International Journal of Artificial Intelligence and Machine Learning
Volume 11 • Issue 2

Power Consumption Prediction of IoT Application Protocols Based on Linear Regression

Sidna Jeddou, Department of Communication Systems, National Institute of Posts and Telecommunications, Rabat, Morocco
Amine Baina, Department of Communication Systems, National Institute of Posts and Telecommunications, Rabat, Morocco
Najid Abdallah, Department of Communication Systems, National Institute of Posts and Telecommunications, Rabat, Morocco
Hassan El Alami, Department of Communication Systems, National Institute of Posts and Telecommunications, Rabat, Morocco

ABSTRACT

The advent of the internet of things (IoT) augurs new cutting-edge applications in modern life such as smart cities and smart grids. These applications require protocols more efficient for ensuring the reliability of data communications in the IoT networks. Many works state that IoT cannot meet their demands without application protocols with artificial intelligence (AI) as IoT is expected to generate unprecedented traffic giving IoT researchers access to data that can help in studying and analyzing the demands and also develop application protocols conceptions to meet the requirement of IoT applications. In literature, several works introduced AI in some layers of the TCP/IP model including wireless communication and routing. In this article, an evaluation of application protocols HTTP, MQTT, DDS, XMPP, AMQP, and CoAP has been presented, and subsequently, the power consumption prediction of MQTT and COAP based on the linear regression model is analyzed in order to enhance data communications in IoT applications.

KEYWORDS

AMQP and CoAP, Artificial Intelligence, DDS, HTTP, IoT, MQTT, Power Consumption, Quality of Service, Security, XMPP

INTRODUCTION

Since the last three decades, there has been a lot of development and use that has taken place on the Internet for effective communication. Today, these communications have continued to connect various Internet devices, which are seen as the Internet of Things (IoT), which is the most popular technology that includes Machine to Machine Connectivity (M2M). This M2M communication device includes sensors, RFID, Wi-Fi, data networks, activators, LTE, WLAN etc. These devices process themselves and exchange information without human input that enabled the world of computer networking for greater accuracy and efficiency (Anusha et al., 2017).

Therefore choosing an appropriate protocol is a very hard task, in choosing the right law, first, we need to understand the requirements of the IoT system messages (Jaikar & Iyer, 2018).

DOI: 10.4018/IJAIML.287585

Choosing a standard and efficient data protocol is a challenging and daunting task for any organization (Naik, 2017).

Unlike the Web, which uses a single HTTP protocol, IoT cannot rely on a single protocol for all its needs (Jaikar & Iyer, 2018). Therefore, many data protocols are convenient to select for various types of needs of the IoT system. Some of them are designed to handle applications that require fast and reliable business transactions such as AMQP and JMS(Cohn, 2012). Many of them are developed to deal with applications that need data collection on a compressed network as well as MQTT and CoAP (Bandyopadhyay, 2013). Most of them are created to control request that necessitates instant messaging (IM) and online presence detection like XMPP and SIP. A few of them are produced to hold web applications that demand Internet connectivity like the restful client/server protocol HTTP and CoAP (Naik, 2017). This indicates that the future of IoT is in several data protocols and any single process will not work with all possible IoT cases. In addition, Communication protocols are very decisive to assemble data and determine how IoT interaction is done(Çorak et al., 2018).

On the other hand, power consumption is a crucial point in the choice of these protocols, and it differs according to this important characteristic. Indeed, the efficient prediction of power consumption becomes more appropriate and accurate. Among the most methods that are used in the prediction and analysis of power consumption is a Linear Regression model (Bianco et al., 2013)(Safa et al., 2015)(Dudic et al., 2020).

As a result, it is necessary to investigate the benefits of these protocols to find their exact fit. Therefore, this article presents an assessment of established IoT applications protocols HTTP, MQTT, DDS, XMPP, AMQP, CoAP, and the power consumption prediction of the MQTT and COAP protocols based on a linear regression model. First, it defines the terms of communication and identifies comparisons between these protocols to present their attributes in comparison. Afterward, it performs analysis and experiments based on other features to gain an understanding of their strengths and limitations especially in terms of energy consumption prediction. Therefore, based on this detailed evaluation, the user can determine their appropriate use for various IoT applications depending on their needs, efficiency, and suitability.

The remainder of this article is organized as follows: Section 2 presents an overview. Section 3 demonstrates a comparison of these protocols for providing their general information and analysis of data protocols for revealing their relative strengths and limitations. Section 4 provides the proposed approach, experimental results, and discussion. Section 5 discusses the conclusion and future work.

DESCRIPTION OF DATA PROTOCOLS FOR IOT SYSTEM

This section detailed description of some widely employed data communication protocols (HTTP, MQTT, DDS, XMPP, AMQP and CoAP) in IoT environment.

Hyper Text Transport Protocol

The Hyper Text Transport Protocol (HTTP) is the basic client-server protocol used by the Web. HTTP uses the Universal Resource Identifier (URI) instead of the headers where the server and client communicate through the URI. It is a text-based protocol and does not define header size and payload message but depends on web server or application technology (Naik, 2017). The HTTP protocol is based on Representational State Transfer (REST), style architectures typically consist of clients and servers, that makes information available as resources identified by URIs(Foster, 2014). Indeed, HTTP that integrates with REST has been used in IoT architecture.

In addition, devices can make their country information more accessible, due to a consistent approach to creating, reading, updating, and deleting data (e.g., CRUD). It uses four modes such as POST, GET, PUT and DELETE (Dizdarevic et al., 2018). It is a very robust, yet expensive protocol and network infrastructure [2]. HTTP uses many bandwidth of the request and response model, and that is not be suitable for low power bandwidth devices(Cynthia et al., 2019). Therefore; it is difficult

to fit HTTP for IoT protocols. It transfers a large number of small web packets but over HTTP causes many problems, such as resource usage and too much delay (Yokotani & Sasaki, 2017). In addition, HTTP uses TCP as the default transport protocol and TLS / SSL security. Figure 1 depict HTTP architecture.

Message Queuing Telemetry Transport Protocol

The Message Queuing Telemetry Transport Protocol (MQTT) is designed to connect objects or sensor networks with applications and middleware(Thota, 2017).

It combines the highest overhead with the highest QoS of TCP and uses one-to-one, one-to-many, and many-to-one connectivity mechanism(Chen & Kunz, 2016). According to(Khalil, 2002), the MQTT protocol is used as an appropriate communication protocol for IoT and M2M. It uses a publish/subscribe protocol designed for lightweight M2M communications. MQTT client publishes messages to an MQTT broker, which are subscribed by other clients or may be reserved for future subscriptions. MQTT is a binary protocol and usually requires a default 2-byte header with small payload messages up to 256 MB maximum size. It uses TLS/SSL for security and TCP as a transport protocol. The MQTT construct is shown in Figure 2. It is ideal for compressed resource devices using unreliable or low bandwidth links. One of the key requirements of the Internet of Things is the idea of a low bandwidth used to send data and requirements for a small device resource. While trying to ensure trust and delivery, MQTT encountered this requirements (Hedi et al., 2017).

Data Distribution Service

The Data Distribution Protocol (DDS) is a standard open source and platform separate middleware, was developed for real-time Machine to interact machine by the Object Management Group (OMG). It's

Figure 1. HTTP architecture

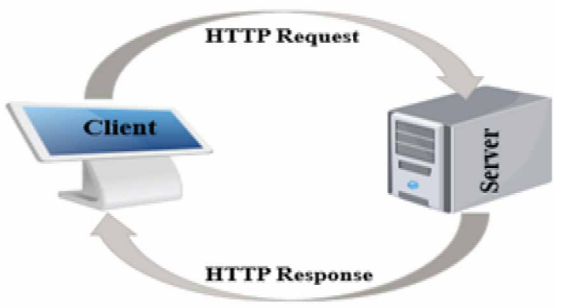


Figure 2. The architecture of MQTT

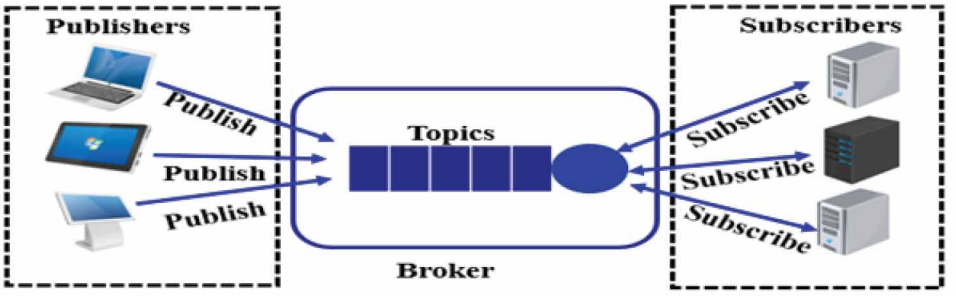
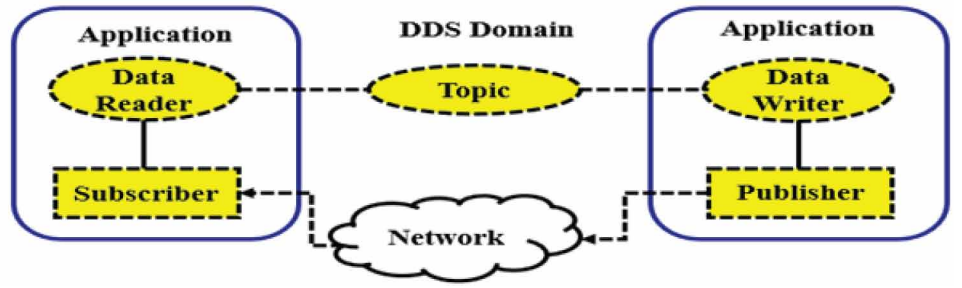


Figure 3. The conceptual model of DDS



a broker-less Publish/Subscribe properties. It use many-to-many as communication model(Almadani et al., 2015). DDS is capable to execute wide variety of mechanisms to define certain QoS according to required(Al-Madani & Ali, 2017). It is highly reliable which provides secure SSL and DTLS connections. It supports both TCP and UDP deployment and has excellent service quality and reliability guarantees such as security, durability, priority, reliability, etc. (Kaur & Kaur, 2017).

In addition, its architecture defines two layers: Data-Centric Publish Subscribe (DCPS) and Data-Local Reconstruction layer (DLRL). DCPS is responsible for providing the information to its subscribers. DLRL, on the other hand, is an optional layer and acts as an interface to DCPS usage. Enables the sharing of distributed data between distributed objects (Al-fuqaha et al., 2015). Figure 3 exhibit the conceptual model of DDS.

Extensible Messaging and Presence Protocol

The Extensible Messaging and Presence Protocol (XMPP) is an open-source messaging protocol, and was originally designed for text messaging and exchange of messages between applications. It is a text-based protocol, based on Extensible Markup Language (XML),it uses both publish/subscribe and request/ response architecture, which works over TCP(Paridhika Kayal, 2017). In IoT solutions are designed to allow users to send messages in real time. This functionality is very important in IoT-fog-cloud environments, which is the basis for many types of applications that require event notifications.

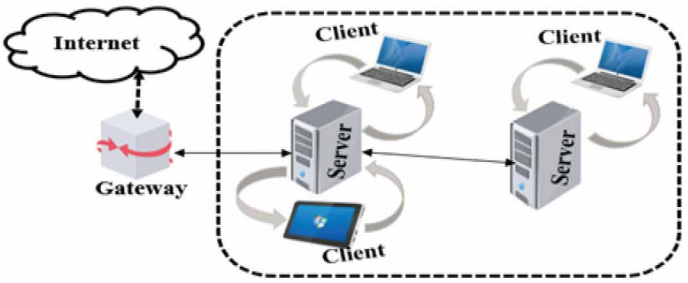
It describes as a adaptable solution provide to construct custom functionalities and give a technology for asynchronous end-to-end exchange of organize data(Celesti et al., 2017).

XMPP clients and servers communicate with each other using XML sources to exchange data in the form of XML stanzas. One of the most important features of this protocol is its security features, which make it one of the most secure messaging systems examined. XMPP incorporates TLS methods, which provide a reliable way to ensure the privacy and integrity of data. In addition, it includes extensions related to security, authentication, privacy and access control. However, more recently, there has been a lot of work to make XMPP better suited for IoT(Yokotani & Sasaki, 2017). According to (Salman & Jain, 2019) It is designed for applications near real-time, and, therefore, best supports small low latency messages. In addition, XML messages produce most overhead due to the various headers and tag formats that growth the power consumption which is critical in IoT system. The XMPP architecture is shown in Figure 4.

Advanced Message Queuing Protocol

The Advanced Message Queuing Protocol (AMQP) is the basis of a lightweight open-source IoT protocol, built for messaging-oriented networks and has a basis for Publisher/Subscriber architecture. It uses TCP as a delivery agreement to provide reliable communication. In addition, it provides three levels of QoS which are: at least once, at most once and exactly once. Furthermore, with publishers

Figure 4. XMPP architecture



and subscribers there are two additional components, Exchange and Message queues (Al-fuqaha et al., 2015). The exchange component is responsible to obtain publisher messages and give out them form a queues following predetermined roles. Subscribers connect to those queues, which basically represent topics, and get details to hear whenever they're available (Salman & Jain, 2019). Figure 5 present The Publish/subscribe mechanism of AMQP.

Constrained Application Protocol

The constrained Application Protocol (CoAP) is a lightweight contract that provides a communication channel and runs over the UDP protocol via a request / response message. This is one of the basic desires for communication between various physical devices. To achieve data transmission, CoAP keeps the message size as small as possible and supports the return mechanism of the wait. Through messaging using CoAP, clients are connected directly to the server or the client is connected to the proxy, which is connected to servers via HTTP (Anusha et al., 2017). CoAP uses Universal Resource Identifier (URI) instead of headers. It is a binary protocol and usually requires a consistent 4-byte header with small payload messages up to a large size depending on the web server or application technology. It uses UDP as a transport protocol and DTLS for security, as a result, it has strong security that enables the desired choice among existing IoT protocols (Rahman, 2016). Therefore, clients and servers communicate using offline data with minimal reliability. However, it uses "valid" or "uncertain" messages to provide two different levels of QoS.

There, verified messages must be received by the recipient with the ACK packet and the non-verified messages are not (Naik, 2017). CoAP is intended to play the same role as HTTP for Web Internet and is considered to be HTTP replacement for IoT networks and has become the standard protocol for many IoT solutions (Thantharate et al., 2019). Figure 6 sketch CoAP Architecture.

Figure 5. Publish/subscribe mechanism of AMQP

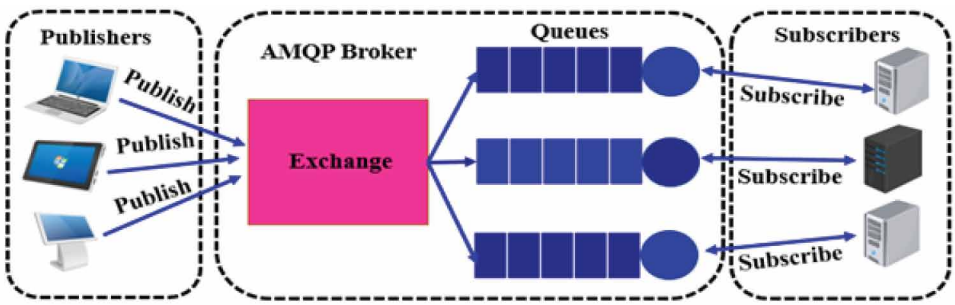
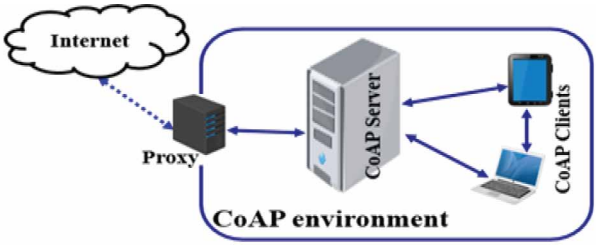


Figure 6. CoAP Architecture



Analytic Hierarchy Process

The multi-criteria analysis methods have been proposed in order to facilitate the decision making(Aali et al., 2017),thus, the analytical hierarchy process (AHP) is a multi-criteria decision-making process. It has been used to solve informal problems in a variety of decision-making situations, from simple personal decisions to complex decisions (Khalil, 2002).

Power Consumption

In order to calculate the power consumption, we will use the following formula, which is used in (A Velinov & Mileva, 2016):

$$Power\ \ consumption = \frac{Energest\_Value \times Current \times Voltage}{RTIMER\_SECOND \times Runtime} \quad (1)$$

Energest_Value: Characterize the difference between two values of modules (CPU, LPM, TX and RX) in two-time intervals. The Voltage value is 3 V. The RITIMER_SECOND is 32768. For the current, the values as well as CPU mode -9mA, Standby Mode - 0.5μA, RX Mode -18.8mA, TX Mode - 17.4mA used for Z1 circuits (Aleksandar Velinov et al., 2019) and a value of 10s as RUNTIME which is the time interval.

Linear Regression Model

The Linear Regression model is one of the most widespread methods using to evaluate the relationship between the independent variables and their influence on the dependent variable(Target) (Yildiz et al., 2017). It is an analysis mechanism in predictive investigation apply to find satisfactory linear and scatter plots as well efficiently as possible (Aviral Gupta et al., 2017). Here, it is implemented to predict the Power Consumption of CoAP and MQTT application Protocols.

Table 1. The scale of relative importance (Khalil, 2002)

Numerical assessment	Linguistic meaning
1	Equal important
3	Moderately more important
5	Strongly more important
7	Very strongly important
9	Extremely more important
2,4,6,8	Intermediate values of importance

COMPARATIVE OF COMMUNICATION PROTOCOLS FOR IOT SYSTEMS

This section presents analysis and evaluation of the performance of HTTP, MQTT, DDS, XMPP, AMQP and CoAP data protocols in terms of energy consumption, security, bandwidth, latency, QoS and applications. The performance of each protocol depends on their application.

The MQTT and CoAP protocols appear as lightweight in IoT market(Elhadi et al., 2018). HTTP performs well on various scales but is less reliable while MQTT is very reliable(Rani & Gill, 2019).

In (Jaikar & Iyer, 2018), the authors have shown that HTTP requires much higher power and resources than any other protocols such as AMQP, MQTT, and then it decreases for the other protocols like CoAP which requires lowest power and resource. According to (Bandyopadhyay, 2013)(Çorak et al., 2018), CoAP is better than MQTT for energy usage. CoAP is incorporated with DTLS, while, MQTT, XMPP and AMQP can be combine with TLS to establish secure communication (Dragomir et al., 2016). In addition, the AMQP protocol covers many security-related features and MQTT was extremely efficient. Accordingly (Naik, 2017), AMQP has the highest level of support for security and additional services, while MQTT is just a data protocol and supports the lowest level of security Except TLS/SSL, MQTT has a minimal authentication characteristics which exclusively depend on simple username and password. The CoAP uses two methods DTLS and IPsec for authentication, integrity and encryption. HTTP facilitates two authentication approaches: HTTP Basic and Digest.

EXPERIMENT AND ANALYSIS

AHP Method Applications (Case Study)

In order to apply the AHP method for those IoT Application protocols, a criterion as well as Security, Energy, Bandwidth, and Latency selected for AHP method. However, the following steps are making (Zaninetti, 2019):

Step 1: Criteria and alternatives are deduced by defining the problem. Hierarchical tree structure is created award to these criteria and alternatives.
Step 2: After the hierarchy created, a pair of 1–9 based on the scale of relative importance in Table 1 is employed.
Step 3: The Pairwise Comparison is created and normalized. Column values are taken for this, and each value is divided by the value of its column. Therefore, a normalized matrix is obtained.
Step 4: After that, the weight vectors for the criterion are calculated.
Step 5: The decision-maker measures are bilaterally consistent. Consistency index (CI), which is evaluated as an indicator of the consistency, is calculated.
Step 6: A consistency ratio (CR) is obtained which is the ratio of CI to the rationality index (RI). In AHP, the CR that is smaller than 0.1 designates that the application is consistent. Afterward, we find as results those values in the Table 3.

The AHP method proposed to find the best alternative within a decision matrix, using certain criteria, finds the best solution.

Additionally, Figure 7 shows the evolution of the protocol criteria as a weight of each criterion. From this figure, we remark that the weight of security is 91.18%, 26.21%, and 26.49% more important than weights of latency, energy, and bandwidth, respectively. For this, we can conclude that the weight for each criterion allows us to choose the criterion for evaluating and improve the data protocols in IoT.

Proposed Approach

As has been shown in the previous sections, application-layer protocols are an essential part of the data communications in the Internet of Things (IoT). In fact, the power consumption of these protocols

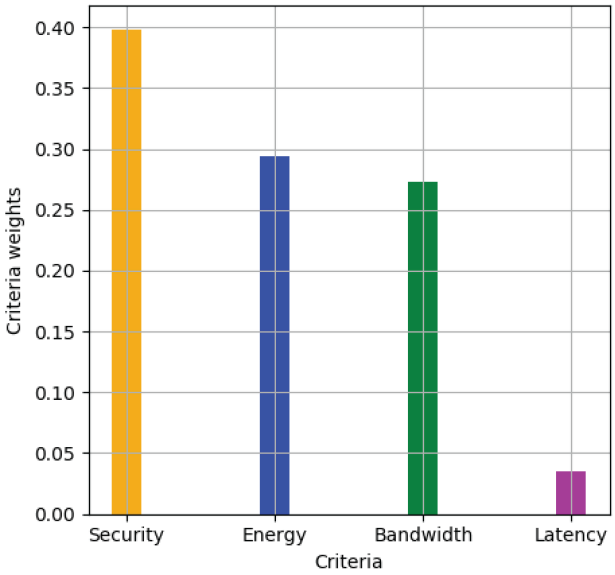
Table 2. Comparative of communication protocols for IOT systems: HTTP, MQTT, DDS, XMPP, AMQP and CoAP

Characteristics	HTTP	MQTT	DDS	XMPP	AMQP	CoAP
Architecture	Client/Server	Client/Broker	broker-less	Client/Server	Client/Broker or Client/Server	Request/Response or Publish/Subscribe
Abstraction	Request/Response	Publish/Subscribe	Broker-less Publish/ subscribe	Request/ Response Publish/ Subscribe	Publish/ Subscribe or Request/ Response	Request/Response or Publish/Subscribe
Header Size	Undefined	2 Byte	-	no Header uses XML Stanza	8 Byte	4 Byte
Message Size	Heavyweight	lightweight	-	lightweight	Lightweight	yes
Cache and Proxy Support	Yes	Partial	yes	yes	Yes	yes
Quality of Service (QoS)/ Reliability	Limited (via Transport Protocol - TCP)	QoS 0 - At most once (Fire-and-Forget), QoS 1 - At least once, QoS 2 - Exactly once.	23 policies: Security, reliability, durability, priority etc	No support for QoS	Settle Format (similar to at most once) or Unsettle Format (similar to at least once)	Confirmable Message (similar to at most once) or Non-confirmable Message (similar to at least once)
Transport Protocol	TCP	TCP (MQTT-SN can use UDP)	UDP	TCP	TCP, SCTP	UDP
Energy consumption	requires highest power/energy consumed by HTTP was much larger than with MQTT	MQTT was more energy efficient	----	Increase power consumption	requires slightly higher power	CoAP is more efficient in terms of energy
Security	TLS/SSL	TLS/SSL has the lowest level	TLS/SSL, DTLS	TLS/SSL	TLS/SSL, IPsec, SASL Strongest security	DTLS, IPsec guarantee authentication, integrity and encryption
Connectivity	One -to-one	one-to-one, one-to-many and many-to-many	peer-to-peer communication one-to-one, one-to-many, many-to-many, and many-to-one	One -to-one	point-to-point	one to one and many to many communications
Latency	involves largest latency, HTTP has highest latency than all others	MQTT has lowest latency than HTTP	Low latency	Low latency	AMQP has lowest latency than MQTT	CoAP has lowest latency than all others
Bandwidth consumption	involves largest bandwidth	consumes higher bandwidth	Low	Low	High consumption of bandwidth	involves lowest bandwidth
Encoding Format	Text	Binary	Binary	Text	Binary	Binary
Standards	IETF and W3C	OASIS, Eclipse Foundations	OMG	IETF	OASIS, ISO/ IEC	IETF, Eclipse Foundation
Applications	Web	Home automation, Enterprise level applications	Medical Imaging, Military Systems,	Instant Messaging, Group chat, Gaming, Vehicle Tracking	Business Messaging, and in Banking Industry	Smart homes, smart grid and Building automations

Table 3. AHP methods result

Characteristics	Criteria weights
Security	0.3982
Energy	0.2938
Bandwidth	0.2729
Latency	0.0351

Figure 7. Evaluation of criteria of communication protocols using AHP method

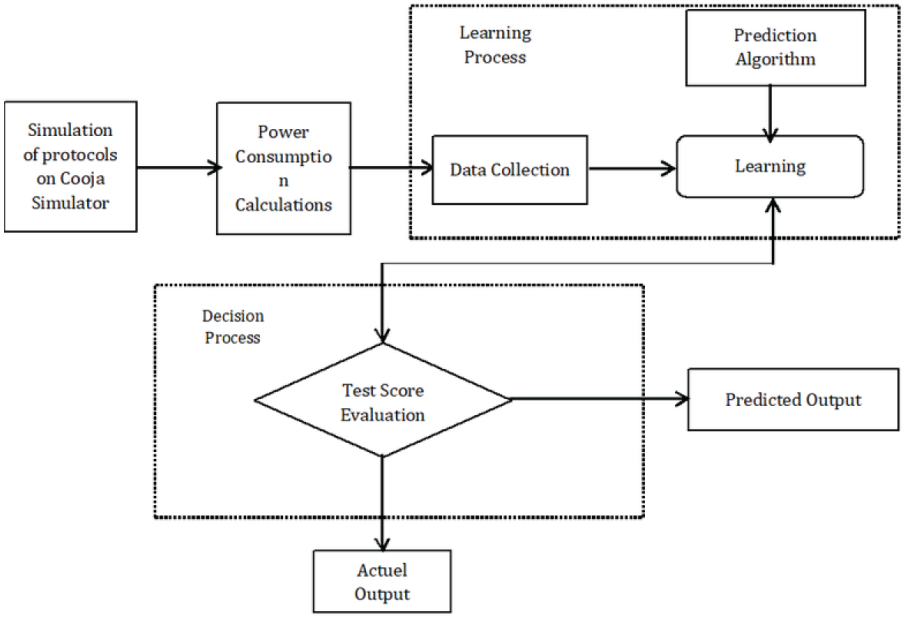


is a crucial problem in IoT. Therefore, in (Baranauskas et al., 2019; Kargar & Soleimani-roozbahani, 2018; Toldinas et al., 2019; Aleksandar Velinov et al., 2019) authors studied and evaluated the power consumption of MQTT and CoAP protocols. However, to the best of our knowledge, there do not exist many works addressing the prediction of power consumption of these protocols, indeed, several steps have been carried out to predict the power consumption of the IoT application layer protocols, in particular, both of them that are namely CoAP and MQTT. First, in the beginning, the simulation of both CoAP and MQTT protocols was performed on the Cooja simulator, which is the Contiki network simulator based on java and it allows various network simulations of Contiki motes. Contiki is an open-source operating system for constrained systems and the Internet of Things.

Moreover, modules as well as the MSP430 microcontrollers, CC2420 radio transceivers, and Zolertia motes, more specifically Z1 motes(A Velinov & Mileva, 2016)(Martí et al., 2019), used on both clients and server to simulate CoAP protocol. Besides, the communication between our networks has been ensured through the RPL border router. On the other hand, the simulation of the MQTT protocol is provided by using three entities: a publisher, subscriber, and border router. However, in cooja, there is a tool that is 'Powertrace' to calculate the power consumption, it introduced by adding these lines: (APP += powertrace, #include "powertrace.h", and powertrace_start (CLOCK_SECOND * 10) in the Makefile and client file respectively(Aleksandar Velinov & Mileva, 2018).

As a result of these simulations, the data of different states modules such as ALL_CPU, ALL_LMP, ALL_TX, and ALL_RX at the mote output for the Z1 module in Cooja have been obtained.

Figure 8. Proposed Approach Methodology



Furthermore, formula (1) has been used to calculate the power consumption of those protocols. In fact, thanks to this formula, a dataset including 200 rows and 6 columns was created. Its columns have attributes like Energyst_vallue, current, voltage, RTIMER_Second, Runtime, and Power Consumption. Finally, the power consumption prediction process based on a linear regression model is started by means of this dataset.

Result and Discussion

By using the dataset that is mentioned in the previous section and applying the Linear Regression Model, we obtain these results.

As can be seen, Figure 9 is shown the distribution of the data, Figure 10 is exhibited the relationship between the power consumption and Energest_value. The training set score is displayed in Figure 11. The test set score is presented in Figure 12. Figure 13 shows how actual and predicted data matched together. It was clear that the predicted and actual data were correlated significantly and the linear regression model can predict power use with an acceptable error and the highest accuracy in the tested prediction. However, the percentage error of a mean squared error was about 0.13%. Moreover, both Training and Testing set got the best score of Power Consumption prediction based on this method.

These results have highlighted the efficiency of the proposed approach in terms of the prediction of power consumption of those protocols.

CONCLUSION

The data communication efficiency, in IoT systems, is a major factor in the development of IoT data protocols. To achieve data communication efficiency, we analyzed and evaluated the principles application protocols of IoT. In addition, we focus more on benchmarking and comparison of HTTP, MQTT, DDS, XMPP, AMQP, and CoAP in terms of power, security, QoS, communication, and

Figure 9. Power Consumption and Energest_value of CoAP and MQTT Protocols

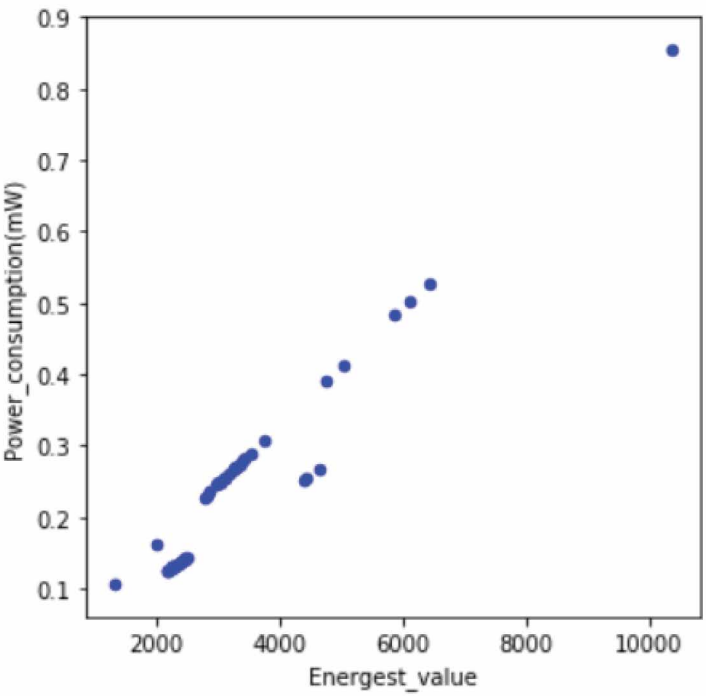


Figure 10. Relationship between Power Consumption and Enegest_value of CoAP and MQTT Protocols

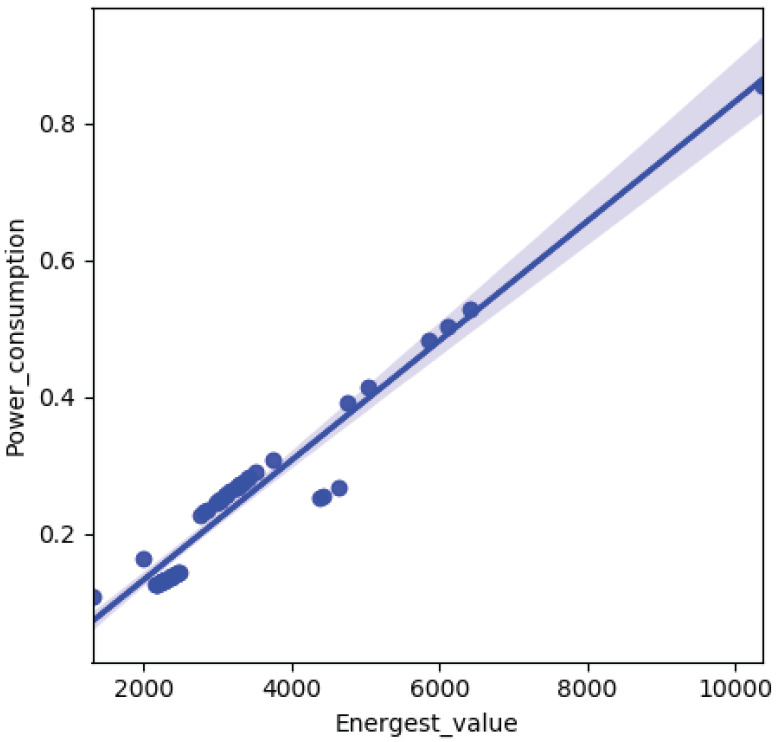


Figure 11. Training set score

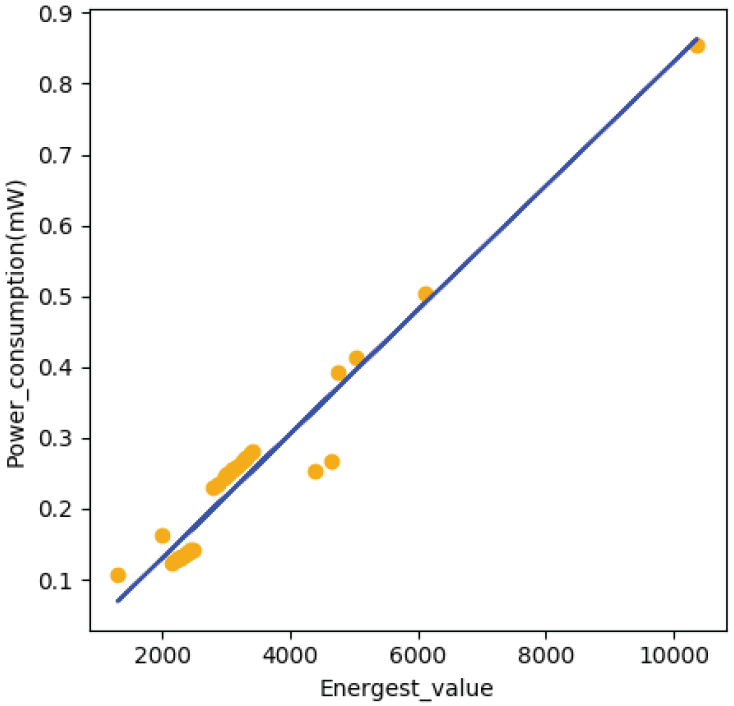


Figure 12. Test set score

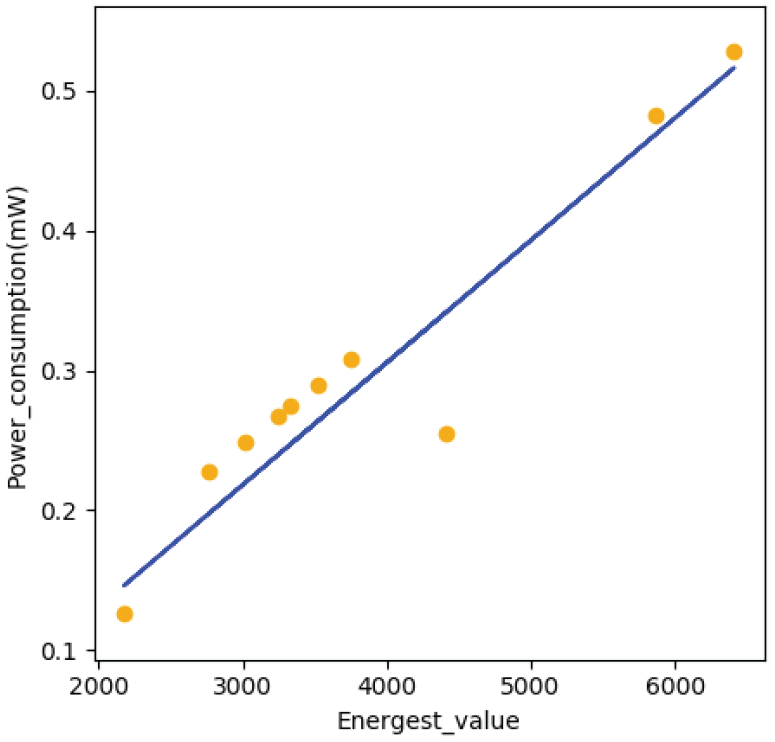
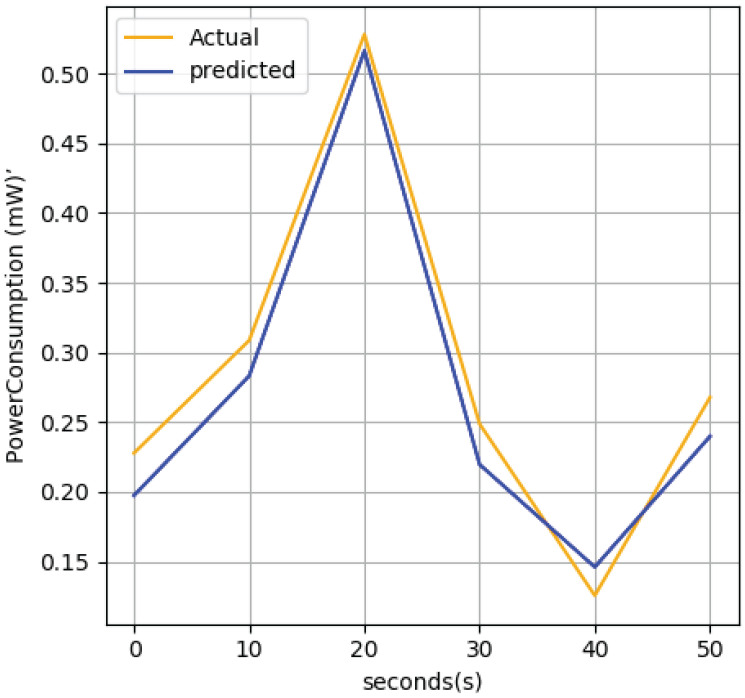


Figure 13. Actual and Predicted power consumption output of both CoAP and MQTT protocols



durability. To make this comparison easy, some applications are introduced using the advantages and disadvantages of each protocol in relation to other user policies. Additionally, in order to improve the reliability of data communications in IoT applications, the power consumption prediction of MQTT and COAP has been analyzed based on a linear regression model. After analyzing and evaluating all protocols of the application layer, the HTTP requires higher power than the other protocols, while the AMQP, CoAP, and DDS protocols are more robust than the HTTP, MQTT, and XMPP in terms of security.

In this paper, the performance of data protocols in IoT was analyzed in terms of power, security, QoS, communication, and latency. As future work, it can be expanded to manage simulation and to ensure analytical comparisons. A schedule can be added to select the appropriate data process for each case using other algorithms of Artificial Intelligence. Also, additional oversight of this function would be to find the appropriate protocol for energy efficiency and security and to compare the protocol with existing protocols.

REFERENCES

Aali, N. A., El Bouzekri El Idrissi, Y., Baina, A., & Echabbi, L. (2017). Collaboration decision making based on AHP method in Tr-OrBAC model: Case study. *Colloquium in Information Science and Technology, CIST*, 779–784. 10.1109/CIST.2016.7804992

Al-fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. doi:10.1109/COMST.2015.2444095

Al Khalil, M. I. (2002). Selecting the appropriate project delivery method using AHP. *International Journal of Project Management*, *20*(6), 464. doi:10.1016/S0263-7863(01)00032-1

Al-Madani, B., & Ali, H. (2017). Data Distribution Service (DDS) based implementation of Smart grid devices using ANSI C12.19 standard. *Procedia Computer Science*, *110*, 394–401. doi:10.1016/j.procs.2017.06.082

Almadani, B., Bajwa, M. N., Yang, S. H., & Saif, A. W. A. (2015). Performance evaluation of DDS-based middleware over wireless channel for reconfigurable manufacturing systems. *International Journal of Distributed Sensor Networks*, *2015*(7), 863123. Advance online publication. doi:10.1155/2015/863123

Anusha, M., Suresh Babu, E., Sai Mahesh Reddy, L., Vamsi Krishnam, A., & Bhagyasree, B. (2017). Performance analysis of data protocols of internet of things: A qualitative review. *International Journal of Pure and Applied Mathematics*, *115*(6), 37–47.

Bandyopadhyay, S. (2013). *Lightweight Internet Protocols for Web Enablement of Sensors using Constrained Gateway Devices*. Academic Press.

Baranauskas, E., Toldinas, J., & Lozinskis, B. (2019). *Evaluation of the impact on energy consumption of MQTT protocol over TLS.* Academic Press.

Bianco, V., Manca, O., & Nardini, S. (2013). Linear regression models to forecast electricity consumption in Italy. *Energy Sources. Part B, Economics, Planning, and Policy*, *8*(1), 86–93. doi:10.1080/15567240903289549

Celesti, A., Fazio, M., & Villari, M. (2017). Enabling secure XMPP communications in federated IoT clouds through XEP 0027 and SAML/SASL SSO. *Sensors (Switzerland)*, *17*(2), 1–21. doi:10.3390/s17020301 PMID:28178214

Chen, Y., & Kunz, T. (2016). Performance evaluation of IoT protocols under a constrained wireless access network. *2016 International Conference on Selected Topics in Mobile and Wireless Networking, MoWNeT 2016*. doi:10.1109/MoWNet.2016.7496622

Cohn, R. (2012). *A Comparison of AMQP and MQTT*. Academic Press.

Çorak, B. H., Okay, F. Y., Güzel, M., Murt, Ş., & Ozdemir, S. (2018). Comparative Analysis of IoT Communication Protocols. *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018*. doi:10.1109/ISNCC.2018.8530963

Cynthia, J., Sultana, H. P., Saroja, M. N., & Senthil, J. (2019). *Security Protocols for IoT*. Springer International Publishing. 10.1007/978-3-030-01566-4

Dizdarevic, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2018). A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. *Survey of Communication Protocols for Internet-of-Things and Related Challenges of Fog and Cloud Computing Integration.*, *1*(1), 1–30. doi:10.1145/3292674

Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016). A Survey on Secure Communication Protocols for IoT Systems. *2016 International Workshop on Secure Internet of Things (SIoT)*, 47–62. doi:10.1109/SIoT.2016.012

Dudic, B., Smolen, J., Kovac, P., Savkovic, B., & Dudic, Z. (2020). Electricity usage efficiency and electricity demand modeling in the case of Germany and the UK. *Applied Sciences (Switzerland)*, *10*(7), 2291. Advance online publication. doi:10.3390/app10072291

Elhadi, S., Marzak, A., Sael, N., & Merzouk, S. (2018). Comparative Study of IoT Protocols. SSRN *Electronic Journal*. 10.2139/ssrn.3186315

Foster, A. (2014). *Messaging Technologies for the Industrial Internet and the Internet of Things Whitepaper.* Prismtech. http://www.prismtech.com/sites/default/files/documents/MessagingComparsionMarch2014USROW-final.pdf

Gupta, A., & Sharma, A. (2017). Review of Regression Analysis Models. *International Journal of Engine Research*, *V6*(08), 58–61. doi:10.17577/IJERTV6IS080060

Hedi, I., Špeh, I., & Šarabok, A. (2017). IoT network protocols comparison for the purpose of IoT constrained networks. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 501–505. doi:10.23919/MIPRO.2017.7973477

Jaikar, S. P., & Iyer, K. R. (2018). A Survey of Messaging Protocols for IoT Systems. *International Journal of Advanced in Management, Technology and Engineering Sciences, 8*(2), 510–514. http://www.ijamtes.org/gallery/12.feb ijamtes 254.pdf

Kargar, M. H., & Soleimani-roozbahani, F. (2018). *The Effect of Using COAP Protocol on Reducing Energy Consumption in Smart Houses (Case Study : Uromieh Culture House)*. Academic Press.

Kaur, J., & Kaur, K. (2017). Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends. *International Journal of Computer Network and Information Security*, *9*(4), 57–70. doi:10.5815/ijcnis.2017.04.07

Kayal. (2017). *A Comparison of IoT Application Layer Protocols Through A Smart Parking Implementation*. Academic Press.

Martí, M., Garcia-Rubio, C., & Campo, C. (2019). Performance Evaluation of CoAP and MQTT_SN in an IoT Environment. *Proceedings*, *31*(1), 49. doi:10.3390/proceedings2019031049

Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. *2017 IEEE International Symposium on Systems Engineering, ISSE 2017 - Proceedings*, 1–7. doi:10.1109/SysEng.2017.8088251

Rahman, R. A. (2016). *Security analysis of IoT protocols : A focus in CoAP*. Academic Press.

Rani, D., & Gill, N. S. (2019). Review of various IoT standards and communication protocols. *International Journal of Engineering Research & Technology (Ahmedabad)*, *12*(5), 647–657.

Safa, M., Kc, B., & Safa, M. (2015). Linear Model To Predict Energy Consumption Using Historical Data From Cold Stores. *International Journal of Advances in Science Engineering and Technology Spl, 3*, 2321–9009. https://researcharchive.lincoln.ac.nz/bitstream/handle/10182/8479/6-205-1449220970146-150.pdf?sequence=1

Salman, T., & Jain, R. (2019). *A Survey of Protocols and Standards for Internet of Things. 1*(1). https://arxiv.org/abs/1903.11549

Thantharate, A., Beard, C., & Kankariya, P. (2019). CoAP and MQTT based models to deliver software and security updates to IoT devices over the air. *Proceedings - 2019 IEEE International Congress on Cybermatics: 12th IEEE International Conference on Internet of Things, 15th IEEE International Conference on Green Computing and Communications, 12th IEEE International Conference on Cyber, Physical and So,* 1065–1070. doi:10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00183

Thota, P. (2017). *Implementation and Analysis of Communication Protocols in Internet of Things.* https://digitalscholarship.unlv.edu/thesesdissertations/3047

Toldinas, J., Lozinskis, B., Baranauskas, E., & Dobrovolskis, A. (2019). MQTT Quality of Service versus Energy Consumption. *2019 23rd International Conference Electronics*, 1–4.

Velinov, A., Mileva, A., & Stojanov, D. (2019). *Power Consumption Analysis of the New Covert Channels in CoAP.* Academic Press.

Velinov, A., & Mileva, A. (2016). Running and Testing Applications for Contiki OS Using Cooja Simulator. *International Conference on Information Technology and Development of Education,* 279–285. http://eprints.ugd.edu.mk/16096/1/Zbornik-ITRO-2016-283-289.pdf

Velinov, A., & Mileva, A. (2018). Power consumption analysis of application layer protocols for the Internet of things. *Advances in Intelligent Systems and Computing*, *665*, 193–202. doi:10.1007/978-3-319-68855-8_19

Yildiz, B., Bilbao, J. I., & Sproul, A. B. (2017). A review and analysis of regression and machine learning models on commercial building electricity load forecasting. *Renewable and Sustainable Energy Reviews, 73*(March), 1104–1122. 10.1016/j.rser.2017.02.023

Yokotani, T., & Sasaki, Y. (2017). Comparison with HTTP and MQTT on required network resources for IoT. *ICCEREC 2016 - International Conference on Control, Electronics, Renewable Energy, and Communications 2016, Conference Proceedings*, 1–6. doi:10.1109/ICCEREC.2016.7814989

Zaninetti, L. (2019). Evaluation of the Difficulties in the Internet of Things (IoT) with Multi-Criteria Decision-Making. *Processes (Basel, Switzerland)*, *7*(3), 164. Advance online publication. doi:10.3390/pr7030164

Sidna Jeddou has a Master's degree in Electronics and Telecommunication from Abdelmalek Essaâdi University, Tetouan, Morocco, in 2018. Currently, he is a Ph.D. student in computer science and telecommunications at the National Institute of Posts and Telecommunications (INPT), Rabat, Morocco. His research interests focus on the Internet of Things and the application of artificial intelligence on the prediction of energy consumed by the Internet of Things application layer protocols.

Amine Baina is an Associate Professor at the National Institute of Posts and Telecommunications Rabat, Morocco. He had his PhD in Computer Science in "Access Control for Critical Infrastructures" in 2009 from the Laboratory of Systems Analysis and Architecture in Toulouse. He had his Computer Engineer's degree from the National Engineering School of Bourges, France, in 2005.

Abdellah Najid received the M.Sc. degree in networking and communication systems and the Ph.D. degree in electronic engineering from ENSEEIHT, Toulouse, France. He has several years of research experience with ENSEEIHT, ENSTA, INRIA, and ALTEN. He joined the National Institute of Posts and Telecommunications (INPT), Rabat, Morocco, in 2000, as a Full Professor of microwave and telecommunication engineering. He has devoted more than 16 years to teaching microwave engineering, wireless networking, network architectures, and network modeling courses, and directing research projects in wireless network performance analysis, wireless sensor networks, microwave, and antennas design.

Hassan El Alami received the master's degree in electronics and computer science from Mohammed Premier University, Oujda, Morocco, in 2012, and the Ph.D. degree in computer science and telecommunications from the National Institute of Posts and Telecommunications (INPT), Rabat, Morocco, in 2019. His current research interests include the Internet of Things, with a focus on the application of artificial intelligence and optimization algorithms for the Internet of Things. He is a TPC Member of the International Conference on Fuzzy Systems and Data Mining. He is a Student Member of the IEEE Computer Society. He serves as a reviewer for many leading international journals and conferences.