Towards Universal IoT Metrics Automation

Hassan Soubra[1]

[1]German University in Cairo, New Cairo, Egypt

Abstract

The Internet of Things (IoT) refers to a network of physical objects: embedded devices- also known as "things"- with sensors/actuators and connectivity (Internet) that enables them to exchange huge amounts of data. Metrics are an omnipotent means allowing better management of systems, Software and devices. This paper discusses the current state of IoT metrics and the underlying diversity in defining them. It also attempts to define a universal list of IoT metrics to cover most of the basic measurable attributes for any IoT device. A tool to visualize and automate IoT metrics' readings using the MQTT protocol has also been implemented and is presented in this paper.

Keywords

IoT, Metrics, MQTT, performance, ISO 25023, Measurement Automation

1. Introduction

The Internet of Things allows objects to sense and be controlled remotely across existing telecommunication networks, enabling thus the 'smart' paradigm. On the one hand, IoT devices are omnipresent in many domains e.g. healthcare, transportation and logistics. On the other hand, metrics help transform the vague requirements of a system or a device into a series of numbers that can be used to accurately map a process for its efficiency.

Metrics give objective indicators whether a process is good enough to meet the end goals of the system or if there is a possibility for improvement. Conclusions are hard to be drawn from raw metrics alone and they are usually assisted by computer visualization techniquessuch as graphs and diagrams. Measuring IoT metrics is also a hard task as IoT devices are usually composed of smaller hardware devices and Software components; and where the simplistic approach of just adding their metrics together does not usually represent the overall measurement of the system as a whole. Some metrics can also be hard to measure such as reliability and interoperability which are key metrics for an IoT device.

To our best knowledge, there are no published works on universal IoT metrics due to how complex and diverse the IoT environment is. This paper attempts to define the basic universal metrics that should offer useful insight for any IoT device regardless of the device's use or application domain and does not include device specific metrics which cannot be applied to all IoT devices. An implemented tool to automate and visualize IoT metrics using the MQTT protocol is also presented in this paper.

IWSM/MENSURA 22, September 28–30, 2022, Izmir, Turkey

hassan.soubra@guc.edu.eg (H. Soubra)
0000-0003-0056-6015 (H. Soubra)

© 2022 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3272/IWSM-MENSURA22_paper6.pdf

The rest of the paper is organised as follows. While Section 2 presents the related literature on the subject, Section 3 presents the approach of this paper. Section 4 presents the automation and the implemented tool. A conclusion follows in section 5.

2. Literature review

Universal IoT metrics are scarce, because IoT devices are complex and diverse. To our best knowledge, the literature review shows no published works proposing universal IoT metrics. The literature review shows that the related previous works focused on specific metrics such as Interoperability, Security, Reliability, Network, Energy and Software related metrics and measurement. Additional metrics related studies that are relevant to the IoT paradigm are also presented in this section.

In [1], IoT security issues are presented and a security metric as an attempt to fix them is proposed. The hierarchical scale of measuring interoperability and attempts to measure the degree of interoperability using a metric scaled quantity is proposed in [2].

Network metrics such as bandwidth, packet error rate, packet delay, delay jitter; and a formula for calculating packet delay and delay jitter are proposed in [3]. A formula for measuring the bandwidth metric which is the amount of data network that can transfer per unit time is proposed in [4]. Received Signal Strength Indicator measurement as the estimate of the power of the signal is proposed in [5].

A method for estimating noise power and Signal to Noise Ratio for OFDM Based Wireless Communication Systems is proposed in [6]. Network metrics, in addition to the formulas for measuring packet delivery ratio, connectivity range and spreading factor are proposed in [7]. [8] discussed the coding rate metric of the network and provided its measurement formula. Network load, reliability, data rates, effective utilization of channels and energy efficiency metrics are used in [9]. Additional network metrics are found in [10].

The formulas for measuring control message overhead, throughput, data loss rate and residual energy metrics are proposed in [11]. Spectrum efficiency metric is defined as throughput divided by bandwidth in [12]. Data rate is used as a metric in [13]. Network reliability is used as a metric in [14]. Measuring the implementation complexity metric is found in [15]. In [16], the sampling frequency metric is measured. In [17], IoT network, hardware, energy and quality of experience metrics; and the mean opinion score metric are discussed. In [18], network metrics, including the availability metric, are measured. Measuring network lifetime and energy consumption ratio are proposed in [19].

The formula for measuring end-to-end delay and packet loss ratio metrics are proposed in [20]. A formula for measuring scalability metric is found in [21]. In [22], LoraWan physical layer integration on IoT devices is evaluated using bit error rate, signal to noise ratio and some other metrics. A formula for measuring the bit error rate metric is found in [23]. A formula for measuring the congestion which is the summation of queue length and channel contention, and how the queue length and channel contention can be calculated is in [24]. Temperature, number of alive nodes, residual energy, etc. are used as network and energy metrics in [25] and [26].

A comparison between different IoT communication protocols in terms network metrics including the packet creation time metric is proposed in [27]. A comparison of four LPWAN IoT technologies using energy and network metrics is in [28]. While [29] evaluated the capabilities and behaviors of some wireless technologies in IoT using network size and power consumption. A formula for measuring the energy efficiency metric is proposed in [30]. Different IoT communication protocols using power consumption, spreading are compared in [31]. The time duration for which the sensor is sensing metric is in [32].

IoT software, quality and test metrics and how to measure them are presented in [33]. Formulas and definitions for measuring software metrics such as volume of code and code redundancy are presented in [34].

A formula for measuring the cohesion software metric is proposed in [35]. Software metrics for evaluating android based IoT applications are used in [36].

The quality of information and data metrics in IoT based smart environments are discussed in [37]. Formulas for measuring quality of information and data metrics for IoT systems are provided in [38]. Quality metrics for evaluating IoT applications such as recoverability and efficiency are in [39]. Security metrics for assessing security of the IoT are defined in [40]. Inference and data privacy metrics in IoT networks are discussed in [41]. Privacy policies metrics are divided into four categories in [42]. In [43], machine learning algorithms for attack and anomaly detection in IoT sensors are presented.

In [44], a Functional Size Measurement for IoT real-time embedded software and a measurement example as a guideline are proposed.

3. Universal IoT metrics approach

The approach proposed towards the universal IoT Metrics relies on the following definition of IoT by the OECD [45]: “all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals”. The ISO 25023 standard [46] is used as a reference in our approach. The ISO 25023 defines quality measures for evaluating system and software characteristics and provides an explanation of how to apply each one. Each ISO 25023 inspired metric was given an applicability score using the Likert [47] scale with the following coding: Very Good, Good, Neutral, Poor, and Very Poor; depending on the applicability of the characteristic to IoT devices. The applicability perspective is whether the characteristic applies to very a specific device or applies universally to all devices.

3.1. Functional Suitability

Functional Suitability guaranties that functions meet stated and implied needs when used under specified conditions. It contains functional completeness which measures the amount of implemented functions relative to the specified functions in the design. In addition, Functional correctness measures how precise the data coming out of a device is, and functional appropriateness which measures the device’s capacity to only perform the necessary functions performed by the user. All three metrics have an applicability score of very good since they are very relevant to IoT.

3.2. Performance efficiency

Performance efficiency enables assessing the performance relative to the amount of resources used under stated conditions and may include software products, system configuration or materials. It includes time related metrics such as: mean response time, response time adequacy, mean turnaround time, turnaround time adequacy and mean throughput. These time related metrics are all relevant to IoT as any IoT device is expected to have some time constraints. Unlike hard real time systems, which are expected to have 100another category of performance metrics which includes processor, memory, I/O device and bandwidth utilization. All these performance metrics indicate the consumption of CPU time, memory, and bandwidth, they are hence relevant to any IoT device and have a score of very good. Capacity metrics include transaction processing capacity, user access capacity and user access increase adequacy. These metrics are related to the ability of the system to accommodate simultaneous user access. These metrics are partly relevant to all IoT devices. These metrics offer useful insight if the device in question can have more than one simultaneous user. Since not all devices have more than one simultaneous user, these metrics get a score of Good as they are partly applicable.

3.3. Compatibility

Compatibility metrics assess the degree to which a product, system or component can exchange information with other products, systems or components, and perform its required functions while sharing the same hardware or software environment. Compatibility related metrics include Co-existence that measures the ability of a device to co-exist without interference with other devices or components, a very relevant metric to IoT and gets a score of very good. Interoperability measures the ability of two or more devices to interact together and the beneficiality of data exchanged. The ISO 25023 defines data format exchangeability and data exchange protocol sufficiency as subcharacteristics of the interoperability. These metrics do not seem relevant to all IoT devices and hence are given a score of neutral.

3.4. Usability

Usability measures ensure the comprehensibility of product usage, learning and operation. Usability metrics include description completeness, demonstration coverage, and entry point self-descriptiveness. All three metrics are relevant to IoT. These metrics are highly subjective to the user base of the device and consequently are given a score of good. Learnability is another category of usability metrics. It includes entry fields defaults which is irrelevant to IoT and does not provide any useful added insight, hence is given a score of very poor. Error messages understandability and user guidance completeness are very relevant to IoT, as they are key measures of how easily an IoT device can be operated. Very good applicability, self-explanatory user interface is also another learnability metric but as it is partly subjective to the user base, it has good applicability. Operability, which is part of usability, measures operational consistency, input device support and monitoring capability that are very relevant metrics to IoT. Consistency and monitoring are key measures to any device and are given a score of very good. Functional customizability and user interface customizability are yet another user subjective metrics and are given a score of good. Undo capability however, is not very relevant to IoT as it is more device specific. User error protection metrics include avoidance of user operation error, user entry error correction and user error recoverability are given very good applicability, as they are relevant. User interface aesthetics and accessibility metrics that include appearance aesthetics of user interfaces, accessibility for users with disabilities and supported languages adequacy are device specific metrics, hence having neutral applicability.

3.5. Reliability

Reliability refers to the degree to which a system, product or component performs specified functions under specified conditions for a specified period of time. Reliability metrics include fault correction, mean time between failure (MTBF), failure rate, test coverage, system availability, mean down time, failure avoidance, mean fault notification time, mean recovery time and backup data completeness. All previously mentioned metrics are key indicators of how reliable an IoT device is and have very good applicability. The redundancy of component however, is not applicable to all devices as it measures how redundant each component is and in some devices redundancy is not implemented, therefore has good applicability as it is partly device specific.

3.6. Security

Security relates to the protection of data, networks, and hardware, with data security being most important. Security metrics include: access controllability, data encryption correctness, strength of cryptographic algorithms, authentication mechanism sufficiency, authentication rules conformity, data integrity, data corruption prevention and buffer overflow prevention. These metrics are more device specific, are not universally measurable and are given a score of neutral. Security metrics such as user audit trail completeness and system log retention are very relevant to IoT and can be easily universally measured as in the proportion of the user and system performed actions to the proportion of logged actions. These metrics are given very good applicability.

3.7. Maintainability

Maintainability refers to the ease at which a system can be modified after it has been operationalized. It includes replacement, addition of individual components to the system. Maintainability metrics include modification capability, coupling of components, reusability assets, modification efficiency, modification correctness and test function completeness. These metrics are given an applicability score of very good, as they are key metrics to IoT devices being modular and easily modified. Coding rules conformity, system log completeness, diagnosis function effectiveness and diagnosis function sufficiency do not provide useful insight when applied to all devices and are partly device specific, hence given good applicability. Test restartability is on the other hand is given a score of very poor as it does not provide any useful value when applied to IoT.

3.8. Portability

Portability is used to judge the level of transferability among different hardware, software or operational environments. Portability metrics include adaptability, hardware environmental adaptability, system software environmental adaptability, operational environment adaptability, installation time efficiency, ease of installation, product quality equivalence and data reusability/import capability. These metrics are key metrics to IoT, as they measure how adaptable an IoT device is to different environments and how reusable is the old device data when the device is upgraded; hence given very good applicability.

4. Automation of IoT metrics

This section presents first the IoT system used as a proof of concept in our study and second, the advanced dashboard-tool implemented for improved metrics' visualization.

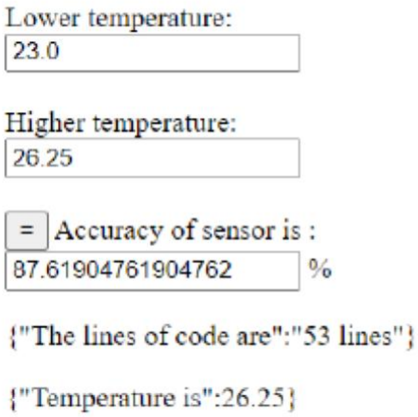
4.1. IoT system set-up

A simple IoT system that measures the room temperature has been implemented. The system uses the Message Queueing Telemetry Transport (MQTT) protocol [48], which is one of the most used protocols in Device-to-Device communication in the IoT environment. The ESP8266 chip has also been used because it is WiFi enabled and is hence able to send the IoT system's data to the basic User Interface through MQTT broker over the Internet. The ESP8266 connects to the internet through a local Wi-Fi access point. Eclipse broker has been used to publish and subscribe to topics. A topic about the temperature measured by the sensor is created - to be used for the functional correctness metric. In addition, this topic also include the number of lines of code LOC-as a Software metric. The dashboard is subscribed to this topic and hence receives these two data. The accuracy metric of the sensor is then measured using the difference between the sensor data (Higher temperature) and the actual temperature (Lower temperature), as shown in Figure 1.

4.2. Advanced dashboard-tool

Metrics help the user draw conclusions based on numbers. However, these conclusions might be hard to reach by only looking at raw numbers. The goal of this tool is to ease the analysis of metrics and display them in a user friendly way. The tool implements a secure authentication system that allows a user to login to the system in order to use its features. The authentication system hashes the password before inserting it into the database for additional security. More than one user can register and use the tool concurrently. After logging in, the user can specify their own Device Schema, see Figure 2.

A Device Schema is a list of MQTT Topics which the tool should listen to. The device should also be given a unique name as an identifier. The client or device ID is expected to be the second level of the topic, e.g.: "smart door/ aduino1970/cpu/usage" where "aduino1970" is the device ID. The device sends some metric readings to the tool which displays them. The user is presented with a table that presents the metrics specified in the schema and their respective values. These



Lower temperature: 23.0

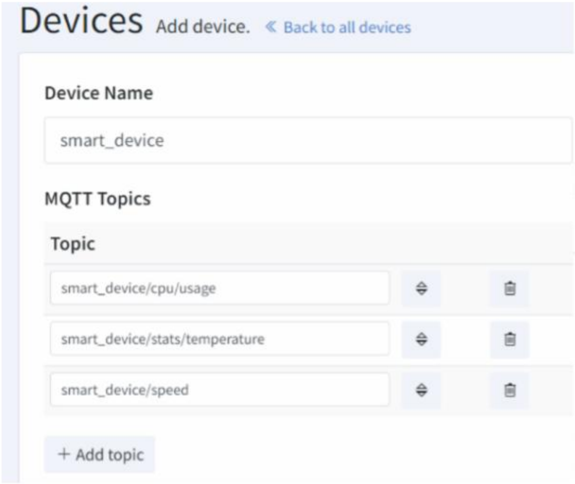
Higher temperature: 26.25

Accuracy of sensor is : 87.61904761904762 %

{"The lines of code are":"53 lines"}

{"Temperature is":26.25}

Figure 1: Measured vs actual temperature, sensor accuracy and LOC



Device Name: smart_device

MQTT Topics

Topic:
smart_device/cpu/usage
smart_device/stats/temperature
smart_device/speed

Figure 2: Device Schema example

metrics are then displayed in a table showing their values for each connected client or device. Since many devices can co-exist, the user can filter each metric by range of values, exact value, less than or greater than a value. Compound filters are also applicable, as in the user can filter by a metric and then apply another filter to those results. The user can also export the entire table currently in view in formats such as: CSV, Excel and PDF.

The user can click the "View Metrics" button in the table to view the metrics as graphs, or widgets-as shown in Figure 3. A widget can have multiple attributes that the user can modify such as: Display Location (which device schema should the widget be displayed in), Widget Type (Speedometer, Gauge, Pie, Pyramid), Size, Minimum and Maximum Ranges and Units.

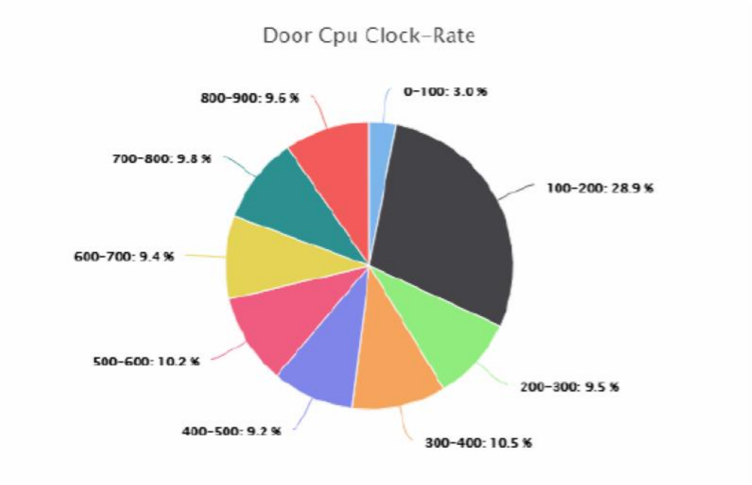


Figure 3: A Pie Widget automatically groups data of the selected metric into ranges and displays the percentages of the total devices in those ranges

In addition, the user is also presented with a robust history graph which displays a graph (line, column, pie) of the one or multiple metrics, see Figure 4. The graph supports a zoom in function enabling the focus on a certain region of the graph to get a better view. There is also a date-time picker so the user can choose the time range of the metrics to be displayed. It also supports real time graphing of metrics as the device reports them.

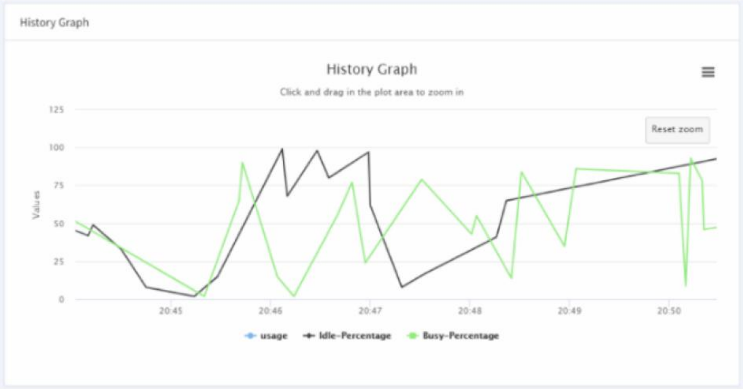


Figure 4: History Graph showing metrics over selected time range

Each widget has a set of options, which include full screen view of the widget, exporting it as excel file or an image. Finally, the dashboard-tool was built with responsiveness in mind. The tool automatically resizes to fit any screen whether it be a mobile screen of a desktop computer screen. All charts and tables resize automatically to fit a small screen such a mobile phone’s.

5. Conclusion

This paper presented an approach to define universal metrics that can be applied to any IoT device with the help of the ISO 25023 standard and other metrics from the scientific literature. The functional, software, hardware and network aspects of an IoT device are covered by the proposed metrics. Each metric includes a definition and a measurement formula when applicable. A room temperature measurement IoT system was setup using the MQTT protocol and used as a proof of concept for the automation of the proposed approach. An advanced dashboard visualization tool is also presented in this paper. The advanced dashboard implements modern visualization techniques and a variety of graph types, and it enables a high range of customization using widgets and the ability to add custom metrics that are specific to the user's device. Nevertheless, our work presents some limitations: the implementation tool only supports one protocol (the MQTT protocol). In addition, some of the proposed metrics throughout this study cannot be measured due to their nature and cannot hence be represented by a formula compared to the functional metrics for example.

Finally, although our approach originally aimed at defining universal metrics that are applicable to any IoT device, some metrics will always be specific to a particular device type, manufacturer or user and hence cannot be considered universal.

6. Acknowledgements

We would like to thank Ahmed Emad, Loaa El Zahar and Omar Elamin for their precious contribution to this project.

References

[1] Bonilla, Rafael I., et al. "A metric for measuring IoT devices security levels." 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress. IEEE, 2017.

[2] Decker, Sebastian Kotsteina Christian. "An approach for measuring IoT interoperability using causal modeling." Intelligent Environments 2019: Workshop Proceedings of the 15th International Conference on Intelligent Environments. Vol. 26. IOS Press, 2019.

[3] Dvornikov, Andrey, et al. "Qos metrics measurement in long range iot networks." 2017 IEEE 19th Conference on Business Informatics (CBI). Vol. 2. IEEE, 2017.

[4] R. Prasad, C. Dovrolis, M. Murray, and K. Clay, "Bandwidth estimation: metrics, measurement techniques, and tools," IEEE network, vol. 17, no. 6, pp. 27-35, 2003.

[5] K. Levis et al., is under appreciated," in Proceedings of the third workshop on embedded networked sensors, Cambridge, MA, USA, vol. 3031, p. 239242, 2006.

[6] H. Arslan and S. Reddy, power and snr estimation for ofdm based wireless communica-

tion systems," in Proc. of 3rd IASTED International Conference on Wireless and Optical Communications (WOC), Ban, Alberta, Canada, 2003.

[7] O. Iova, A. Murphy, G. P. Picco, L. Ghiro, D. Molteni, F. Ossi, and F. Cagnacci, "Lora from the city to the mountains: Exploration of hardware and environmental factors," in Proceedings of the 2017 international conference on embedded wireless systems and networks, 2017.

[8] R. Dougherty, C. Freiling, and K. Zeger, "Unachievability of network coding capacity," IEEE Transactions on Information Theory, vol. 52, no. 6, pp. 2365-2372, 2006.

[9] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From iot to 5g i-iot: The next generation iot-based intelligent algorithms and 5g technologies," IEEE Communications Magazine, vol. 56, no. 10, pp. 114-120, 2018.

[10] H.-J. Lee, M.-S. Kim, J. W. Hong, and G.-H. Lee, "Qos parameters to network performance metrics mapping for sla monitoring," KNOM Review, vol. 5, no. 2, pp. 42-53, 2002.

[11] M. Faheem and V. C. Gungor, "Mqrp: Mobile sinks-based qos-aware data gathering protocol for wireless sensor networks-based smart grid applications in the context of industry 4.0-based on internet of things," Future Generation Computer Systems, vol. 82, pp. 358-374, 2018.

[12] A. Alexiou, C. Bouras, V. Kokkinos, A. Papazois, and G. Tsichritzis, "Spectral effciency performance of mbsfn-enabled lte networks," in 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 361-367, IEEE, 2010.

[13] C. H. Barriquello, D. P. Bernardon, L. N. Canha, F. E. S. e Silva, D. S. Porto, and M. J. da Silveira Ramos, "Performance assessment of a low power wide area network in rural smart grids," in 2017 52nd international universities power engineering conference (UPEC), pp. 1-4, IEEE, 2017.

[14] W. Torell and V. Avelar, "Mean time between failure: Explanation and standards," white paper, vol. 78, pp. 6-7, 2004.

[15] T. Benson, A. Akella, and D. A. Maltz, "Unraveling the complexity of network management.," in NSDI, pp. 335-348, 2009.

[16] Y. Zhou, "Sampling frequency for monitoring the actual state of groundwater systems," Journal of Hydrology, vol. 180, no. 1-4, pp. 301-318, 1996.

[17] K. Fizza, A. Banerjee, K. Mitra, P. P. Jayaraman, R. Ranjan, P. Patel, and D. Georgakopoulos, "Qoe in iot: a vision, survey and future directions," Discover Internet of Things, vol. 1, no. 1, pp. 1-14, 2021.

[18] A. Hanemann, A. Liakopoulos, M. Molina, and D. M. Swany, "A study on network performance metrics and their composition," Campus-Wide Information Systems, 2006.

[19] J. Jiang, G. Han, L. Shu, S. Chan, and K. Wang, "A trust model based on cloud theory in underwater acoustic sensor networks," IEEE Transactions on Industrial Informatics, vol. 13, no. 1, pp. 342-350, 2015.

[20] O. Said, Y. Albagory, M. Nofal, and F. Al Raddady, "Iot-rtp and iot-rtcp: Adaptive protocols for multimedia transmission over internet of things environments," IEEE access, vol. 5, pp. 16757-16773, 2017.

[21] L. Alazzawi, A. Elkateeb, et al., "Performance evaluation of the wsn routing protocols scalability," Journal of Computer Systems, Networks, and Communications, vol. 2008, 2008.

[22] C. Bouras, V. Kokkinos, and N. Papachristos, "Performance evaluation of lorawan physical

layer integration on iot devices," in 2018 Global Information Infrastructure and Networking Symposium (GIIS), pp. 1-4, IEEE, 2018.

[23] I. Ali et al., "Bit-error-rate (ber) simulation using matlab," International Journal of Engineering Research and Applications, vol. 3, no. 1, pp. 706-711, 2013.

[24] V. K. Sharma and S. S. Bhadauria, "Agent based congestion control routing for mobile ad-hoc network," Trends in network and communications, pp. 324-333, 2011.

[25] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, "A metaheuristic optimization approach for energy effciency in the iot networks," Software: Practice and Experience, 2020.

[26] M. Ahmad, T. Li, Z. Khan, F. Khurshid, and M. Ahmad, "A novel connectivitybased leach-meec routing protocol for mobile wireless sensor network," Sensors, vol. 18, no. 12, p. 4278, 2018.

[27] B. H. Corak, F. Y. Okay, M. Guzel, S. Murt, and S. Ozdemir, "Comparative analysis of iot communication protocols," in 2018 International symposium on networks, computers and communications (ISNCC), pp. 1-6, IEEE, 2018.

[28] T. G. Durand, L. Visagie, and M. J. Booysen, "Evaluation of next-generation lowpower communication technology to replace gsm in iot-applications," IET Commu- nications, vol. 13, no. 16, pp. 2533-2540, 2019.

[29] M. Elkhodr, S. Shahrestani, and H. Cheung, "Emerging wireless technologies in the internet of things: a comparative study," arXiv preprint arXiv:1611.00861, 2016.

[30] F. Meshkati, H. V. Poor, S. C. Schwartz, and N. B. Mandayam, "An energy-efficient approach to power control and receiver design in wireless data networks," IEEE transactions on communications, vol. 53, no. 11, pp. 1885-1894, 2005.

[31] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols," in 2017 8th International conference on information technol- ogy (ICIT), pp. 685-690, IEEE, 2017.

[32] A. Manzoor, H.-L. Truong, and S. Dustdar, "On the evaluation of quality of context," in European conference on smart sensing and context, pp. 140-153, Springer, 2008.

[33] M. Klima, V. Rechtberger, M. Bures, X. Bellekens, H. Hindy, and B. S. Ahmed, "Quality and reliability metrics for iot systems: a consolidated view," in Interna- tional Summit Smart City 360°, pp. 635-650, Springer, 2020.

[34] R. Baggen, J. P. Correia, K. Schill, and J. Visser, "Standardized code quality benchmarking for improving software maintainability," Software Quality Journal, vol. 20, no. 2, pp. 287-307, 2012.

[35] J. Pantiuchina, M. Lanza, and G. Bavota, "Improving code: The (mis) perception of quality metrics," in 2018 IEEE International Conference on Software Maintenance and Evolution (ICSME), pp. 80-91, IEEE, 2018.

[36] J. Cui, L. Wang, X. Zhao, and H. Zhang, "Towards predictive analysis of android vulnerability using statistical codes and machine learning for iot applications," Com- puter Communications, vol. 155, pp. 125-131, 2020.

[37] B. EUSHAY and F. ANTONIO, "Domain agnostic quality of information metrics in iot-based smart environments," in Intelligent Environments 2020: Workshop Pro- ceedings of the 16th International Conference on Intelligent Environments, vol. 28, p. 343, IOS Press, 2020.

[38] D. Kuemper, T. Iggena, R. Toenjes, and E. Pulvermueller, "Valid. iot: a framework for

sensor data quality analysis and interpolation," in Proceedings of the 9th ACM Multimedia Systems Conference, pp. 294-303, 2018.

[39] M. Kim, "A quality model for evaluating iot applications," International Journal of Computer and Electrical Engineering, vol. 8, no. 1, p. 66, 2016.

[40] M. Ge and D. S. Kim, "A framework for modeling and assessing security of the internet of things," in 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS), pp. 776-781, IEEE, 2015.

[41] M. Sun and W. P. Tay, "Inference and data privacy in iot networks," in 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communi- cations (SPAWC), pp. 1-5, IEEE, 2017.

[42] M. Tavakolan and I. A. Faridi, "Applying privacy-aware policies in iot devices using privacy metrics," in 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), pp. 1-5, IEEE, 2020.

[43] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in iot sensors in iot sites using machine learning approaches," Internet of Things, vol. 7, p. 100059, 2019.

[44] Soubra, Hassan, and Alain Abran. "Functional size measurement for the internet of things (IoT) an example using COSMIC and the arduino open-source platform." Proceedings of the 27th International Workshop on Software Measurement and 12th International Conference on Software Process and Product Measurement. 2017.

[45] OECD, "IoT measurement and applications," OECD Digital Economy Papers 271, OECD Publishing. 2018.

[46] ISO/IEC. ISO/IEC 25023:2016 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Measurement of system and software product quality. 2016.

[47] A. Joshi, S. Kale, S. Chandel, and D. Pal, "Likert scale: Explored and explained," British Journal of Applied Science Technology, vol. 7, pp. 396–403, 01 2015.

[48] Soni, Dipa, and Ashwin Makwana. "A survey on MQTT: a protocol of internet of things (IoT)." International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017). Vol. 20. 2017.