Comparative Study of RIP, OSPF and EIGRP Protocols to Manage WSN-IoT Traffic vs IPTV Traffic Using Cisco Packet Tracer

José Luis García-Navas, Laura Garcia, Oscar Romero, Jaime Lloret
Instituto de Investigación para la Gestión Integrada de Zonas Costeras
Universitat Politècnica de València
Gandía, Valencia (Spain)
email: jogarna3@teleco.upv.es, laugarg2@teleco.upv.es, oromero@dcom.upv.es, jlloret@dcom.upv.es

Pascal Lorenz
Network and Telecommunication Research Group
University of Haute Alsace
Colmar, France
email: lorenz@ieee.org

***Abstract*— Wireless Sensor Networks (WSN) play a highly important role in current life. WSN implementation is constantly growing because of their wide range of applications, such as agriculture, health care, sport, etc. There is no doubt about the advantages of WSN, but there is a problem derived from the fact that the networks are not designed to managed and prioritize Internet of Things (IoT) and WSN traffic. Regarding to this problem, in this paper, a study of IoT data traffic through a traditional network is carried out using Packet Tracer tool. This research compares and analyzes Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocols performance to manage IoT data traffic coming from two different agriculture WSN deployed in different subnetworks and directed to an IoT server. Moreover, IoT data Traffic is going to be analyzed in three different scenarios, transmitted without any other traffic through the network and two different scenarios with Internet Protocol Television (IPTV) traffic sent across the network. IoT update packets will be captured and Round Trip Time (RTT) data will be obtained and analyzed to compare routing protocols performance.**

Keywords- Wireless Sensor Network; Routing Protocol; RIP; OSPF; EIGRP; IoT traffic; Round Trip Time.

I. INTRODUCTION

WSN include several sensor nodes whose applications are widely different, such as agriculture, health care, sport, energy, traffic management, etc. As WSN can be used for monitoring, different applications through the Internet appears the concept Internet of Things (IoT) [1]. Moreover, WSN are playing a key role in the industry and in academic research. They make possible to offer solutions for a wide range of applications. To achieve the necessities and requirements of WSN and the applications used on them, to provide efficient network architectures and suitable telecommunication standard is mandatory [2].

IoT is an emerging field both for researchers and for end-users who wants to benefit of it. IoT creates a world where all electronic devices are connected between them and communicate to monitor human life parameters in different fields. IoT's goal is to create a better world for humans [3]. IoT technologies can be used for multiple reasons, such as Health Care, i.e., monitoring temperature and heartbeat for tracking patients' health and using wireless devices to communicate data [4], or agriculture that is one of the areas on which IoT is widely implemented. A well, IoT can be useful to monitor different aspects, such as controlling production of fruit-bearing trees using image processing techniques [5].

IoT presents a massive ecosystem involving elements, applications, functions, services, and network traffic management. A possible problem derived from this type of ecosystem is that traditional networks are not designed to transmit IoT information, and IoT traffic management can be a challenge [6]. In fact, one of the main lines of investigation related to IoT traffic is focused on characterizing and classifying IoT traffic. The amount and variety of data will be useful to predict and improve traffic management. To obtain this type of information, it is important to collect and synthesize traffic traces in different scenarios with a diversity of IoT devices and in different periods of time. After collecting, traffic traces can be analyzed characterize statistical attributes and develop a classification method [7].

Regarding to data traffic analysis, Packet Tracer [8] is a virtual networking simulation software developed by Cisco that can be used to learn and understand concepts of networks. Cisco Packet Tracer offers a variety of network components that represent real devices as they look in reality and work the same way. Material offered by Packet Tracer is beneficial to simulate real network and gives the opportunity to interconnect and configure devices to create a network. By the same way, Packet Tracer includes IoT devices and implements IoT functionalities, such as smart devices, sensors, actuators, etc. Because of that, it is considered as a useful researching tool in the design and modernization of networks and in the educational process for the study of networks [8].

This paper presents a study of IoT data traffic through a traditional network. Two different WSNs are deployed in different subnets of the network. WSNs are composed of microcontrollers that monitors environmental parameters, such as temperature and humidity and send this information

 ISBN: 978-1-61208-900-3

to an IoT server located in another subnet. IoT data are analyzed through the network and compared using different routing protocol, such as RIP, OSPF and EIGRP. These protocols have been selected for being the most used in traditional networks, they are easy to implement and to be computed. Moreover, IoT data are analyzed in a clear scenario referring to traffic as well as in a scenario on which IPTV traffic is managed by the network.

The remainder of this paper is organized as follows. Section II presents some related work. The network structure and design carried out in this paper is detailed in Section III. Section IV describes how the simulation has been performed in this research. Simulation and results are summarized in Section V. Finally, Section VI describes conclusions obtained and future work.

II. Related Work

This section presents different works related with WSN, IoT traffic analysis and the network simulation tool Packet Tracer.

García-Navas et al., [9] presented a practical study that shows an IoT prototype for WSN to measure soil moisture and compare it with a commercial soil moisture sensor. Rocher et al. [10] proposed a WSN solution based on ESP32 board program with Arduino IDE and Wi-Fi technology to control sewerage. The system controls if it is raining or not and controls different scenarios inside the pipelines. Elkin et al. [11] discussed existing methods and algorithms for automated management of traffic flows, with the purpose of applying the Internet of Things technology to the organization of road infrastructure for the dynamic management of traffic flows. Their results showed that IoT technologies significantly reduce the waiting time for cars in the queue at intersections, the total travel time, save fuel, reduce harmful emissions into the atmosphere, reduce the travel time of emergency vehicles to their destination, solve the parking problem and still show many other positive effects.

Some other authors have based their investigations on data traffic analysis, such as Hamid et al. [12] who presented a survey of emerging trends of network traffic classification in IoT and the utilization of traffic classification in its applications. The paper compared the legacy of traffic classification methods and presented an overview of traditional models. Moreover, it included a taxonomy of the current network traffic classification within the IoT context. In their paper, they tried to expose different issues raised in IoT that have been addressed with traffic classification. They concluded that traffic classification in the IoT domain is more challenging in comparison with non-IoT domain, because of the high heterogeneity in the IoT domain. Finally, they highlighted current challenges and possible future direction in IoT traffic network traffic classification. Charyyev et al. [13] demonstrated that an external observer passively sniffing the network traffic can infer IoT device activities, after classifying device events. They evaluated and compared ten machine learning algorithms to classify IoT device events, analyze the impact of different interaction modes with devices, on the performance of classifiers, determine the influence of Local Area Networks (LAN) vs Wide Area Networks (WAN) interaction with the device, and ascertain the effect of region from which the device is connected.

Packet Tracer as a simulation tool can be used to analyze and predict network performance. Teshabaev et al. [14] analyzed, studied, simulated, and modelled a multiservice network on Packet Tracer, to determine the value of delays to increasing value size of Internet Control Message Protocol (ICMP) packet using OSPF protocol. They concluded that the longer the ping length, the more information passes per unit of time. Finally, they considered their research useful in the design and modernization of networks and in the educational process for the development and use of the Packet Tracer program for the study of path of various networks. Dumitrache et al. [15] focused their study on the comparative analysis of the routing protocols RIPv2, OSPF and EIGRP using the soft Cisco Packet Tracer. Their study is an example on how Packet Tracer can be used to analyze network performance and compare routing protocols. Packet Tracer allows designing and simulating virtual networks and strengthen the network security.

As well as Packet Tracer can be used to analyze network traffic performance, thanks to the last Packet Tracer software versions IoT devices and IoT traffic can be analyzed. Ashok et al. in [16] worked with the basic idea that cisco packet tracer can be used to implement smart home. Cisco Packet Tracer offers a variety of network components that represent a real network and gives the opportunity to interconnect and configure devices to create a network. Moreover, it implements IoT functionalities (smart devices, sensors, actuators, etc.). Authors used the latest cisco packet tracer version to introduce smart home, using the home portal for home automation and record smart devices for monitoring them and Microcontroller (MCU-PT) to connect various sensors as well as Internet of Everything (IoE) devices. Gwangwava et al. main objective in [17] was to advance research in the development and implementation of IoT systems. The article bridges the gap on IoT development and deployment. It lays out a quick rollout strategy by using a digital platform that has inbuilt IoT objects and programming capabilities. The article reviewed literature on IoT at different levels and it is a case study of a fertilizer manufacturing plant. Their simulation was only focused on monitoring saturated steam temperature, converter head temperature, and neutralization temperature respectively. Finally, they explain that the model can be extended including key process parameters and adding more levels to the network.

Regarding the related work shown above, it is noted that IoT and WSN are two highly studied topics due to their possible applications and their importance in the modern lifestyle. Furthermore, the analysis of network performance has been studied since the beginning of the use of networks. But it is not so common the study of the network performance managing IoT-WSN traffic. Because of that fact in this paper, we decided to analyze how the most used traditional network's Routing Protocols (RIP, OSPF and EIGRP) manage to exchange IoT packets and how IoT data traffic vary depending on the routing protocol. To carry out this study we decided to use Packet Tracer tool to simulate the network performance.

III. NETWORK DESIGN

The aim of this paper is to analyze how IoT data traffic properties vary depending on the routing protocol used and the type of traffic that the network is managing. The scenario to be analyzed consists of a network divided on 4 subnets, two of them will be WSN and one of them will have an IoT server and an IPTV server. The Core Network will consist of several routers organized to allow multipath between subnets. To create a good scenario to carry out this analysis, some designing criteria have been stablished.

A. *Designing criteria*

In this section, the criteria to design the network analyzed in this paper is defined:

- The network will have two different WSN.
- Each WSN will consist of MCU (microcontroller) boards with one humidity sensor and one temperature sensor.
- All MCU boards of each WSN will be connected to a Gateway, through which sensor data will be sent.
- Apart from the two WSN, the network will have one subnetwork containing one IoT server and one IPTV server, and another subnetwork containing some computers.
- The Core Network will consist of various routers interconnected allowing multiple paths between subnetworks.
- Each subnetwork will have a Dynamic Host Configuration Protocol (DHCP) server to automatically assign IP address.

Figure 1 shows the network designed in Packet Tracer. The network consists of 4 subnetworks interconnected by a Core Network that allows multipath between the WSN and servers.

B. *Network Performance*

Every microcontroller will be programmed to read temperature and humidity data from sensors and to send it to the IoT Server every second. MCUs will connect to the IoT server using an admin account, which can be used as well to remotely control sensors data.

Once the network is totally operational and MCUs are connected to Gateways, paths between MCUs and IoT Server are created and MCUs stablish connection with the server. MCUs are programmed to connect both to their Gateway and to the IoT server. Gateways are configured to accept connections by password. Finally, the IoT server is configured to accept connections by creating accounts. As soon as the MCU is connected it starts to send information to the server. Information sent to the Server is updated every time a packet is received, so the server shows Real-Time temperature and humidity measured for each MCU.

C. *Routing protocols*

The main objective of the paper is to analyze IoT traffic management in different network scenarios. For that reasons, three different scenarios have been defined. Each scenario differs from the rest on the routing protocol used on the routers on the network. RIP, OSPF and EIGRP are the routing protocols selected to analyze how the IoT traffic management can vary.

IV. SIMULATION DESIGN

The simulation carried out in this paper is focused on obtaining data about IoT traffic on traditional networks. IoT traffic can be considered critical depending on his use and applications, because of that, it is important how this traffic is managed by the network and how different situations can affect to IoT Traffic.

The data that is going to be captured is time since every MCU update sensor data until it receives an ACK message, that means RTT of update packets. This data is going to be captured in three different scenarios, using RIP, OSPF and EIGRP. After analyzing IoT traffic in scenarios on which no more information is exchanged through the network, this data is going to be captured when IPTV traffic is exchanged through the network.

This simulation is carried out to analyze how routing protocols and traffic flows with high quality of service requirements, such as IPTV, can affect IoT traffic management.

Regarding to the type of packets exchanged during the simulation, apart from the ones needed to update RIP, OSPF and EIGRP routing protocol tables, packets exchanged are IoT packets, Transmission Control Protocol (TCP) IoT packets, TCP packets and IPTV packets.

- IoT packets transmit sensor data from temperature and humidity sensor to the MCU microcontrollers.
- TCP IoT packets transmit temperature and humidity sensors data updates from the MCU microcontrollers to the IoT Server.
- TCP packets transmit ACK packets from IoT server to MCU microcontrollers, to inform that the server has received the TCP IoT packet.
- IPTV packets are packets generated by a server using the Traffic Generator tool provided by Packet Tracer. The IPTV service that is going to be used is High-Definition Television (HDTV) with a bit rate of 8 Mb/s.

For each one of the three scenarios proposed, RTT information of IoT traffic is going to be captured in three different data flows situations. First, IoT traffic is captured without any other flows through the network. Secondly, IoT traffic is captured whereas IPTV traffic is sent from the IPTV server to one PC on subnetwork on which no WSN is configured. Finally, IoT traffic is captured whereas three different IPTV flows are sent by the IPTV server, one for each subnetwork.

All data will be captured and analyzed to obtain every significant information that can be used in future work to improve IoT traffic management.

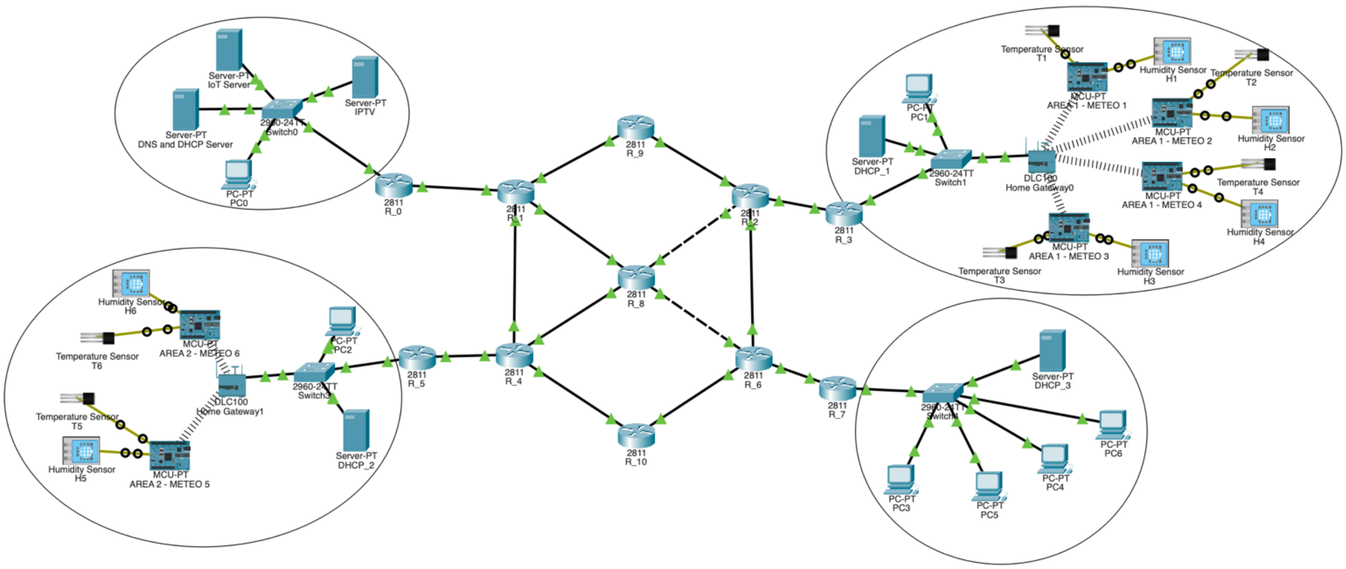

Figure 1. Network designed in Packet Tracer to analyze IoT traffic management

V. Simulation and Results

In this section, simulation results obtained by the research carried out are shown and analyzed. Routing protocols performance is compared on three different situations which vary on the type and amount of traffic managed by the network.

Two different WSN have been designed and simulated so it is important to bear it in mind whereas analyzing data. The two different WSN are identified by Area 1 and Area 2, and MCU microcontroller are identified by Meteo X. Each data shown and analyzed in this paper is the mean of 5 different data measures. The network designed on packet tracer has been studied using packet tracer simulation mode, and 5 consecutive RTT IoT packets have been captured for each one of the six MCU microcontrollers.

Figure 2 shows RTT data of IoT traffic on A Situation on which no other traffic is managed by the network. As it is shown, the three routing protocols perform in similar ways, but EIGRP seems to be lower than RIP and OSPF. These other two protocols show similar results comparing theirs results between them.

Figure 3 shows RTT data of IoT traffic on B Situation on which IPTV traffic is sent from the IPTV server to one PC on subnetwork on which no WSN is configured. Comparing Figure 2 and Figure 3 results, RIP protocol shows worst results when IPTV traffic is managed by the network, whereas OSPF and EIGRP routing protocols perform in the same way in both situations.

Finally, Figure 4 shows RTT data of IoT traffic on C Situation on which three different IPTV flows are sent by the IPTV server, one for each subnetwork. While the variation on RTT between situation A and B is very soft and, in some cases, RTT decreases when IPTV traffic is managed, on situation C RTT shows a high increase. Moreover, it seems to be that EIGRP is the one that performs better than the others when high amount of IPTV traffic is managed by the network.

Furthermore, protocols can be compared by analyzing them individually studying the three different situations (A, B, C) for each routing protocol. Table 1 shows the RTT data measured on A Situation, considered as a base situation, and the increase or decrease experienced by the RTT on B situation ($\triangle 1$) and C situation ($\triangle 2$). As can be seen, RIP protocol performs better when there is no other traffic, but if there is other type of traffic, IoT traffic suffers higher delays. OSPF and EIGRP routing protocols performs better on situations on which there is more traffic through the network. EIGRP is the best one to transmit IoT data traffic when IPTV traffic is managed by the network.

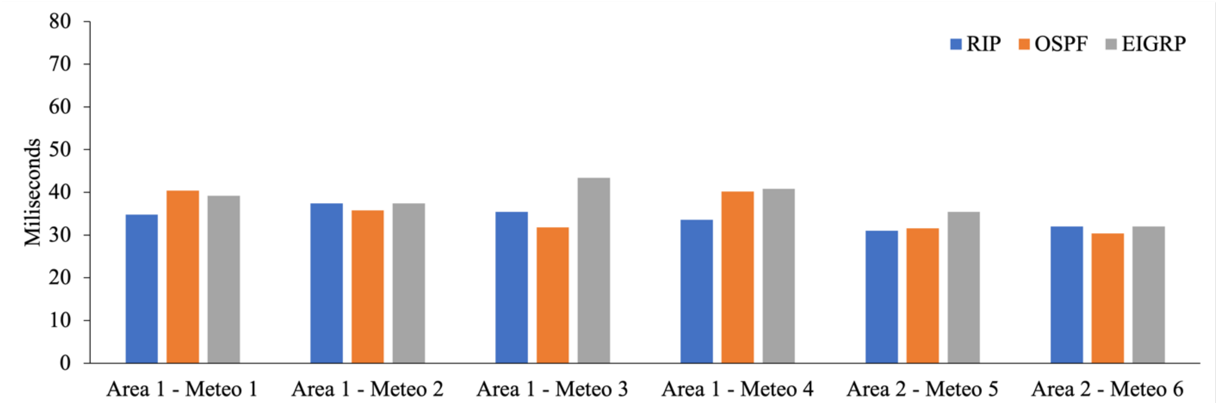

Figure 2. RTT data of only IoT Traffic

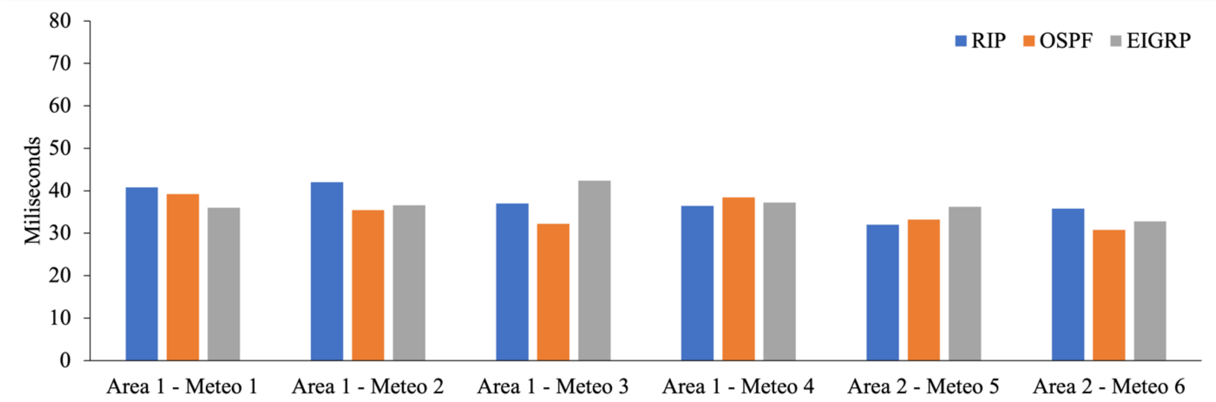

Figure 3. RTT data of IoT Traffic whereas IPTV traffic is sent to network 3 (network without WSN)

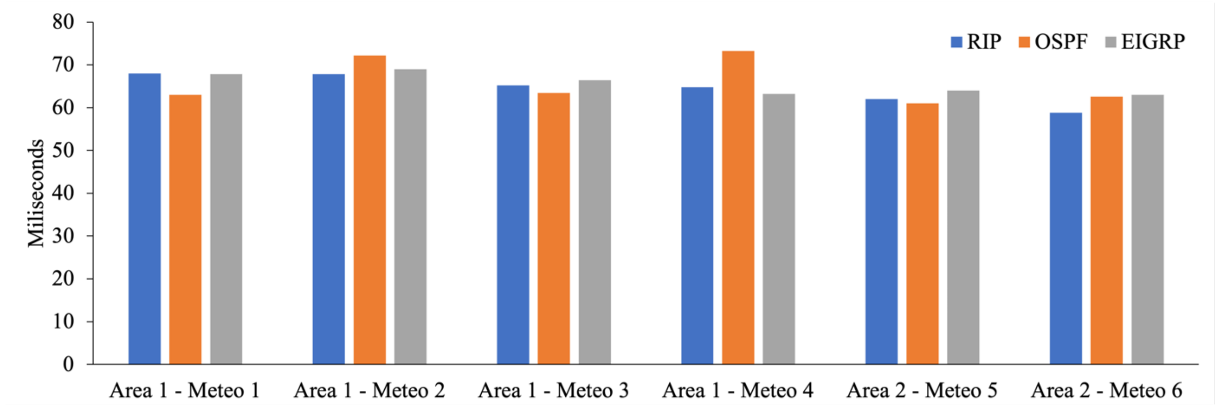

Figure 4. RTT data of IoT Traffic whereas IPTV traffic is sent to the three subnetworks

TABLE I. COMPARISON BETWEEN RTT IOT TRAFFIC WITHOUT ANY OTHER TRAFFIC AND WITH IPTV TRAFFIC

	RIP			OSPF			EIGRP		
	RTT IoT Traffic	*Δ1*	*Δ2*	*RTT IoT Traffic*	*Δ1*	*Δ2*	*RTT IoT Traffic*	*Δ1*	*Δ2*
Area 1 - Meteo 1	34.80	6.00	33.20	40.40	-1.20	22.60	39.20	-3.20	28.60
Area 1 - Meteo 2	37.40	4.60	30.40	35.80	-0.40	36.40	37.40	-0.80	31.60
Area 1 - Meteo 3	35.40	1.60	29.80	31.80	0.40	31.60	43.40	-1.00	23.00
Area 1 - Meteo 4	33.60	2.80	31.20	40.20	-1.80	33.00	40.80	-3.60	22.40

	RIP			OSPF			EIGRP		
	RTT IoT Traffic	*Δ1*	*Δ2*	*RTT IoT Traffic*	*Δ1*	*Δ2*	*RTT IoT Traffic*	*Δ1*	*Δ2*
Area 2 - Meteo 5	31.00	1.00	31.00	31.60	1.60	29.40	35.40	0.80	28.60
Area 2 - Meteo 6	32.00	3.80	26.80	30.40	0.40	32.30	32.00	0.80	31.00

VI. CONCLUSION

In this paper, a study of how routing protocols (RIP, OSPF and EIGRP) and IPTV traffic can affect to WSN-IoT data traffic have been carried out using Packet Tracer. The routing protocols performance to manage IoT traffic has been studied through a network consisting of 4 subnetworks, on which two of them are WSN. Each one of the routing protocols has been tested on three different situations depending on how much IPTV traffic is managed by the network. In conclusion RIP routing protocol is the one that best manages IoT traffic when no IPTV traffic is needed to be sent. OSPF performs well in similar conditions whereas EIGRP is the worst. On the other hand, when IPVT traffic is managed by the network, EIGRP is the better option while RIP is worst. Finally, OSPF can be considered as a neutral option between RIP and EIGRP on managing WSN-IoT traffic vs IPTV traffic.

In future works, another comparative study can be carried out using different types of traffic instead of IPTV traffic. In addition, this type of study can be implemented in real scenarios so real devices can be tested. Moreover, this type of research can help to create data bases of different types of traffic, to classify and prioritize.

REFERENCES

[1] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-WSN: Software-Defined WSN Management System for IoT Applications," IEEE Systems Journal, vol. 12, no. 3, pp. 2074-2081, Sept. 2018.

[2] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, "A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities," IEEE Wireless Communications, vol. 21, no. 4, pp. 113-119, August. 2014.

[3] S. G. H. Soumyalatha, “Study of IoT: understanding IoT architecture, applications, issues and challenges,” In 1st International Conference on Innovations in Computing & Net-working (ICICN 16), CSE, RRCE. International Journal of Advanced Networking & Applications, May. 2016, No. 478, pp. 477-482

[4] D. S. R. Krishnan, S. C. Gupta, and T. Choudhury, "An IoT based Patient Health Monitoring System," 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2018, pp. 01-07.

[5] L. Garcia, et al., “Quantifying the production of fruit-bearing trees using image processing techniques,” Proc. The Eighth International Conference on Communications, Computation, Networks and Technologies, IARIA, (INNOV 2019), Nov. 2019, pp. 14-19.

[6] B. K. J. Al-Shammari, N. Al-Aboody, and H. S. Al-Raweshidy, "IoT Traffic Management and Integration in the QoS Supported Network," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 352-370, Feb. 2018.

[7] A. Sivanathan et al., "Characterizing and classifying IoT traffic in smart cities and campuses," 2017 IEEE Conference on Computer Communications Workshops, IEEE (INFOCOM WKSHPS), 2017, pp. 559-564.

[8] S. R. Javid, “Role of packet tracer in learning computer networks,” International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, no. 5, pp. 6508-6511, May. 2014.

[9] J.L. García-Navas, et al., “Practical Study of the Temperature Effect in SoilMoistureMeasurements,” Proc. The Eighth International Conference on Communications, Computation, Networks and Technologies, IARIA, (INNOV 2019), Nov. 2019, pp. 7-13.

[10] J. Rocher, J.L. García-Navas, O. Romero, and J. Lloret, “A WSN-based Monitoring System to Control Sewerage,” 2019 Sixth International Conference on Internet of Things: Systems, Management and Security, IEEE (IOTSMS 2019), Oct. 2019, pp. 277-282.

[11] D. Elkin, and V. Vyatkin, “IoT in Traffic Management: Review of Existing Methods of Road Traffic Regulation” In Applied Informatics and Cybernetics in Intelligent Systems. Proc. 9th Computer Science On-line Conference. (CSOC 2020) 2020, Vol. 3, pp 536-551.

[12] H. Tahaei, F. Afifi, A. Asemi, F. Zaki, and N. B. Anuar, "The rise of traffic classification in IoT networks: A survey," Journal of Network and Computer Applications, Vol. 154, Article. 102538, pp. 1-20, March. 2020.

[13] B. Charyyev, and M. H. Gunes, "IoT Event Classification Based on Network Traffic," 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 854-859.

[14] T. Z. Teshabaev, M. Z. Yakubova, and O. A. Manankova, "Analysis, research and simulation of a multiservice network based on the Packet Tracer software package to determine the value of delays to increasing value size of ICMP packet," 2020 International Conference on Information Science and Communications Technologies (ICISCT 2020), 2020, pp. 1-4.

[15] C. G. Dumitrache, G. Predusca, L. D. Circiumarescu, N. Angelescu, and D. C. Puchianu, "Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer," 2017 5th International Symposium on Electrical and Electronics Engineering (ISEEE), 2017, pp. 1-6.

[16] G. Ashok, P. Akram, M. Neelima, J. Nagasaikumar, and A. Vamshi, “Implementation of smart home by using Packet Tracer,” International Journal of Scienfic & Technoloy Research, Vol. 9, no. 2, pp. 678-685, 2020.

[17] N. Gwangwava, and T. Mubvirwi, “Design and Simulation of IoT Systems Using the Cisco Packet Tracer,” Advances in Internet of Things, Vol. 11, no. 2, pp. 59-76, 2021.