IoT Protocol Selection for Smart Grid Applications: Merging Qualitative and Quantitative Metrics

Ullah Mehar, Kakakhel Syed Rameez Ullah, Westerlund Tomi, Wolff Annika, Carrillo Dick, Plosila Juha, Nardelli Pedro H. J.

DOI: 10.23919/MIPRO48935.2020.9245238

IoT Protocol Selection for Smart Grid Applications: Merging Qualitative and Quantitative Metrics

Mehar Ullah*, Syed Rameez Ullah Kakakhel**, Tomi Westerlund**, Annika Wolff*,
Dick Carrillo*, Juha Plosila**, Pedro H. J. Nardelli*
* LUT University, Lappeenranta, Finland
** University of Turku, Finland
Contact: mehar.ullah@lut.fi

***Abstract*—The concept of Internet of Things (IoT) implies that objects are connected to share information with each other and/or with a platform based on standardized communication protocols such as MQTT and HTTP. Recently, their performance has received much attention due to more widespread utilization. But, the vital aspect of the adoption of these IoT protocols is not just performance per se but also their feature set. However, comparative analysis that takes into account both the features and performance aspects are rarely presented. This paper investigates a combination of a qualitative comparison model (based on communication, operational and security attributes) with quantitative metrics in terms of CPU/memory utilization and time consumption. Quantitative metrics are collected for two of the four IoT protocols. Our analysis shows that there is no one-size-fits-all solution in terms of application layer IoT protocols. Additionally we emphasize that, on a higher level, both qualitative and quantitative measures are necessary for IoT stakeholders to consider before selecting the most appropriate protocol for the specific application to be deployed. We illustrate the results using a smart grid example simulating a collection of 1000 smart meters connected to the grid.**

***Index Terms*—IoT protocols, smart grid, MQTT, HTTP,**

I. Introduction

The Internet of Things (IoT) concept was first coined by Keven Ashton in 1999 during a presentation to Proctor and Gamble and later referenced by him in the MIT Auto-ID Center [1]. IoT is one of the fastest growing technologies that is gaining momentum in the various domains like smart grid, transportation, healthcare, industrial automation etc. Nowadays, IoT applications have already moved further away than just simple RFID tags and are incorporating different sources of data and sensors. This stream of data needs to be moved somewhere else to be processed, for example, to train machine learning models and visualization. This place is what we call an IoT platform. For companies to run their specific IoT applications, an IoT platform is thus needed. The IoT platform provides important services and features to applications: endpoint management, connectivity and network management, analysis and processing, data management, application development, security, event processing, monitoring, access control and interfacing [2], [3].

Many devices nowadays use the technologies in the IoT stack for inter-connection and sharing of information. For those devices to connect to various heterogeneous devices they need different types of protocols to overcome the problem of interoperability. The application layer is responsible for the interaction to the end user. With the advancement in technology new devices enter the market that need protocol support to perform well. [4]. With varying needs and diverse set of devices come a diverse set of protocols.

In the current scenario, there are many IoT based technologies which are available to fulfill the needs of smart grid (SG) applications. The IoT technologies are used in SG mainly for long range data transmission bi-directionally between the user side and the utility through IoT based devices like smart meters. The IoT based SG systems requires advanced wireless technologies compared to wired based technology in most of the cases to reduce the deployment and usage complexity. The information flow of data in smart grid can be divided in two channels: one is the flow between all the smart meters connected in a hub with the IoT enabled devices and appliances. The second flow is between the control centers and the utility providers. The data flow with the smart meters and the IoT enabled devices can be achieved by wireless technologies [5].

The question thus arises, which protocol will better suit the needs of these aforementioned channels. To answer that we utilize both qualitative and quantitative measures. The qualitative metrics are presented for four major IoT protocols while quantitative measures are presented for two of them (HTTP and MQTT). We then apply this knowledge to a smart grid model to identify suitable protocols for the diverse grid applications.

The rest of the paper is organized as follows. Section II contains related work. In Section III, we highlighted the four IoT protocols and smart grid attributes. Section IV contains the results, analysis and discussion. Section V concludes the paper and presents future expansion to the work.

II. Related work

In the literature some similar work is done by Niccolo et al. [6] and Edielson et al. [7]. They offer a qualitative comparison between MQTT and CoAP. The comparisons are thorough but expressive and thus not easily extendable. Their comparison is also limited to a subset of the attributes we have collected and identified (nine and seven respectively). Vasileios

et al. [8] and Ala et al. [9] provide a detailed description of major application layer IoT protocols. However, they do not provide criteria for cross comparison. Yuang et al. [10] offers a quantitative comparison of DDS, MQTT and CoAP in the context of eHealth. Paridhika et al. [11] provide a performance analysis in the context of smart parking. Antonio et al. [12], look at semantic and syntactic interoperability in the context of HTTP, CoAP and MQTT. Jens Dede and Anna Forster [13] offer a qualitative analysis of connectivity protocols such as Wi-Fi Direct and BLE for opportunistic communication. Kabeer et al. [14] provide a qualitative comparison of routing protocols.

The aforementioned is a small subset of the literature on IoT protocol comparisons. However, the theme remains the same; the studies focus on quantitative comparisons in varying contexts while offering brief qualitative comparisons. Even if provided, the qualitative assessments are limited to a subset of the protocols, expressive and not easily extendable.

IoT protocol assessments towards smart grids are primarily limited to connectivity protocols such as, WiFi, Zigbee, LoRa, LTE and 5G [15]. Another study [16] highlights an overview of the IoT elements along with architecture layers, and compared the IoT protocols like HTTP, CoAP, MQTT, and XMPP in terms of the features provided by those protocols in smart grid applications i.e. interoperability, scalability, security, latency, and provisioning. This work focuses on both features and performance of application layer protocols.

III. IoT Protocols and Smart Grid Attributes

In this study we have selected four main IoT protocols *MQTT, HTTP, CoAP, XMPP*. Similarly, smart grids also constitute different models and architectures, we present the seven main components relevant to grid communication and distribution.

A. IoT Protocols and their attributes

MQTT (Message Queuing Telemetry Transport) was introduced by IBM in 1999 and is used to collect data from remote devices. It is designed for lightweight devices that are constrained by both processing power and memory and in 2014 it became an organization for the Advancement of Structured Information Standards (OASIS) [17].

HTTP (Hyper Text Transfer Protocol) is the protocol that is used for the exchange of information between internet connected nodes that communicate via hypertext. HTTP is most commonly used application layer protocol on the internet and was first proposed in 1989.

CoAP is REST (Representational State Transfer) styled request-response protocol standardized by the Internet Engineering Task Force (IETF) [10]. CoAP can be used on devices with limited processing power, storage and bandwidth. The main difference compared to HTTP is the lower header size.It is a dual-layered protocol.

XMPP (Extensible Messaging and Presence Protocol) was originally a text-based messaging protocol for messaging between devices over a network using the XML document format, versions on XMPP are being explored for IoT by the XMPP Standards Foundation for control, sensor data and provisioning. Its strong point is its very familiar device@server naming approach. Besides that it provides end-to-end security, provisioning, and publisher-subscriber style communication.

Below is a brief of the classification model presented in [18]. There are five main categories in this section, namely, Communication Attributes, Security Attributes, Connection Attributes, Operational Attributes and Message and Payload support. All of these have sub-categories that further expand on the main characteristics. We provide a brief description of these attributes here, for deeper explanation we refer authors to [18].

1) Communication Attributes: Communication attributes constitute five main features, paradigm or architecture, i.e., is it publish-subscribe based, request-response or does it offer a message queuing architecture. Second, which underlying transport protocol is used (TCP or UDP). Sheng et al. offer a good discussion on the importance of transport protocol [11]. Third, is there multicast support? Often it is required to send messages to multiple recipients at once, a typical scenario for IoT as thousands of devices would be present in a locality. Fourth, reliability/QoS, Does the protocol offer any surety of delivery? Fifth, congestion control, when systems are overloaded and packet loss occurs, does the protocol offer any congestion control, surety or packet re-transmission mechanisms.

2) Connection Attributes/Performance: This explains the establishing and maintaining of connections. Sub categories for connection attributes include four characteristics. First, *communication complexity* in this case refers to the number of steps required to establish/setup a connection and be ready to send actual data packets. Second, *signaling traffic generated* or *frequency of updates* means besides the normal operation, how much extra traffic is generated that is not related to the user transmission, but the functioning of the protocol itself, e.g. ping requests to identify available clients or periodic updates to assess the network etc. Third, *connection establishment speed and performance*, this one deals only with the number of packets required to establish a connection. The measurements are fast, medium and slow. Slow is when a protocol has high communication complexity and requires two or more steps to establish a connection. Fourth, *session orientation* is the ability to handle sessions, this improves performance as a single user session can be used to send many updates.

3) Security Attributes: The IoT will inherit the same security issues as the current internet and will amplify them because of its deep penetration and direct connection to the real world. A major differentiating factor for the choice of the protocol is the security attributes. A point to note here is that we will be talking about the features provided by the protocol (in the protocol's draft documentation) and not the ones provided via third-party add-ons (unless officially recognized) or provided via commercial implementations of the protocol. The three different aspects of security are: First, *connection security* relates to any mechanisms provided by

TABLE I
QUALITATIVE COMPARISON. ADAPTED FROM [18].

		MQTT	HTTP	CoAP	XMPP
Communication Attributes	Communication pattern	Publish/Subscribe	Request/Response	Req./Resp.& Pub./Sub.	Req./Resp. & Pub./Sub.
	Transport protocol	TCP	TCP	UDP	TCP
	Multicast support	Yes	No	Yes	Yes
	Reliability/QoS	Yes	Nil/via TCP	Yes	Nil/via TCP
	Congestion Control	Yes	Relies on TCP	Yes	Relies on TCP
Connection Performance	Communication Complexity	Medium	Mininal	Minimal	High
	Signaling Traffic	Low to high	Low	Low	Low
	Communication Speed	4	3	3	5
	Session Orientation	Yes	Yes	Yes	Yes
Security Attributes	Connection Security	TLS	SSL	DTLS	TLS
	Communication Security	TLS	SSL	DTLS	TLS
	User Security	User/Password	User/Password	Nil	SASL
Operational Attributes	Operations	Centralized	Centralized	Decentralized	Both
	Discovery	No	Yes	Yes	Yes
	Message Durability	Yes	Yes	Some How	Yes
	Caching	Yes	Yes	Yes	Yes
Message/ Payload Support	Message Overhead	Minimal	High	Minimal	High
	Design Orientation	Byte-wise	Payload Specific	Payload Specific	Payload Specific
	Block Transfer	No (Max. msg256MB)	Yes	Yes	Yes

the protocol that enable the authentication of the nodes before any actual communication takes place. Some of the methods can include a secure key exchange between the endpoints and authentication. Second, *communication security* relates to securing communication between two nodes or endpoints. Communication security features would ensure that a third-party interception would result in no sound or identifiable information leakage. Third, *user security* in our context means whether the protocol ensures the validity/authentication of a user utilizing the system to communicate, either to the server or the broker.

4) Operational Attributes: Distributed Operation or Centralized operation refers to whether there is a control of a single node on the operation and communication of the remaining nodes or that the communication is one-to-one where both the nodes are on equal grounds. Some protocols might request that all the data go through a central point (a server or broker) and is then distributed to the intended recipients, in other cases direct messages would be the norm. Hybrid solutions can also exist. Service/node discovery defines if there are ways that the protocol offers via which machines can notice peers or associated group members. Other point is: are messages retained or discarded as soon as they are delivered? In unreliable environments or guaranteed delivery requirements, it is vital to have message retaining, although this comes at the cost of memory.

5) Messages and Payload Support: Knowing which protocol will easily integrate with the current systems is valuable and knowing the payload helps in that regard. Current web services and technologies will benefit from a protocol that offers support for web payloads (i.e., HTML, Plain text, XML). Situations that require machine-to-machine interaction will benefit from JSON or byte-wise transmission. First, Message Overhead, in the shortest form, how many more data bytes are required to make a transmission happen (in headers, checksums) for each packet to be transmitted. Second, Design Orientation, does the protocol define any document format or not? If the protocol defines a specific document format that makes it document-centric and if it does not, that will make the protocol data-centric. Third, Fragmentation/Block Transfer, the capability to divide a large data set into smaller ones and then transfer them automatically without user intervention.

B. Attributes of Smart Grid network

There are several logical networks for smart grid communication, i.e., home are network (HAN), neighborhood area network (NAN) and field area network (FAN). Various applications are expected to emerge with different requirements and features within these networks. In the section we will be discussing a few selected applications that has got significant attention from researcher in smart grid paradigm. The characteristics and requirements of those applications are highlighted below.

1) Automatic meter reading: One of the basic and simplest application of smart grid is automatic meter reading (AMR) and is used to collect meter readings, events, and alarm data from smart meters. The important published standards used in AMR are ANSI C12.1-2008, IEEE 1377 and IEC 61968-9. However, the most used one is IEC 61968-9 more general and covers most of the AMR communication, i.e., meter reading, meter connect and disconnect, meter data management, outage detection, prepaid metering etc. Both IEEE 1377 and ANSI C12.19 standards are used to provide specifications for the

communication syntax for data exchange between the end device and the utility server [19].

2) Demand response: Demand response (DR) is used by the utility operators for the optimal balancing of the power generation and consumption by utilizing the implementation of various load control programs or by offering dynamic pricing. Dynamic pricing programs are used to encourage the customers to use less energy during the peak hours. The primary role of the DR application is to communicate to the customer the price information by sending it to the smart meter in the form of a price signal. After receiving the pricing signal, the customer adjusts the energy usage to the minimum pricing period to reduce the power bill [20].

3) Electric vehicles: Electric vehicles (EV) use rechargeable batteries instead of fossil fuels and can be charged from the distributed feeder. Mostly the EV's are expected to be charged at home, however there is also the possibility to charge the EV's at the public charging stations established in parking areas [21]. Smart charging is one of the good options which enables controlled charging of the EV's using the bidirectional communication capabilities of smart grid. Centralized charging control is the device used for smart charging and allows the energy transfer session in real time. It checks the time taken by the EV's for charging and the energy available.

4) Substation automation: The substation automation mainly concerns with the monitoring, protection, and control functions that are carried out at the substation and feeder equipment. The main protocols used at the substation automation domain are IEC 61850 and DNP3/IEE1815. The DNP3 protocol is used to provide the communication specifications for low-bandwidth monitoring and control operations. IEC 61850 standard is based on interoperable intelligent electric devices (IEDs) that interacts with each other. IEC61850 standard is covering a maximum of the aspects of SAS which includes real-time, high bandwidth protection and control applications [22].

5) DER/Microgrid: Distributed energy resources (DER) are the small power sources that can generate and store power and are connected to the distributed grid. The DER can be a renewable source such as solar panels, wind turbine and battery storage system or non-renewable source such as combustion turbine and fuel cell. The DER can be implemented as a distributed generation source, distributed storage source or a combination of both. A microgrid is a small local electric power system that consist of one or more DER units and loads. In a normal operation, the microgrid is connected to the grid and performs operations in a synchronized mode. During any fault or maintenance event, the microgrid operates autonomously in an island mode and is able to support its own load [23]. Based on the purpose, there are two types of microgrids, utility microgrids that serves parts of the utility and industrial/commercial microgrids that serves customer facilities [24].

6) Wide Area Measurement: Wide area measurement system (WAMS) is an advanced sensing and measurement system that is continuously monitoring the health of the power grid and it obtains the system state and power quality information from the state modules based on phasor measurement units (PMUs). The PMUs utilise GPS to provide the accurate system state measurements in real time and provide time stamp for each measurement.The utility control center can obtain high resolution phase information because of the precise information by the PMUs and enables them to initiate proper response time in seconds and protect the whole wide area network from black out events. In smart grids the PMUs are installed at the distribution domains to monitor the overall power system in real time [25].

7) Distribution supervision: The main duty of the distribution supervision is to increase the visibility of the power distribution network, so that to take the proactive actions to prevent equipment failure and ensure pubic safety. The distribution supervision scope is distributed and include passive infrastructure like transmission lines, cables and branching points. Most of the overhead transmission lines in smart grid are equipped with the adequate sensors and actor nodes for continuous monitoring and preventive measures. There are also sensors used in the underground transmission lines to monitor the thermal condition and corrosion of the buried conductors. Also, some sensors are used in some cases to detect line faults and monitor nearby environment to prevent contact with vegetation [26]. For the weather conditions wireless sensors networks are used because the renewable energy sources are mainly dependent on the weather.

IV. Analysis and Discussion

To augment the qualitative comparison model in Table I, we performed memory, CPU utilization, latency and throughput tests for two of the aforementioned protocols (HTTP and MQTT). The test was executed on a Core i7 machine (4 cores, 8 threads), running Ubuntu 14.06 with 32 GB of RAM. Messages were routed via local-host (to mitigate network effects). HTTP webserver was implemented via mongoose, while MQTT service was provided via the Mosquitto broker. Stress testing for HTTP was conducted via ApacheBench and for MQTT via custom shell scripts utilising tools provided by Eclipse Mosquitto project [1]. To stress test the capability of the system acting as a data concentrator in a grid network we simulated 1000 clients sending a total of up-to one million messages. For clearance, the test failed at 2000 clients with messages exceeding half a million.

A. Results

Figure 1 represents the throughput and figure 2 represents latency of both protocols. The red line in figure 2, across x-axis is HTTP latency as it stayed below 1 ms (1 ms is the mean value across all concurrent requests, mean value per request was 27 ms.) MQTT latency fluctuated from 7 ms to 12 ms depending upon the total message load. The blue lines

[1]The tools used during the experiment are:
https://mosquitto.org/
https://github.com/cesanta/mongoose/
https://httpd.apache.org/docs/2.4/programs/ab.html.

TABLE II
TRAFFIC REQUIREMENTS FOR THE IMPORTANT SMART GRID APPLICATIONS

Application	Reference standards	Traffic characteristics	Suggested IoT Protocol	Discussion
AMR/AMI/DR	ANSI C12.19, IEEE 1377, IEC61968-9 OpenADE, OpenADR	Delay tolerant Mostly periodic/event based Small burst size Multicast/broadcast	MQTT	Consistent latency performance Better suited to telemetry Low message overhead Designed for multicast transmission Low footprint on client side
DER/Microgrid/EV	IEEE 1547.x, IEC 61850-7-420	Delay sensitive Semi-periodic/event based Multicast/broadcast	MQTT	Consistent latency performance Better suited to telemetry Low message overhead Designed for multicast transmission Low footprint on client
Substation automation	IEC 61850, DNP3/IEE1815, IEEE 1646	Extremely Delay sensitive No re-transmission Event based Reliable multicast	MQTT	MQTT QoS 3 assured delivery ensures no re-transmission
Wide area monitoring	IEEE C37.118	Delay sensitive Periodic Limited re-transmission	HTTP	Integration into area monitoring tools Varied payload support Triggers can be programmed in easily
Distribution supervision	IEEE 1451.x	Delay sensitive/tolerant Periodic/event based Random Low power consumption	HTTP	Integration into area monitoring tools Varied payload support Triggers can be programmed in easily HTTP REST API's for advanced integration i.e. Tableau for visualization Microsoft PowerBI for analysis

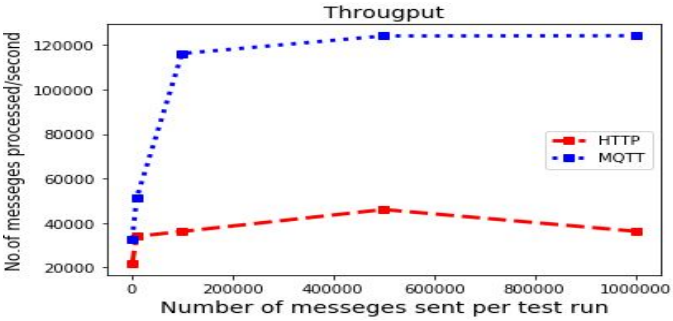

Fig. 1. Throughput

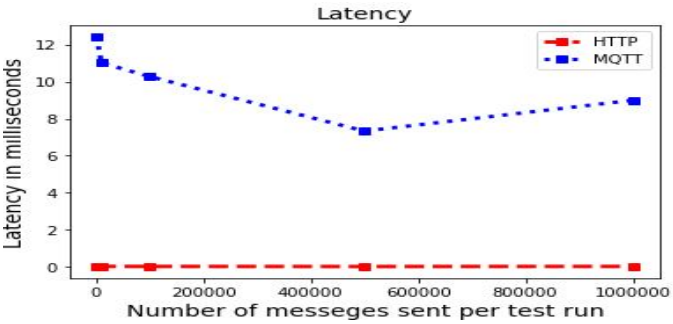

Fig. 2. Latency

in figure 1 represents throughput and we can see that MQTT offers 2-3x the throughput of HTTP. HTTP throughput was low even though it offered mean lower latency because of the deviation in results. Under stress approx. 2 percent of the requests took more than 1s to process, highest being 3 s with a standard deviation (sd) of up-to 120 ms. MQTT latency however remained relatively consistent with an sd of 3.2 ms. Figure 3 represents the time consumed to process

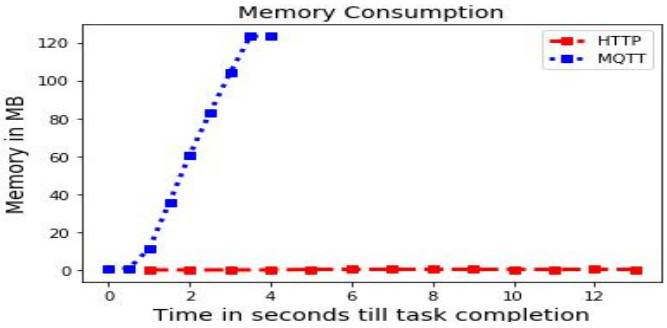

Fig. 3. Memory consumption.

one million messages from 1000 clients concurrently and the overall memory consumption. MQTT concluded the test in approx. 3.5 seconds, consuming 123 MB of RAM. The mongoose web-server performed the tests in approx 13 seconds consuming less than 1MB of RAM. Even though application design choices, purpose, features and loaded libraries will significantly affect its memory footprint, one insight that can be derived is that MQTT memory consumption increases overtime as a result of message caching at the broker. It is a design choice enforced by the protocol (broker has to maintain the list of clients, topics, and messages; Mosquitto does so via an in-memory database). Since keep-alive for HTTP was not used as each connection terminated mongoose clears the buffers resulting in significant total memory reduction. CPU utilization was 100 percent for both protocols and all test runs, hence that graph will not be included.

B. Discussion

The test results show that MQTT provides the best throughput, up to 4 times better than HTTP. While HTTP provides ten to twenty times better latency for the same load although

with a lot of disparity. MQTT broker module is less processor intensive, about four times as efficient as compared to HTTP. Reliability is much better with MQTT as well because of its intrinsic quality of service levels. While HTTP gives a significantly lower system memory footprint and easy integration into the current World Wide Web (to create Web of Things). Table II represents the smart grid traffic characteristics provided by [15]. We can now make a more informed choice towards protocol selection based on the knowledge of Section III and IV (A). The suggested IoT Protocol section of Table II offers our assessment and reasoning as to why a specific protocol would be a better choice. However, with the varied needs, requirements and compatibility with internal systems, CPU and power performance on client and server side, the final choice will always be in the hands of designers and implementers. Security (cryptography) was not included in the assessment as both rely on SSL/TLS combination. Strict security would make XMPP a contender as it enforces the use of TLS and SASL, unlike HTTP and MQTT. The analysis confirms our previous notional assessment that different protocols will reside to cater to different needs. In complex systems, like smart grids, multiple protocols will be used. CoAP does try to bring the middle ground but fails in adoption and support.

V. Conclusions and future work

The purpose of this work was to highlight the complexity of the protocol selection problem and offer more than one tool/view towards a suitable selection. The point of doing this exercise is to highlight that mere performance results or quantitative results on their own is not an optimal strategy for protocol selection. The analysis, inevitably, also highlights that there is no one-size-fits-all IoT application layer protocol. The selection comes down to a protocol that offers the least compromise in terms of features and utilization available computational capabilities of the devices. The work can further be expanded by testing more IoT protocols. Interoperability is also a big concern, especially considering that the different IoT platforms might offer different protocol support.

Acknowledgments

This work is partly supported by Academy of Finland: FIREMAN (CHIST-ERA/n. 326270), ee-IoT (n.319009) and EnergyNet Research Fellowship (n.321265/n.328869).

References

[1] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-Physical Systems and Internet of Things NIST Special Publication 1900-202 Cyber-Physical Systems and Internet of Things," 2019.

[2] M. Ullah, P. H. Nardelli, A. Wolff, and K. Smolander, "Twenty-one key factors to choose an iot platform: Theoretical framework and its applications," *arXiv preprint arXiv:2004.04924*, 2020.

[3] M. Ullah and K. Smolander, "Highlighting the Key Factors of an IoT Platform," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 901–906, 2019.

[4] M. B. Yassein, M. Q. Shatnawi, and D. Al-Zoubi, "Application layer protocols for the Internet of Things: A survey," *Proceedings - 2016 International Conference on Engineering and MIS, ICEMIS 2016*, 2016.

[5] N. Shaukat, S. M. Ali, C. A. Mehmood, B. Khan, M. Jawad, U. Farid, Z. Ullah, S. M. Anwar, and M. Majid, "A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid," *Renewable and Sustainable Energy Reviews*, vol. 81, no. April 2016, pp. 1453–1475, 2018.

[6] N. De Caro, W. Colitti, K. Steenhaut, G. Mangino, and G. Reali, "Comparison of two lightweight protocols for smartphone-based sensing," *IEEE SCVT 2013 - Proceedings of 20th IEEE Symposium on Communications and Vehicular Technology in the BeNeLux*, pp. 0–5, 2013.

[7] E. P. Frigieri, D. Mazzer, and L. F. C. G. Parreira, "M2M Protocols for Constrained Environments in the Context of IoT : A Comparison of Approaches," *XXXIII Brazilian Telecommunications Symposium (SBrT)*, no. April 2016, pp. 1–4, 2015.

[8] V. Gazis, M. Gortz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger, and E. Vasilomanolakis, "A survey of technologies for the internet of things," *IWCMC 2015 - 11th International Wireless Communications and Mobile Computing Conference*, pp. 1090–1095, 2015.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[10] Y. Chen and T. Kunz, "Performance evaluation of IoT protocols under a constrained wireless access network," *2016 International Conference on Selected Topics in Mobile and Wireless Networking, MoWNeT 2016*, 2016.

[11] P. Kayal and H. Perros, "Through a Smart Parking Implementation," *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, pp. 331–336.

[12] A. J. Jara, A. C. Olivieri, Y. Bocchi, M. Jung, W. Kastner, and A. F. Skarmeta, "Semantic Web of things: An analysis of the application semantics for the IoT moving towards the IoT convergence," *International Journal of Web and Grid Services*, vol. 10, no. 2-3, pp. 244–272, 2014.

[13] J. Dede and A. Förster, "Comparative analysis of opportunistic communication technologies," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 190, pp. 3–10, 2017.

[14] K. Khan, A. Waris, and H. Safi, "A Qualitative Comparison of Various Routing Protocols in WSN," vol. 1, no. 1, pp. 7–13, 2016.

[15] R. H. Khan and J. Y. Khan, "A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network," *Computer Networks*, vol. 57, no. 3, pp. 825–845, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2012.11.002

[16] S. K. Viswanath, C. Yuen, W. Tushar, and W.-T. Li, "SyStem DeSign of the internet of thingS for reSiDential Smart griD," *Smart Microgrids*, no. October, pp. 31–63, 2016.

[17] D. Pratikkumar, S. Amit, and A. Pramod, "Semantic Gateway as a Service architecture for IoT Interoperability," *IEEE Software*, vol. 32, no. 2, 2015.

[18] S. R. U. Kakakhel, T. Westerlund, M. Daneshtalab, Z. Zou, J. Plosila, and H. Tenhunen, "A qualitative comparison model for application layer IoT protocols," *2019 4th International Conference on Fog and Mobile Edge Computing, FMEC 2019*, pp. 210–215, 2019.

[19] P. Koponen, M. L. Pykälä, J. Peltonen, and P. Ahonen, *Interfaces of consumption metering infrastructures with the energy consumers: Review of standards*, 2010, no. 2542.

[20] G. R. Newsham and B. G. Bowker, "The effect of utility time-varying pricing and load control strategies on residential summer peak electricity use: A review," *Energy Policy*, vol. 38, no. 7, pp. 3289–3296, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.enpol.2010.01.027

[21] S. Shao, M. Pipattanasomporn, and S. Rahman, "Grid integration of electric vehicles and demand response with customer choice," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 543–550, 2012.

[22] IEEE, "IEEE standards for electric power systems communication and distribution."

[23] K. Benjamin, L. Robert, I. Toshifumi, and M. Satoshi, "Making the MicroGrid," no. june, pp. 54–65, 2008.

[24] B. Kroposki, T. Basso, and R. DeBlasio, "Microgrid standards and technologies," *IEEE Power and Energy Society 2008 General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*, 2008.

[25] A. Naumann, P. Komarnicki, M. Powalko, Z. A. Styczynski, J. Blumschein, and M. Kereit, "Experience with PMUs in industrial distribution networks," *IEEE PES General Meeting, PES 2010*, pp. 1–6, 2010.

[26] M. Erol-Kantarci and H. T. Mouftah, "Wireless multimedia sensor and actor networks for the next generation power grid," *Ad Hoc Networks*, vol. 9, no. 4, pp. 542–551, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2010.08.005