Survey: Classification of the IoT Technologies for Better Selection to Real Use

Peter Kaňuch, Dominik Macko, and Ladislav Hudec
Faculty of Informatics and Information Technologies
Slovak University of Technology
Bratislava, Slovakia
Email: peter.kanuch@stuba.sk, dominik.macko@stuba.sk, ladislav.hudec@stuba.sk

***Abstract*—Nowadays, more and more devices are connected to the Internet labeled as the Internet of Things (IoT). They are used everywhere and anytime to improve our everyday life and make processes easier. In our work, we specify the term of IoT for better understanding. These systems are usually powered by batteries, which is critical to power consumption. Each team, researcher or expert should consider it while designing the new application or solution for uses in the area of the Internet of Things. Therefore, we provide a brief survey and introduce the classifications for IoT technologies, specifically IoT devices and processors, communication technologies, and security protocols used in such networks. We focused primarily on power consumption, and according to that, we specified rules or criteria for a better selection of the related technology. In the end, we described the application of the IoT solution into real life in the area of healthcare.**

***Keywords*—classifications; energy-efficiency; Internet of Things; IoT technologies; recommendations**

I. Introduction

The use of the term Internet of Things (IoT) increases rapidly in recent years [1]. So far, the content was created by people on the Internet, but the time is limited. There was a space for the area of IoT, where pieces of information from real life can be and will be created by devices and sensors connected to them [2]. There are many applications and use cases for IoT, which should meet some requirements and criteria. Two of the most important criteria are mobility and wireless. Therefore, these devices are usually powered by batteries with the ability to switch into the energy-efficiency state (power down, idle mode) in case of inactivity [3]. The next requirements for IoT devices are energy-efficiency, security, scalability of systems in terms of high growth, applicability or interoperability with/in embedded system, diversity of systems for different applications, cost, etc. [4].

Despite using IoT device everywhere, there are still some challenges for IoT itself or for new communication technology 5G which should bring a lot of possibilities for connecting a lot of smart devices. Between common IoT challenges belong Privacy and Security, Usability, Cost, Energy consumption, Scalability, Interoperability, Data and device management, or for 5G network: very dense crowd people, high data rate, mobility, multi-homing, device discovery, interference and others [5]–[8].

This paper is focused mainly on the classification of IoT technologies. There are some existing classifications based on different IoT requirements or criteria. For example, classifications of wireless IoT technologies classified according to distance, bandwidth, or power consumption [9]–[12], categorizations of IoT security protocols [7], [13]–[17], or at least classifications of the IoT device itself [18]. Nevertheless, all these classifications should be concentrated in one place. By this brief survey, we suppose we can help many IoT developers, designers, and researchers to better selection of desirable IoT device, technology, or protocol.

This survey introduced the areas with IoT applications in Sec. II, classifications of IoT devices (Sec. III-A, III-B, III-C), the power consumption of security protocols in Sec. III-D, criteria, and recommendations on how to choose IoT device or technology (Sec. IV), and classification of IoT in the area of healthcare.

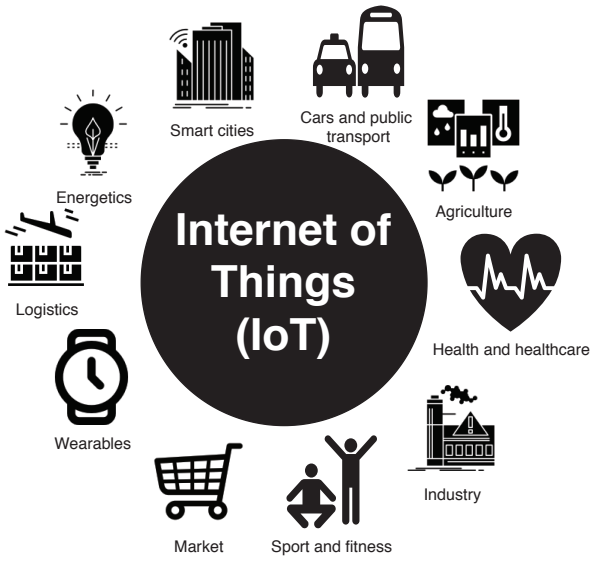

Fig. 1. The areas of IoT use.

This work was partly supported by the Ministry of Education, Science, Research and Sport of the Slovak Republic (Incentives for Research and Development, Grant No.: 2018/14427:1-26C0), the Eset Research Centre, and the Slovak University of Technology.

This is an accepted version of the paper:
P. Kaňuch, D. Macko and L. Hudec, "Survey: Classification of the IoT technologies for better selection to real use," in 2020 43nd International Conference on Telecommunications and Signal Processing (TSP), 2020, pp. 500-505.
doi: 10.1109/TSP49548.2020.9163480
URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9163480

II. The Areas of IoT Applications

There are some definitions of IoT. In recent years, smartwatches, wearable electronics, and smart homes have become popular between people, and it is the most common answer once you are asking about IoT [19] [20]. It is a set of ubiquitous devices, which are connected and communicated by the Internet. Moreover, they connect virtual and real-life [21]. The IoT is a combination of two words, the first one, "Internet", meaning communication and interconnection, and the second one "things", meaning everything around us. So we can use them in everyday life (see Fig. 1).

Agriculture and industry - by using IoT devices in the area of industry or agriculture, a lot of processes can be automated, which will make human work easier. A typical example is a field air condition monitoring.

Logistics - analysis of collected data from IoT sensors makes it easier to plan the transport of goods or truck road or to monitor the stock levels in the warehouse. Thanks to that, we can save the driver time, fuel, and environment pollution at all.

Sport and fitness - using wearable electronics, the sports centers can better determine the usage of individual equipment and sports gears. People can also use it to monitor vital functions, and it helps to achieve better performance.

Healthcare - IoT devices are used in hospitals and medical applications too. They control a patient's medical condition.

III. Classification of IoT Technologies

Nowadays, there are several manufacturers of IoT devices, standards, or proprietary solutions of wireless communications technologies and security protocols to secure communication or the device itself. The whole IoT solution, consisting of equipment, communication technology, and security protocol, should meet the requirements as much as possible. The following subsections are focused on the classification of IoT devices, communication technologies, and security protocols.

A. Classification of IoT Devices

As mentioned, a lot of IoT device manufacturer exists. We decided to divide them into three main categories (see Fig. 2):

- Devices without operating system, containing firmware for device operation. Despite the name, classification also concludes devices, which can contain some operating systems, but it is not accessible by the end-user and often do not support classical services and calls of the operating systems.
- Devices with an operating system, for more complex systems (an example provided in Fig. 2).
- Closed solutions, where IoT devices communicate only with the server (cloud) provided by the manufacturer.

Every device from each category can be used for a variety of purposes and applications in any area of life. Therefore we can divide them according to it [18]:

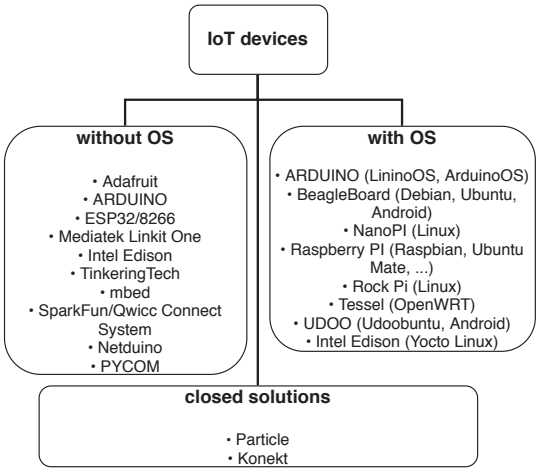

Fig. 2. Classification of IoT devices.

1) Sensors - devices that measure physical values using a variety of connected sensors and convert them into a digital signal.
2) Actuators - devices that can change/control action and interfere with real life.
3) Hybrids - combining both groups of devices.

The third possible classification is according to the controller unit:

1) devices with micro-controller - Intel Quark (Intel Edison), ATmega (TinkeringTech, Arduino).
2) devices with microprocessor - Tensilica Xtensa (Adafruit huzzah32, ESP, SparkFun/Qwicc Connect System), Intel Atom (Intel Edison), ARM Cortex-M (Adafruit Feather, UDOO, mbed, Netduino) and ARM Cortex-A (BeagleBoard, NanoPi, Raspberry Pi, Rock Pi, UDOO, Mediatek Linkit One).

These three classifications are in coexistence. For sensors or actuators, which often perform only a simple action (e.g., temperature measurement) at regular intervals, we can use devices without an operating system (OS) and with a simple energy-efficiency micro-controller. For devices belonging to hybrids, it is necessary to use something more complex, as they mostly carry out several processes simultaneously. Microprocessor devices support the operating system versions shown in Fig. 2. Even non-OS devices support various programming languages (C / C ++, Python, Lua, Shell, Node.js, Javascript, etc.) and environments for development and programming. We separate the closed solutions into a special category as most of them support only manufacturer-specified technologies and communicate directly with the manufacturer's server application in the cloud. There is an application interface created.

B. Classification of Communication Technologies

Wireless communication technologies are classified into three main groups by most of the researches [9]–[12]:

- according to range/distance - from close personal distance to WAN (wide area network),

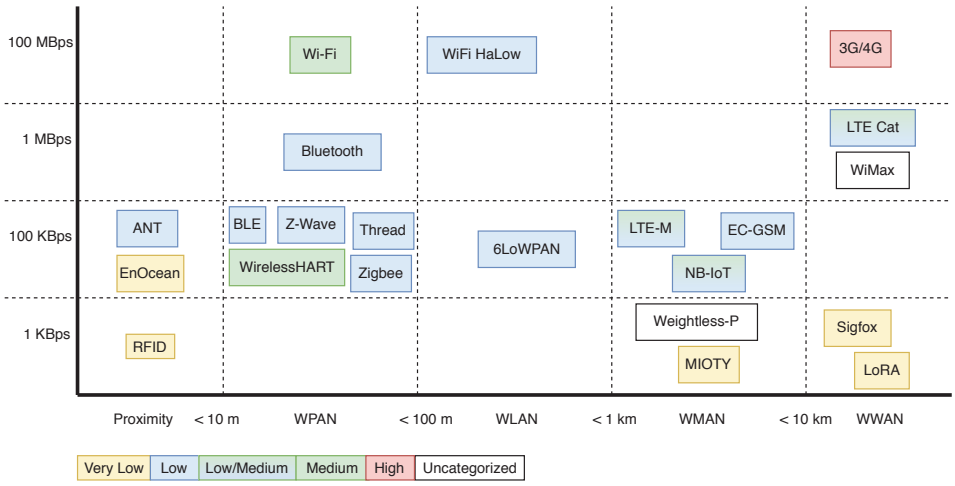

Fig. 3. Classification of communication technologies.

- by bandwidth from 1 KBps - 100 MBps,
- according to energy-efficiency - from very low to high.

Projecting all three types of classification into one (Fig. 3) will allow us to make easier choices with a view to overall energy performance. For each distance and data throughput, we can identify the most economical technology.

It also implies that the most economical technologies can transmit the least data. With higher transfer rates, the energy intensity is increasing gradually.

C. Classification of Security Protocols

There are several security protocols used in computer networks for securing communication. They are intended to maintain the security features known or labeled as CIA (**C**onfidentiality, **I**ntegrity, **A**vailability), which can be achieved by authorization, authentication, encryption [13]–[16].

In addition to the new protocols, many existing ones are tailored to the IoT area to meet the needs of these devices as much as possible.

These protocols can be classified, for example, by key distribution [7], into two main branches - symmetric and asymmetric. The difference is that symmetrical has a certain secret agreed before the actual communication. Shared secrets can be generated stochastically, meaning randomly or deterministically by an algorithm. Asymmetric schemes use shared secret negotiation methods using asymmetric encryption, or public key or also certificate encryption is used.

The other classification of security protocols is based on the appropriate layer of the OSI (Open Systems Interconnection) model or IoT stack [17]. We mentioned a few of them in Table I.

It is crucial to determine and classified the security protocols according to power consumption because of different use. Therefore in the next section, we introduced some of them and their energy-efficiency.

D. Energy-Efficiency of Security Protocols

a) Datagram Transport Layer Security (DTLS): secures data over the datagram (UDP protocol) against interception and fake messages [25]. The power analysis of DTLS is provided in Table II. The research work [22] included values measured during session establishment with the related protocols. In [23], the power consumption of the encryption, hash computation, and certificate parsing was measured.

b) Host Identity Protocol: (HIP) using HIP security associations creates an end to end communication link supporting changes to the IP address [26]. The power comparison of some HIP variants is provided in Table III. In [27], the session establishment consisting of communication and computation cost is measured and compared.

c) Internet Key Exchange (IKE/IKEv2): consists of several protocols that operate over UDP protocol, provides authentication and creation of the security associations SA [30]. The power analysis of IKEv2 is provided in Table IV.

d) Internet Protocol Security (IPSec): provides CIA security features for the packet on the network layer, also provides encryption, decryption, and authentication [10]. The

TABLE I. CLASSIFICATION BASED ON THE LAYER OF THE OSI MODEL OR IOT STACK

Layer	Protocol
Transport	HIP, DTLS, PANA/EAP, IKE
Network	IPSec, RPL security
Datalink	IEEE 802.15.4 security

TABLE II. OVERVIEW OF DTLS POWER CONSUMPTION

Protocol	Power consumption
DTLS Handshake Energy + Preamble Sampling Protocols [22]	$\leq$ 30 mJ
DTLS Handshake Energy + Beacon-Enabled IEEE 802.15.4 Networks [22]	4 - 5,5 mJ
DTLS Handshake Energy + 802.15.4 RSA key (2048b) [23]	579 mJ
DTLS Handshake Energy + 2048-bit key [24]	487,8 mJ

power analysis of IPSec portions is provided in Table V.

IV. IoT Technologies Selection

It is really important to ensure that the requirements are met as much as possible while designing the IoT system. The following text summarizes the rules for IoT technologies selection.

A. The Rules for Processor Selection

There are several rules or criteria [33], [34], that each team (experts) should consider during the selection of a processor for an embedded system (IoT device), depending on the application for which the system is intended. We can divide these rules into two large groups, according to some recommendations. Mandatory one - criteria to be considered in each case:

1) Computing power - for each processor, it is necessary to analyze the computational tasks that the system will process to avoid overloading. It is also necessary to realize that the amount of processed data may increase several times in the future.
2) Interrupt subsystem - the importance of fast response to interruptions.
3) Good hardware support for individual technologies such as virtualization, floating-point, vector and matrix operations, segmenting, paging, multi-user, or multi-processor systems.
4) Power consumption, in particular, the possibility of switching to an energy-efficiency state.
5) Cost related to its development (e.g., the experience of the designer and his team, etc.)

Optional one:

1) Operating system support for the processor type.
2) Code inheritance - the ability to reuse existing code on a given device.
3) Manufacturer support - support for the system in the future.
4) Mines - Eliminate known errors by the manufacturer.

For choosing the right microprocessor, it is also important to choose a suitable operating system. We may be interested in criteria such as processor support, debug mode, OS services (queues, semaphores, monitors), performance, designer experience, software components, drivers, standards compatibility, technical support, source code, and customization options, license, and others.

TABLE III. Overview of HIP Power Consumption

Protocol	Power consumption
Standard HIP [27]	142,901 mJ
HIP-BEX [27]	221,44 mJ
C-HIP [27]	110,808 mJ
Ben-Saied et al. [27]	97,98 mJ
D-HIP [27]	101,76 mJ
D-HIP (2) [28]	48,9 mJ
CD-HIP [27]	67,09 mJ
OpenHIP [27]	130 mJ
E-HIP [29]	104 mJ

TABLE IV. Overview of IKE/IKEv2 Power Consumption [31]

Protocol	Power consumption
IKEv2 (16/32/64 B of data)	0,02/0,04/0,06 mJ
IKEv2 + IPSec AH (16/32/64 B of data)	0,07/0,09/1,02 mJ
IKEv2 + IPSec ESP (16/32/64 B of data)	0,24/0,30/0,44 mJ

TABLE V. Overview of IPSec Power Consumption [32]

Protocol	Power consumption
IPSec - Authentication (Transmit/Receive)	357,3/154,65 mJ
IPSec - Key exchange	36,91 mJ
IPSec - SA creation (Transmit/Receive)	362,4/154 mJ

B. The Rules for Communication Technology Selection

Similarly, there are some rules for communication technology selection [35]:

1) Standardization - it is related to technologies used by users. Also, it is a good practice developed solution that is multi-platform.
2) Functional range (transmitted power, antenna gain, free space loss, data transmission rate, etc.).
3) Geographic relevance - or geographic position is related to standardization. There can be unequal network coverage and the frequency band used in each country. It is good practice to know the deployment site in advance.
4) Data considerations (data flow) - some technologies do not allow two-way or bidirectional communication, which may be sufficient in use with sensor devices.
5) Private/public networks - network design, customization, and configuration options need to be considered during the designing phase. It can be quite expensive for private networks.
6) Chip (Hardware) providers - some technologies are supplied only by a single manufacturer, which can lead to several issues during the life of IoT devices (e.g., price increases, manufacturer bankrupt).
7) Cost - also related to network services.
8) Energy-efficiency.

C. The Rules for Security Protocol Selection

All security protocols meet some of the security requirements. The main difference is in the security strength and in the appropriate layer of the OSI model, on which data are secured.

From these requirements, some rules for security protocol selection results. Each expert should:

- identify assets and vulnerable data,
- identify data on the appropriate layer of the OSI model,
- analyze the security features of the protocol,
- analyze the strength level of the protocol,
- identify power consumption,
- analyze hardware, and software support for cryptography mechanisms.

V. IoT Solution in Real Life

As we mentioned in Sec. II, IoT is everywhere, and billions of devices are connected to the Internet [36]. The number of

cyber-attacks increases too, and the device should be secured as best as possible, which can be a challenge considering power consumption. Therefore, it is necessary to take care of the system's power consumption as a whole solution, not only individually during micro-controller / microprocessor, communication technology, or security protocol selection.

In our research, we focus on the optimization of security protocol, and the following things are the right motivation for us to get the best results. It is:

- application of IoT devices in life,
- maximizing device battery life,
- minimizing the energy requirements of the security protocol,
- maintaining security features.

A. Health and Healthcare

Healthcare are one of the largest areas of life, requiring a high level of security and reliability. There are still some challenges like limitations of IoT devices regarding power consumption, diversity of devices and protocols used, mobility, etc. [37]. According to the classification in Sec. III-A, we can classify devices used in this area to sensors, which are monitoring a patient's medical condition, and actuators, which can set individual values of the devices and affect the patient's treatment procedure. According to locality or distance:

1) devices used within the medical room,
2) devices used within hospitals,
3) mobile devices used within an ambulance, or remote use within the home treatment.

The selection of the communication protocol strongly depends on application use, which bandwidth with distance do we need. By the mentioned classification, we can easily choose more efficient technology, e.g., some protocols from the group signed as low. In our research [29], we used Bluetooth v4. We know that a lower data rate can save some energy, too. We also used the Raspberry Pi. By classification in Section III-A and recommendation in Sec. IV, we can choose one, which will meet our requirement to energy-efficiency much better.

VI. Conclusion

As we mentioned, the number of connected devices to the Internet of Things increased in recent years. There are still some challenges in that area of interest. One of them is power consumption since the devices are usually powered by batteries. In our work, we introduced brief classifications for IoT devices and technologies regarding energy-efficiency. It will help us to make better decisions during the selection of the related technology in our next research aimed to optimize security protocols for uses in the IoT area. It can also be used by other researchers and architecture designers to systematically select appropriate devices and technologies for their real use cases.

References

[1] J. Morgan, "A simple explanation of'the internet of things'," *Retrieved November*, vol. 20, p. 2015, 2014.

[2] "Internet of Things (IoT)," https://www.techopedia.com/definition/28247/internet-of-things-iot, accessed: 2018-02-19.

[3] K. Sandoval, "OAuth 2.0 – Why It's Vital to IoT Security," https://nordicapis.com/why-oauth-2-0-is-vital-to-iot-security/, accessed: 2018-02-19.

[4] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)," in *International Conference on Network Security and Applications*. Springer, 2010, pp. 420–429.

[5] M. Fiorani, P. Monti, B. Skubic, J. Mårtensson, L. Valcarenghi, P. Castoldi, and L. Wosinska, "Challenges for 5g transport networks," in *2014 IEEE international conference on advanced networks and telecommuncations systems (ANTS)*. IEEE, 2014, pp. 1–6.

[6] M. Noura and R. Nordin, "A survey on interference management for device-to-device (d2d) communication and its challenges in 5g networks," *Journal of Network and Computer Applications*, vol. 71, pp. 130–150, 2016.

[7] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the internet of things," *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.

[8] K. K. Patel, S. M. Patel *et al.*, "Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science and computing*, vol. 6, no. 5, 2016.

[9] "Comprehensive and visual classification of wireless iot protocols and network technologies," https://www.i-scoop.eu/internet-of-things-guide/wireless-iot-protocols-technologies/, accessed: 2019-19-20.

[10] "An overview of protocols involved in internet of things devices and applications. help clarify with iot layer technology stack and head-to-head comparisons." https://www.postscapes.com/internet-of-things-protocols/, accessed: 2019-19-20.

[11] M. S. Mahmoud and A. A. Mohamad, "A study of efficient power consumption wireless communication techniques/modules for internet of things (iot) applications," 2016.

[12] M. R. Mallick, "A comparative study of wireless protocols with li-fi technology: A survey," in *43rd IRF International Conference*, 2016, pp. 8–12.

[13] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of things: a definition & taxonomy," in *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. IEEE, 2015, pp. 72–77.

[14] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring data security issues and solutions in cloud computing," *Procedia Computer Science*, vol. 125, pp. 691–697, 2018.

[15] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of things security: Layered classification of attacks and possible countermeasures," *Electronic Journal of Information Technology*, no. 9, 2016.

[16] D. M. Mendez, I. Papapanagiotou, and B. Yang, "Internet of things: Survey on security and privacy," *arXiv preprint arXiv:1707.01879*, 2017.

[17] P. K. Misra, L. Mottola, S. Raza, S. Duquennoy, N. Tsiftes, J. Hoglund, and T. Voigt, "Supporting cyber-physical systems with wireless sensor networks: An outlook of software and services," *Journal of the Indian Institute of Science*, vol. 93, no. 3, pp. 463–486, 2013.

[18] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, "Comparison of iot platform architectures: A field study based on a reference architecture," in *2016 Cloudification of the Internet of Things (CIoT)*. IEEE, 2016, pp. 1–6.

[19] "5 things people still don't understand about iot," https://www.iotforall.com/5-things-people-dont-understand-about-iot/, accessed: 2020-05-20.

[20] "5 ways the internet of things will affect your daily life," https://www.ics.ie/news/view/1729, accessed: 2020-05-20.

[21] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the internet of things," *Cluster of European Research Projects on the Internet of Things, European Commision*, vol. 3, no. 3, pp. 34–36, 2010.

[22] M. Vučinić, B. Tourancheau, T. Watteyne, F. Rousseau, A. Duda, R. Guizzetti, and L. Damon, "Dtls performance in duty-cycled networks," in *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on*. IEEE, 2015, pp. 1333–1338.

[23] T. Kothmayr, W. Hu, C. Schmitt, M. Bruenig, and G. Carle, "Poster: Securing the internet of things with dtls," in *Proceedings of the 9th ACM*

Conference on Embedded Networked Sensor Systems. ACM, 2011, pp. 345–346.

[24] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[25] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," Internet Requests for Comments, RFC Editor, RFC 6347, January 2012, http://www.rfc-editor.org/rfc/rfc6347.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6347.txt

[26] R. Moskowitz, T. Heer, P. Jokela, and T. Henderson, "Host identity protocol version 2 (hipv2)," Internet Requests for Comments, RFC Editor, RFC 7401, April 2015, http://www.rfc-editor.org/rfc/rfc7401.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7401.txt

[27] S. Sahraoui and A. Bilami, "Efficient hip-based approach to ensure lightweight end-to-end security in the internet of things," *Comput. Netw.*, vol. 91, no. C, pp. 26–45, Nov. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2015.08.002

[28] Y. Ben Saied and A. Olivereau, "(k, n) threshold distributed key exchange for hip based internet of things," in *Proceedings of the 10th ACM international symposium on Mobility management and wireless access*. ACM, 2012, pp. 79–86.

[29] P. Kaňuch and D. Macko, "E-hip: An energy-efficient openhip-based security in internet of things networks," *Sensors*, vol. 19, no. 22, p. 4921, 2019.

[30] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Rfc 5996-internet key exchange protocol version 2 (ikev2)," 2010.

[31] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6lowpan with compressed ipsec," in *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*. IEEE, 2011, pp. 1–8.

[32] R. Karri and P. Mishra, "Optimizing ipsec for energy-efficient secure wireless sessions," in *System-level power optimization for wireless multimedia communication*. Springer, 2002, pp. 133–152.

[33] A. Bhavsar, "A guide for selecting the right microcontroller for your iot project," https://iiot-world.com/connected-industry/a-guide-for-selecting-the-right-microcontroller-for-your-iot-project/, accessed: 2019-11-27.

[34] A. Gerber, "Choosing the best hardware for your next iot project," https://developer.ibm.com/articles/iot-lp101-best-hardware-devices-iot-project/, accessed: 2019-11-27.

[35] D. Oxlee, "Iot communication protocols: choosing the right one for you," Issued by Little Black Book PR for Sebata Holdings, https://www.itweb.co.za/content/5yONP7EEONb7XWrb, 2018, accessed: 2019-11-27.

[36] T. Alam, "A reliable communication framework and its use in internet of things (iot)," *International Journal of Scientific Research in Computer Science, Engi-neering and Information Technology (IJSRCSEIT), ISSN*, pp. 2456–3307, 2018.

[37] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.