Wi-SUN FAN Interoperability: Verification through Experiment Test

Ananías Ambrosio, Rodrigo J. Riella, Luciana M. Iantorno, Victor B. Gomes, Evelio M. G. Fernández

***Abstract*— In this work, experimental tests of interoperability between devices from different providers were performed using the Wireless Smart Ubiquitous Network Field Area Network (Wi-SUN FAN) profile. This profile is part of the Wi-SUN Alliance, supporting Low Power and Lossy Networks (LLNs). The interoperability experiments were carried out in two different operation modes of the profile. Additionally, security was enabled and disabled, as well as channel hopping functionality, using the 915 MHz-b band allocated to Brazil. The interoperability was verified through the communication between the different devices, using response time and success rate as metrics of the communication analysis.**

***Keywords*— Wi-SUN FAN, interoperability, channel hopping, fixed channel, security, response time, experimental test.**

I. Introduction

The Wi-SUN Alliance [1] was established in April 2012 in Tokyo as an initiative of the NICT (National Institute of Information and Communications Technology). The alliance seeks to promote certified standards for different wireless network applications, offering solutions for public services, smart cities, utilities and IoT (Internet of Things). Among the technical profiles promoted by the Wi-SUN Alliance, the FAN Profile is a specification for Field Area Networks based on the mesh topology – each node in the network can serve as a router for the others, which means information can hop over several nodes before reaching its destination. The main concern of the profile is the interoperability between devices from different manufacturers, hence the use of open protocols: IEEE 802.15.4-2015 [2] in the physical and data link layers; IPv6 with 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) as an adaptation layer [3] and RPL (IPv6 Routing Protocol for LLNs) [4] in the network layer; UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) in the transport layer; IEEE 802.1X and EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) in security access control.

The FAN profile defines a discovery and joining procedure composed of five join states in which nodes exchange control messages in order to reach the operational state within the network [5]. This procedure is examined in Wi-SUN FAN certification tests to evaluate the technical interoperability [6] of different products, ensuring their compliance to the FAN standard [7]. Interoperability research work on IoT technologies focuses on a more global vision due to their heterogeneity, especially with studies on different semantic models (exact meaning of the content to be exchanged) [8], [9], [10], that help the integration of the different devices that would make up an IoT ecosystem [11], [12]. This work does not cover this global vision, but it is focused on the technical interoperability among Wi-SUN FAN technology products, verifying the interoperability in their physical, link and network layers.

As indicated, the initial objective of the suppliers is the certification of the profile, and therefore the interoperability of their own customized products in their models of their manufacturing line. Also, the FAN profile seeks the interoperability of the products of different suppliers, a first demonstration was carried out at the DistribuTECH 2020 event [13], where interoperability tests were performed with different certified suppliers.

On the user side, achieving this interoperability would be beneficial mainly in cost, flexibility and ease of choice of the product for an application [14]. In Brazil, many electricity utilities aim to implement Wi-SUN FAN networks for Smart Grid application. So far, some of these utilities have run pilot tests with this protocol. In most of them the equipment used during the test were Wi-SUN like, thus could not interoperate with other Wi-SUN devices. For this reason, this work seeks to replicate these tests, carrying out experimental communication tests between a prototype provided by Lactec (called Multilink End Device and Multilink Concentrator) and devices from two other suppliers in order to verify interoperability between them.

Although the Wi-SUN Alliance have promoted and carried out interoperability tests, none of these tests were performed using the Brazilian configuration. Besides, the main goal of the tests promoted by the alliance is to demonstrate the connection of the devices in the same network. This paper aims to analyze the interoperability not only by verifying the connection of the devices, searching through the verification of the links, for possible interoperability difficulties between providers, but also by analyzing the performance of the communication.

The network setup in each experiment was composed of two devices, one configured as Border Router (BR) and the other as a Router (R) Node. The interoperability was analyzed using several Wi-SUN FAN configurations, including PHY operating modes 1b (50 kbps) and 3 (150 kbps), fixed channel and channel hopping (in the 915 MHz-b band assigned to Brazil, which has some limitations as explained in the next section), and security enabled and disabled. Two items/points

Ananías Ambrosio, Rodrigo J. Riella e Evelio M. G. Fernández, Federal University of Parana, Curitiba. E-mails: ananiasambrosio@ufpr.br, riella@ufpr.br, evelio@ufpr.br. Rodrigo J. Riella, Victor B. Gomes, and Luciana M. Iantorno, Lactec Institutes. E-mails: riella@lactec.org.br, victor.gomes@lactec.org.br, luciana.iantorno@lactec.org.br. This work was financed by the project PD 0047 0080/2017of the P&D Aneel program of the Neoenergia group.

were considered in order to analyze the experiment results: first, whether the joining procedure was successful or not; and second, the communication latency after joining the network, calculated by the time difference between ICMPv6 (Internet Control Message Protocol Version 6) Echo Request and Echo Reply packets ("ping").

This work is organized as follows: in addition to this introductory Section I, Section II describes the Wi-SUN FAN technical specification, which was used in the work; Section III details the proposed interoperability scheme, as well as the configurations and device providers; in Section IV, the results are presented according to the indicated metrics; and finally, Section V presents the final conclusions.

II. Wi-SUN FAN

The Wi-SUN FAN Profile protocol stack consists of four layers in the OSI (Open System Interconnection) model, as shown in Fig. 1.

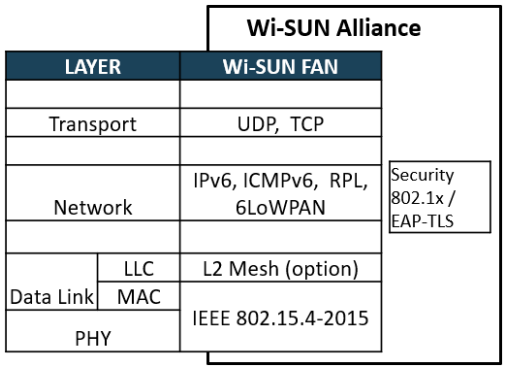


Fig. 1. Wi-SUN FAN profile protocol.

The transport layer is based on the UDP and TCP protocols. The network layer uses IPv6 with 6LoWPAN adaptation and for the formation of the network uses RPL with ICMPv6 for control messages. The data link is formed by the LLC (Logical Link Control) and MAC (Media Access Control) sub-layers based on the IEEE 802.15.4-2015 standard. The physical layer is also based on this same standard. For security and authentication, Wi-SUN FAN employs IEEE 802.1X and EAP-TLS [5].

A. Modes of operation

The physical layer of the FAN profile is derived from a sub-set of IEEE 802.15.4-2015, addressed to the physical specifications for SUN (Smart Ubiquitous Network) devices with different modes of operation for different regions. In the case of Brazil [15], according to regional regulatory requirements from ANATEL (National Telecommunications Agency), Wi-SUN FAN operates in the 902-907.50 MHz and 915-928 MHz unlicensed frequency bands. The experiments described in this work employed Physical Operating Modes 1b and 3, whose characteristics are presented in Table I. All Wi-SUN FAN devices in the Brazil region must support Operating Modes 1b and 3, while support for the remaining operating modes (2a, 4a and 5) is not mandatory.

The channel frequencies of the band for Wi-SUN FAN are defined according to [5]:

$$F_c = F_{c0} + N_c S_c, \tag{1}$$

where F_c is the center channel frequency, F_{c0} is the channel 0 center frequency, N_c is the channel number and S_c is the channel spacing. In the case of Brazil, Operating Mode 1b uses F_{c0} = 902.2 MHz, while Operating Mode 3 uses F_{c0} = 902.4 MHz. All channels in the 902-928 MHz range are numbered; even the channels between the two non-contiguous Brazilian bands, which are blocked from operation. When using a channel spacing of 200 kHz, devices may transmit on channels 0-25 and 65-128, making a total of 90 channels. Therefore, channels 26 through 64 were excluded, as indicated in the profile. The channel spacing of 400 kHz is applied to channels 0-11 and 33-63, making a total of 43 channels, excluding channels 12 through 32.

B. Join states

The join states are the steps through which the nodes pass to establish the routing of the network layer [5].

a) Join State 1 (PAN selection): the node has no information about neighbors or PANs (Personal Area Network) available. To discover the available PANs, a node transmits and listens to PAS (PAN Advertisement Solicit) and PA (PAN Advertisement) frames, respectively. The node must select the EAPOL (Extensible Authentication Protocol over LAN) destination and transition to Join State 2.

b) Join State 2 (Authentication): the node performs authentication, group key acquisition (GTK) and IEEE 802.1X security flow provided by the BR base station at the PAN to enter the Join State 3. If authentication and key acquisition are not successful, the node must fall back to Join State 1.

c) Join State 3 (Acquire PAN configuration): the node sends PCS (PAN Configuration Solicit) frames, requesting the transmission of a PC (PAN Configuration), which provides configuration information for a PAN. The node transmits PCS frames at a frequency directed by a trickle timer [16]. If the node fails to receive a valid PC frame after a certain amount of PCS transmissions, a node returns to Join State 1. If the PC is successfully received, it transitions to Join State 4.

d) Join State 4 (Routing configuration): upon entering this state, the node is a secured member in its PAN. Then, the node must establish connectivity at layer 3 using the RPL protocol [4]. After joining the RPL DODAG (Destination Oriented Directed Acyclic Graph), the node transitions to Join State 5.

e) Join State 5 (Operational): the node is fully operational in the network and can communicate using IPv6. Operational nodes must transmit PA and PC frames at an interval directed by trickle timers in order to maintain the connection with its PAN. The BR is always in this state.

TABLE I
PHYSICAL SPECIFICATIONS OF WI-SUN FAN FOR BRAZIL.

Frequency Band (MHz)	Operating Mode	Symbol Rate (ksymbol/s)	Modulation	Modulation Index	Channel Spacing (kHz)	Number of Channel
902-907.5 e	1b	50	2FSK	1.0	200	90
915-928	3	150	2FSK	0.5	400	43

C. Security enabled and disabled

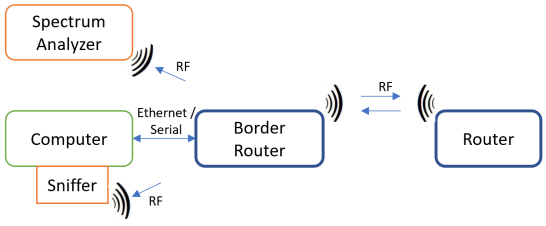
The security-enabled option follows the complete joining procedure, composed of five Join States. The security-disabled option in Wi-SUN FAN deactivates Join State 2 (Authentication). In other words, nodes transition from Join State 1 directly to Join State 3 upon selection of an available PAN. This significantly reduces the complexity of the joining procedure, but disables all security features of the protocol stack.

D. Channel function

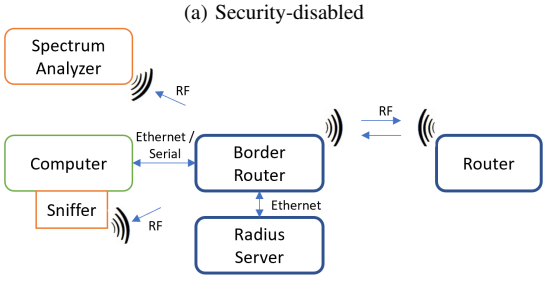
A channel function defines the method used by the device to select the operation channel, from the list of available PHY channels, at a given time. Wi-SUN FAN supports multiple channel functions on the MAC sublayer for both unicast and broadcast operations: TR51CF (TR51 Channel Function), DH1CF (Direct Hash Channel Function), Fixed Channel and Vendor Defined Channel Function. A node can additionally advertise a set of channels to be excluded from its hopping sequence. Each node announces its channel schedules with information necessary for the neighboring node to determine which channel a node will be operating at any time. The fixed channel mode is supported for situations in which the channel hopping is not desired.

III. METHODOLOGY FOR INTEROPERABILITY TEST

The methodology used in the interoperability experiments is based on an architecture with two configurations: security-disabled, as shown in Fig. 2 (a) and security-enabled, as shown in Fig. 2 (b).



(a) Security-disabled



(b) Security-enabled

Fig. 2. Experiment architecture.

The main difference in the architectures is the RADIUS Server added in the case of security enabled. In the point-to-point communication of the BR and R, the analysis and data collection of the FAN network is performed at Computer. The distance between the BR and the R devices was set to two meters, making the link combinations between the different providers, as shown in Fig. 3.

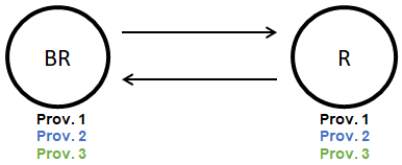


Fig. 3. Link diagram.

The methodology began with the verification of the Join State sequence, carried out through capture of log data via serial interface of the BR and/or R Node. The BR node already starts in Join State 5, whereas the R node begins in Join State 1 and goes through the joining process until reaching Join State 5, as shown in Fig. 4.

```
PAN: Join State 1 -> Select PAN
PAN: Resetting PAN Advertisement Solicit timer
PAN: Scheduling PAN Advertisement Solicit timer 195 ticks in future (Interval)
  .                 .                 .
  .                 .                 .
PAN: Selected candidate 0007810801d25f6f as preferred EAPOL target
PAN: Join State 2 -> Authenticate
AUTH: Request need PMK, need PTK, GTKs present: 00, GTKs live: 00
AUTH: Send EAP with 106 bytes to 0007810801d25f6f
AUTH: Recv EAP with 9 bytes from 0007810801d25f6f
  .                 .                 .
  .                 .                 .
AUTH: Recv PTK efea73d1bd9652481ac780a622c7ec50bc96f0dcee510063b8fa8068d4b4bb2601ec99
AUTH: Recv GTK #0 0102030405060708090a0b0c0d0e0f10 (valid: 01)
PAN: Join State 3 -> Acquire PAN Config
PAN: Resetting PAN Configuration Solicit timer
PAN: Scheduling PAN Configuration Solicit timer 217 ticks in future (Interval)
PAN: Received PAN Configuration from 0007810801d25f6f
PAN: Join State 4 -> Configure Routing
RPL: Init of IPv6 data structures
RPL: RPL started
  .                 .                 .
  .                 .                 .
RPL: Received a DAO ACK with sequence number 241 (current: 241) and status 0 from fc9
PAN: Join State 5 -> Operational
PAN: Resetting PAN Advertisement timer
```

Fig. 4. Log capture in R.

The Spectrum Analyzer was used to verify the RF operating modes of the experiments, parameters such as the frequency band, number and spacing of channels, as shown in Fig. 5.

The verification of RF frames was carried out through the Wireshark program, which captures frames with a Sniffer at a fixed channel, allowing us to verify the relevant profile settings, as shown in Fig. 6.

A. Experiment scenarios and setting

For the interoperability experiments, four scenarios were tested, as shown in Table II. The channel function is configured either as fixed channel or as channel hopping, which,

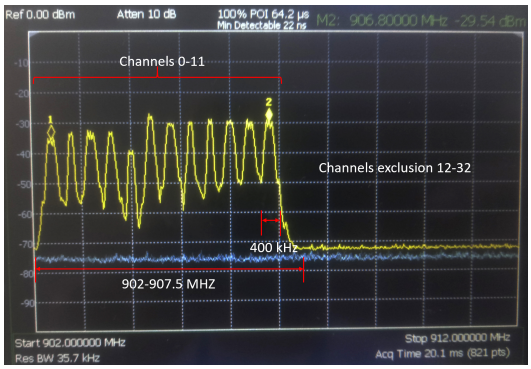


Fig. 5. Capture of spectrum analyzer in operating mode 3 (first part of the frequency band of Brazil).

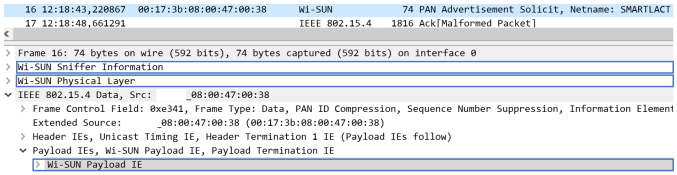


Fig. 6. Verification of RF frames with Wireshark.

according to the profile, must be implemented by regulatory domains in Brazil. The function to determine the current channel is DH1CF; the function TR51CF is not used as it was not implemented in the test devices (it is not mandatory).

TABLE II
EXPERIMENT SCENARIOS.

Item	Security	Operating Mode	Channel Function
Scenario 1 (S1)	Disabled	1b	Fixed channel
Scenario 2 (S2)	Disabled	1b	Channel hopping (DH1CF)
Scenario 3 (S3)	Enabled	1b	Channel hopping (DH1CF)
Scenario 4 (S4)	Enabled	3	Channel hopping (DH1CF)

Device configurations were performed according to Table III and verified with the spectrum analyzer and Wireshark.

TABLE III
SCENARIO SETTINGS.

Description	Configuration	Verification
Operating mode	1 / 3b	Wireshark
Channel spacing (kHz)	200 / 400	Spectrum analyzer
Fixed channel	Ch14 (S1)	Spectrum analyzer
Frequency hopping	Ch. 0-25 and 65-128 / Ch. 0-11 and 32-63	Spectrum analyzer
Modulation	2FSK	Wireshark
Data rate (kbit/s)	50 / 150	Wireshark
Unicast/Broadcast dwell interval	100 ms, 120 ms	Wireshark

In all scenarios, the ping test was performed by sending 100 ICMPv6 Echo packets with 65 data bytes each, one every five seconds. Since the Multilink devices are still under development, its command interface does not yet offer a ping generator. Therefore, this part of the test was not performed with Multilink BR.

B. Data from tested devices

The list of devices used in the experiments is shown in Table IV.

TABLE IV
TESTED PROVIDERS.

Description	Device	Provider
Prov. 1	Border Router, Router: Multilink	Lactec
Prov. 2	Border Router BR2, Router R2	Provider 2
Prov. 3	Border Router BR3, Router R3	Provider 3

The Multilink and Provider 2 devices can be easily configured using tools supplied by the providers. In the case of Provider 3, the devices factory configuration cannot be changed. Thus, for this experiment, the provider arranged devices pre-configured for each test scenario.

IV. RESULTS

The success of communication link establishment between different providers is shown in Table V, where a successful interoperability scenario is represented by a checkmark (✓).

TABLE V
INTEROPERABILITY BETWEEN PROVIDERS.

BR	R	S1	S2	S3	S4
Prov. 1	Prov. 2	✓	✓	✓	✓
Prov. 2	Prov. 1	✓	✓	✓	✓
Prov. 2	Prov. 3	✓	✓	✓	-
Prov. 3	Prov. 2	-	-	-	-
Prov. 3	Prov. 1	✓	✓	✓	-
Prov. 1	Prov. 3	✓	✓	✓	-

The results show that, in all tested scenarios, the different devices were able to complete the discovery and join process through the Join States of the FAN profile. The link Prov. 3 - Prov. 2 in all scenarios and the links Prov. 2 – Prov. 3, Prov. 3 – Prov. 1 and Prov. 1 – Prov. 3 in Scenario 4 were not made, represented by a dash (-), this is due to limited access to equipment configuration.

The results of packet success rate obtained in the ping test are shown in Fig. 7 for different combinations of providers. For the links Prov. 1 - Prov. 2 and Prov. 1 - Prov. 3, communication was only verified through a serial terminal, the pings were not processed due to the lack of a ping generator in the Multilink BR prototype.

It was verified that for the links BR Prov. 2 - R Prov. 2 and BR Prov. 2 - Prov. 1 in all scenarios it has a success rate of 100%, which indicates an optimal communication between these two providers. In the case of the links BR Prov. 3 - R Prov. 3 in scenarios S2 and S3, a success rate of 90% and 93% was verified, respectively, this indicates a lower performance compared to the other providers. Therefore, this decrease in the event rate is especially reflected in the link BR Prov. 2 - R Prov. 3 with 85%, this result indicates that the device configuration of Prov. 3 is not totally equal to the devices Prov. 1 and Prov. 2, which affects the data success rate.

The results of response time are shown in Fig. 8 for different combinations of providers.

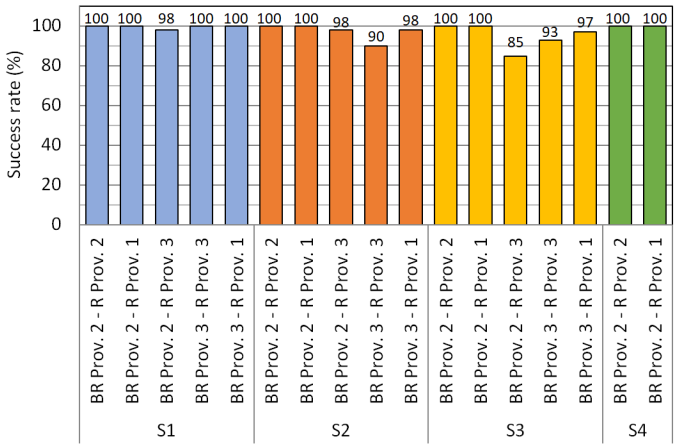


Fig. 7. Success rate of ping.

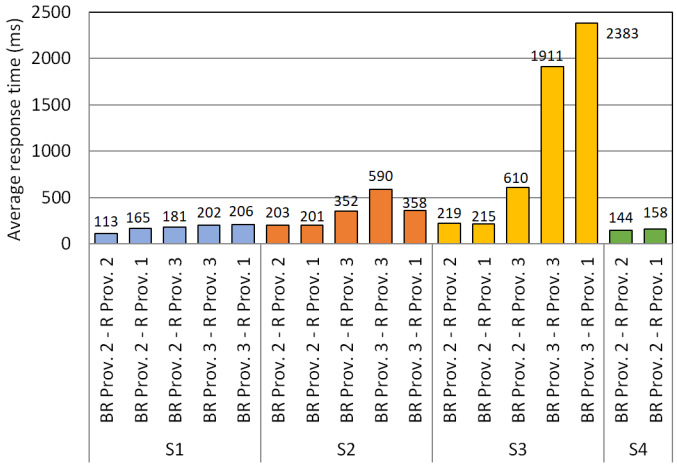


Fig. 8. Response time of ping.

In tests using the device of Prov. 3, response times were much higher in the security-enabled scenario, especially in the link BR Prov. 3 - R Prov. 1 of scenario 3, with a response time of 2383 ms. This correlates to the higher packet loss rate of this device compared to the others. The provider may want to adjust configurations and review the implementation of the Wi-SUN FAN stack to improve performance.

The methodology used allowed for the practical and quick verification of technical interoperability in the physical, link and network layers by verifying the configuration and link of the devices. The results of the experiments showed a first approach to interoperability between the different devices of the test, also obtaining the measurements of the metrics such as response time and the packet success rate. The results of the prototype called Multilink are comparable with the result of the device with the best performance during the test. But, the use of a different configuration application provided by each provider was observed, which does not allow a standard configuration for each device.

Interoperability is not only limited to adopting open protocols. A realistic interoperability is reaching an agreement between the different providers to offer greater flexibility for the configuration of device, providing a general application that allows access to the essential configurations of the profile. Therefore, the same vision of other research is reached, the importance of aiming to have an ideal interoperability platform that allows the coexistence of different devices for IoT. A great challenge for interoperability remains open for different providers.

V. Conclusion

This work proposes a scheme for experimental interoperability tests of Wi-SUN FAN. The proposed scheme was employed to evaluate the interoperability of devices of three different providers and it was observed that, in most scenarios, the devices were able to perform the joining procedure and communicate effectively. In addition, it was observed that the Multilink prototype has similar results to those of the device with the best performance in the experiments.

Acknowledgment

This work was financed by the project PD 0047 0080/2017 of the P&D Aneel program of the Neoenergia group.

References

[1] Wi-SUN alliance, “Wi-SUN Alliance,” https://www.wi-sun.org.
[2] IEEE 802.15.4, “IEEE Standard for Low-Rate Wireless Personal Area Networks (WPANs) ”, IEEE Std 802.15.4-2015.
[3] V. Kumar and S. Tiwari, “Routing in IPv6 over low-power wireless personal area networks (6LoWPAN): a survey”, Journal of Computer Networks and Communications, 2012.
[4] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, R. Alexander, “RPL: IPv6 routing protocol for low-power and lossy networks,” IETF RFC 6550, Mar. 2012.
[5] WI-SUN FAN, “Technical Profile Specification Field Area Network, Field Area Network Working Group (FANWG)”, Confidential c Wi-SUN Alliance, 2017.
[6] H. Rahman, and M. I. Hussain. "A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges." Transactions on Emerging Telecommunications Technologies 31.12 (2020): e3902.
[7] Wi-SUN alliance, “Wi-SUN FAN Certification Program: The Foundation For IoT End Device Interoperability” [Fact sheet], https://wi-sun.org/wp-content/uploads/Wi-SUN-Alliance-Fact-Sheet.pdf, 2018.
[8] H. J. Kim, et al. "A comprehensive review of practical issues for interoperability using the common information model in smart grids." Energies 13.6 (2020): 1435.
[9] A. Cimmino, M. Poveda-Villalón, and R. García-Castro. "ewot: A semantic interoperability approach for heterogeneous iot ecosystems based on the web of things." Sensors 20.3 (2020): 822.
[10] M. Noura, M. Atiquzzaman, and M. Gaedke. "Interoperability in internet of things: Taxonomies and open challenges." Mobile Networks and Applications 24.3 (2019): 796-809.
[11] A. Bröring, et al. "Enabling IoT ecosystems through platform interoperability." IEEE software 34.1 (2017): 54-61.
[12] R. A. Deshmukh, et al. "Data Spine: A Federated Interoperability Enabler for Heterogeneous IoT Platform Ecosystems." Sensors 21.12 (2021): 4010.
[13] Wi-SUN alliance, “What to Expect from the Wi-SUN Alliance in 2021”, https://wi-sun.org/blog/wi-sun-alliance-20201, 2021.
[14] N. Mahda, M. Atiquzzaman, and M. Gaedke. "Interoperability in internet of things: Taxonomies and open challenges". Mobile Networks and Applications, v. 24, n. 3, p. 796-809, 2019.
[15] IEEE Std 802.15.4v, “IEEE Standard for Low-Rate Wireless Networks - Amendment 5: Enabling/Updating the Use of Regional Sub-GHz Bands”, IEEE Std 802.15.4v-2017.
[16] P. Levis, T. Clausen, J. Hui, O. Gnawali, J. Ko, “The trickle algorithm,” IETF RFC 6206, Mar. 2011.