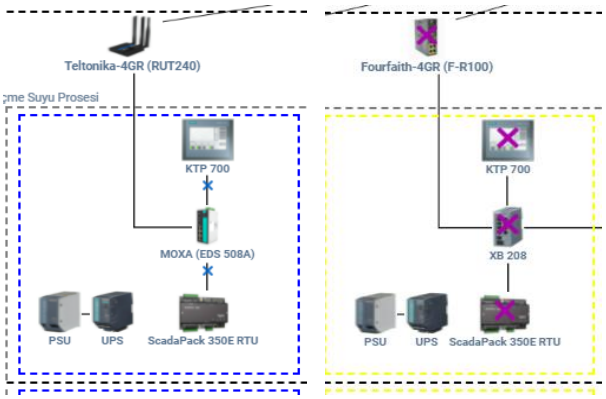

Figure 5. Connection problem examples

The information on which ports the devices are connected to each other is recorded in the database. The system is constantly monitored about the status of these connections and the connection status information is recorded in the database.

A problem in the connection between two devices is expressed by a cross in different colors on the devices (or on the connection line). Example connection problems are given in Figure 5.

The meanings of the signs are as follows:
X - Device not reachable.
X - The device is reachable and supports Snmp, but Snmp information cannot be obtained from the

device at this time.

X - The port connected to the device is not active. The cable may have been disconnected or plugged into the wrong port.

X - Unable to connect to the firewall that connects the related station. Therefore, the devices in that section cannot be accessed either.

The table in the upper right corner of the main page briefly shows the colors and meanings of these signs.

When one of the devices in the topology is clicked on, the device detail page (Figure 6), which contains detailed information about the relevant device, opens.

On the device detail page, 21 different information about the device is displayed. Examples of this information are the system name, the activity status of the device ports, and the incoming and outgoing byte values to the ports. Live graphics are used to better understand and evaluate data such as ICMP packet, IP datagram, TCP segment incoming and outgoing device ports.

The device detail page will be described with the numbers indicated in Figure 6:

- Section 1 contains instant CPU and temperature information of the device. This information is expressed as a percentage and as a donut chart.
- In section 2, there are active or passive status of the ports of the device. With this section, how many ports the device has, and the status of these ports can be examined. If there is a connection problem due to ports, it can be understood by looking at which ports are active/passive from the interface information.
- Section 3 contains system information of the device. These are: system description, system name, system last update, system location and system service information.
- Section 4 contains information about device ports. Each port has the following information: port number, MAC address, status information, last change, incoming-outgoing byte, incoming-outgoing ICMP packet, incoming-outgoing IP datagram, incoming-outgoing TCP segment.
- In section 5, there are live graphics showing the data flow on the device. These are incoming and outgoing ICMP, TCP and IP data from the device. Graphs on the time-byte axes are created using the last 100 recorded records. In this way, the monitoring of the system can be done more effectively by examining the data of the recent past.

The device detail page is updated every 60 seconds. Less update time has made the page more dynamic and real-time. Depending on the need, this period can be increased or decreased.

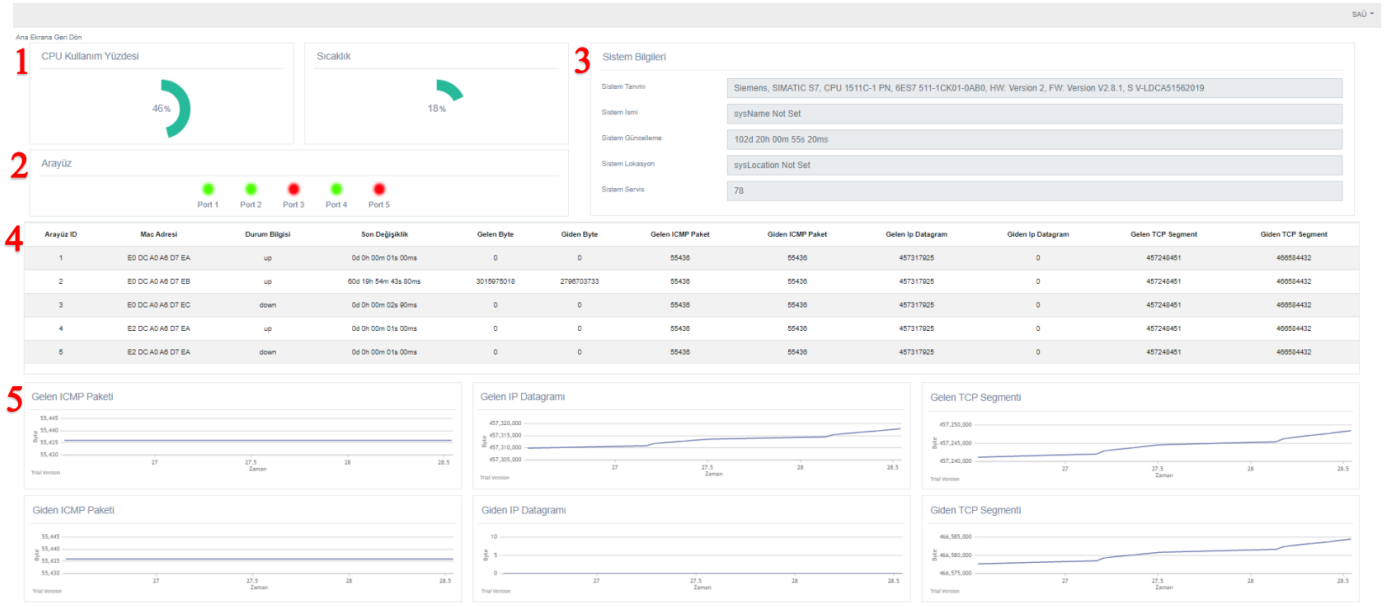

Figure 6. Device detail page

Conclusions And Future Works

In this study, SNMP Health Check software, which is a web-based network monitoring application using Snmp protocol, was developed. It is aimed to increase the usability and make it understandable by developing the application web-based. Developed for smart water management systems, this application can be used not only in this area, but also in almost any system with network devices that support Snmp protocol. The application can be designed according to the information that users want to learn about the network, and then the database can be tailored to the needs.

It is aimed for the application to contain more various Snmp information and to have more visualization elements as a future work. In this context, the problem of controlling the people who can access the system that will emerge was foreseen and a system of login to the application from the user login panel was planned for this. It is estimated that with the realization of this target, the scope of system follow-up will be expanded, and it will allow easier follow-up in this direction.

In addition to these, it is planned to make the application compatible with the criteria of secure software development and to develop it as a dynamic learning system.

References

[1] L. A. Maglaras, K. H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras and T. J. Cruz. "Cyber security of critical infrastructures." Ict Express 4.1 (2018): 42-45.

[2] İ. Özçelik, M. İskefiyeli, M. Balta, K. O. Akpinar and F. S.Toker. "Center water: a secure testbed infrastructure proposal for waste and potable water management." 2021 9th

International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2021.
[3] Ulusal Siber Güvenlik Stratejisi ve Eylem Stratejisi, Ulaştırma ve Altyapı Bakanlığı, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf [Accessed 20 June 2022].
[4] The White House, Office of the Press Secretary, "Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience". Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [Accessed 24 June 2022].
[5] NIST, "Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security", 2015. Available: 10.6028/NIST.SP.800-82r2 [Accessed 26 April 2022].
[6] R. Janke, M. E. Tryby, and R. M. Clark. "Protecting water supply critical infrastructure: An overview." Securing water and wastewater systems (2014): 29-85.
[7] Gondim J., Albuquerque R., Orozco A., "Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols", Future Generation Computer Systems, Vol 108, July 2020, Pages 68-81.
[8] M. A. Brdys. "Integrated monitoring, control and security of Critical Infrastructure Systems." Annual Reviews in Control 38.1 (2014): 47-70.
[9] U. Ani, J. Watson, B. Green, B. Craggs and J. Nurse, "Design Considerations for Building Credible Security Testbeds: Perspectives from Industrial Control System Use Cases", Journal of Cyber Security Technology, pp. 1-49, 2020. Available: 10.1080/23742917.2020.1843822.
[10] Y. Geng, Y. Wang, W. Liu, Q. Wei, K. Liu and H. Wu, "A survey of industrial control system testbeds", IOP Conference Series: Materials Science and Engineering, vol. 569, p. 042030, 2019. Available: 10.1088/1757-899x/569/4/042030 [Accessed 26 April 2021].
[11] A. Almalawi, Z. Tari, I. Khalil and A. Fahad, "SCADAVT-A framework for SCADA security testbed based on virtualization technology", 38th Annual IEEE Conference on Local Computer Networks, 2013. Available: 10.1109/lcn.2013.6761301 [Accessed 6 May 2022].
[12] MPV. Wadal and S. R. Gupta. "An Overview of Network Management System." International Journal Of Computer Science And Applications 6.2 (2013).
[13] D. Mauro, and K. Schmidt. Essential SNMP: Help for System and Network Administrators. " O'Reilly Media, Inc.", 2005.
[14] Boyko A., Varkentin V., Polyakova, "Advantages and Disadvantages of the Data Collection's Method Using SNMP", International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 01-04 Oct 2019.
[15] Almseidin M., Alkasassbeh M., Kovacs S., "Fuzzy Rule Interpolation and SNMP-MIB for Emerging Network Abnormality", Cornell University, Networking and Internet Architecture, 21 Nov 2018.
[16] Naymat G., Kasassbeh M., Hawari E., "Using machine learning methods for detecting network anomalies within SNMP-MIB dataset", Int. J. Wireless and Mobile Computing, Vol. 15, No. 1, 2018.