The Internet of Things – A survey on technologies and protocols

Zhihao Cao

Abstract

The term “Internet of Things” has been more and more popular in recent years. Especially, many simulation videos of applications of IoT technology gives us full of expectation for it. Indeed, the idea of IoT started from 1999 by Kevin Ashton, but yet the IoT is still upon us. There many reasons that stalls the IoT come to our life. For the major one is a standard IoT architecture has not yet been clearly defined. Other issues are the defining of protocols for objects, transmission, security and etc. To accelerate the speed of deploying IoT, we need more effort from research groups and developers to solve problems and find solutions. In this paper, the concept of IoT with some applications in daily life and different aspects of analysis will be presented. Then, the technologies of IoT that connect heterogeneous smart objects and bring into Internet will be explored. Finally, the protocols of IoT that support different applications working reliably and meet specific requirements will be introduced.

Keywords

Internet of Things (IoT), Technology, Smart building, Smart homes, IoT protocol, M2M, RFID, NFC, V2V0, TinyOS, LiteOS, Riot OS, Contiki, CoAP, DDS, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST, mDNS, DNS-SD, RPL, 6LoWPAN, EPCglobal, IEEE 802.15.4, LTE-A, Z-Wave.

Introduction

In the latest century, human being civilization has gained extraordinary progress which has exceeded the amount of achievements of the history since human being civilization began. The reason why such big change has been done is human’s intelligence is released due to the evolvement of politics. Since then, civilization revolutions reshaped the world time and time again. Now, we are living in an era that dominated by IT technologies. Especially, the Internet technology brings information online so that everyone is able to get it easily. This technology is such significant that allow everyone to be much more knowledgeable than before. Because of it, tons of inventions are came out and people’s live changes tremendously. All of these are in fact improving the efficiency of people’s life and business. Due to the need, people come out an idea that can help us gathering information and making decisions. This is what so many researchers are working on and the thing that are going to reshape the world again - the Internet of Things (IoT).

This idea basically means connecting physical objects to the Internet so that we can get the information from these objects and make decision efficiently or we have some program to make the decision automatically. An example of this idea is the smart building. There are many such physical objects (sensors) that are set to detect the condition of heating, ventilation, AC, lighting, etc. So that, these components can be operated in efficiently.

To enable the IoT works, many kind of sensors are needed to “hear” and “see” the environment, and they share the information and make coordinate decisions to perform the jobs. In another word, The IoT allows things to have intelligence to know the environment and make decisions.

Due to the IoT is able to transform the things to be intelligent and efficient, people have high expectation on how IoT can benefit the quality of life and the world economy. For example, the smart homes will open the door for you when you arrive home. It will open lights up for you when you enter the home, turn on the AC in a comfortable temperature, tell you what food is in the refrigerator and what can be made by these food and remind you when your favorite TV shows is going to begin. Or when you are in outside, it will notify you over the smartphone that who is knocking in the front door. The technologies to achieve these functions are already exist, but so far, they are basically functioning separately. To achieve the goal that have them connected with each other and make cooperate decision, more specific technologies and services are needed. And the standardized protocols are needed to solve the incompatibility between heterogeneous things.

Since the IoT will be integrated into Internet, the Internet architecture needs to be evolved to fit the IoT. The traditional Internet architecture is built based on the need of Web services. Therefore, the heterogeneous objects of IoT are hardly to just fit in the current Internet architecture. By 2010, the number of objects that connected by the Internet exceeds the human being population ([3] D. Evans). So, considering the growing deployment of IoT, a sufficient address field protocol should be applied.

Privacy and security are two crucial issues to deal with before IoT starts blossoming for the market. Due to the Internet is going to penetrate into every aspect of our life, more privacy and sensitive information will be collected into the Internet. More seriously, objects which is connected into Internet might be controlled by hackers. Therefore, these issues will cause disasters if there is no fine solution for them.

The objective of this paper is to deliver the extensive idea of IoT, the technology beneath the IoT and the protocols support the IoT.

The rest of the paper is organized as follows: Section 2 describes the technologies to realize the IoT. Section 3 provides an overview of Internet protocols that support the IoT. Finally, Section 4 present a conclusion based on the previous section.

2 Technologies

In this paper, the technologies will be classified into hardware and software.

2.1 Hardware

In IoT, the hardware should be able to connect the heterogeneous objects together. The special requirement is that the power consumption should be low under the lossy and noisy links circumstances.

2.1.1 Radio Frequency identification (RFID)

RFID is the earliest technology that applied to realize the Machine to Machine (M2M) communication. RFID system is composed of RFID tags and readers. The tag is a chip or label that contains object's identity. The reader is used to communicate with the tag by sending a query and receives response from the tag. RFID is able to perform real-time monitoring.

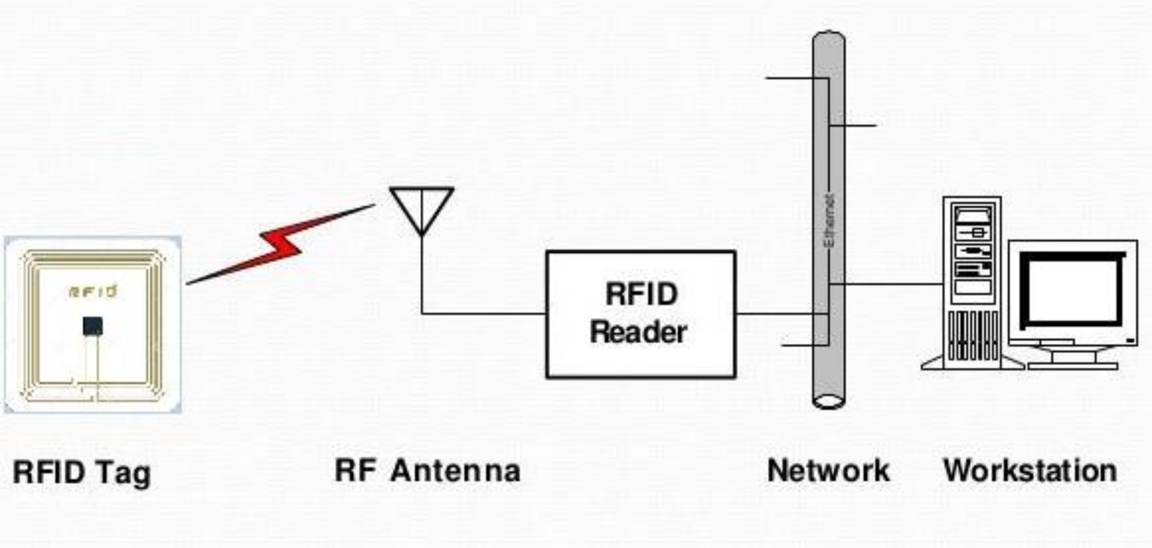

Figure 1 RFID system

RFID tag is a microchip with an antenna as the figure 1 shown. The tag will not only return the identity, it also return some additional information back to RFID reader. The size of RFID Tag can be extremely small. A tag with dimensions 0.4*0.4*0.15 mm has been developed by Hitachi ([19] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo).

RFID tag is designed into three types: active, passive and semi-passive/active. Active tag is powered by battery; Passive tag doesn't need the power; Semi-passive/active tag use board's power when it comes in the proximity of the reader. The transmission range of the RFID system is approximately from 1-2000 feet up to the environment. The transmission frequency is spanning from low frequencies at 123-135 KHz up to ultra-high frequencies at 860-960 MHz.

Identification is very important for the IoT to name and match services. RFID tag applies the Electronic Product Code (EPC) as its identity and data type. The EPC is a unique identification number which is stored inside the RFID tag. The use of EPC for the

RFID is acknowledged as promising technique for the IoT. The reason is that its scalability and reliability fit the primary requirement of IoT.

2.1.2 Near Field Communication (NFC)

NFC is built on the basis of RFID technology. Technically, it is a specialized subset within the family of RFID technology. This technology has been widely applied on smart phone which offers a secure and reliable communication between the smart phone and object.

NFC is a branch of High-Frequency RFID, and it operates at the 13.56 MHz frequency. The approximate effective range of NFC is 20 cm. However, the range is mainly up to the use of antenna in the device ([8] VILMOS, A.; MEDAGLIA, C. M; MORONI).

The benefit of applying NFC is that its small communicate range can avoid the attacker or sniffer and it does not need the paring step comparing to the Bluetooth technology. With these quality, the most typically application of NFC is the mart phone payment.

2.1.3 Machine-to-machine communication (M2M)

M2M is the technology that allow the communication between electronic devices such as sensors, embedded systems and mobile devices. M2M is becoming more and more widely used communication technology. In 2011, the U.S. traffic monitoring of a cellular network showed 250% increased for M2M traffic. By 2022, based on the prediction, M2M traffic flows will occupy 45% of the net Internet traffic. ([3] D. Evans)

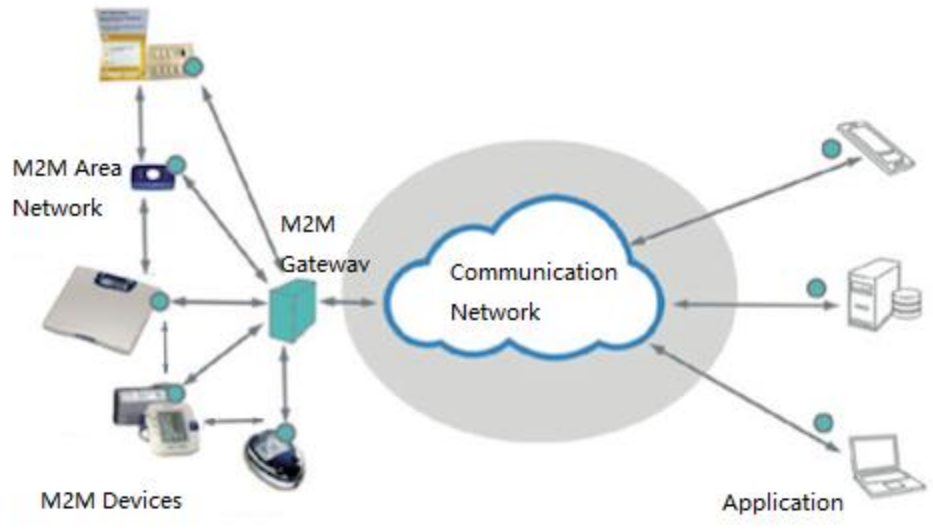

Figure 2 M2M architecture

As the figure 2 shown, the operation of M2M technology can be divided into five parts: ([20] ETSI)

- M2M Devices
  Devices within the M2M Area Network that are able to send or query data.
- M2M Area Network
  Provide connectivity between M2M devices and Gateways.
- M2M Gateway
  Allow M2M devices inter-cooperate with each other and provide the connection to Communication Network.
- M2M Communication Network
  Provide the communication between M2M Gateway and M2M application.
- M2M Application
  Provide the interfaces to control or monitor the M2M devices. Meanwhile, the middleware layer will take use of the data from M2M devices to go through different kind of applications.

The M2M technology is applied in many area such as transportation system, smart building, smart homes, smart grids, manufacturing, urban facilities and especially in health care that it enables the real-time monitoring for patients in anytime, anywhere.

2.2 Software

Software are necessary to provide IoT functionalities. Any software applications are built based on the Operating System, so the OS plays the crucial part on the software area of IoT. Many Real-Time Operating Systems (RTOS) are designed to fit the big market of IoT. For example, the TinyOS, LiteOS and Riot OS offer light weight OS designed for IoT environments. The popular OS is Contiki RTOS because it offer a simulator called Cooja. It is a software that are used to simulate and emulate IoT and Wireless Sensor Network (WSN) applications ([21] Ala A, Mohsen G., Mehdi M., Mohammed A., Moussa A.).

Operating System	Language	Minimum Memory	Event-based programming	Multi-threading	Dynamic Memory
TinyOS	nesC	1 KB	Y	Partial	Y
LiteOS	C	4 KB	Y	Y	Y
RiotOS	C/C++	1.5 KB	N	Y	Y
Contiki	C	2 KB	Y	Y	Y

Table 1 shows the popular Operating Systems used in IoT.

3 Protocols

As the idea of IoT is to connect heterogeneous smart objects to Internet, the need of IoT common standards is extraordinary. Many IoT standards have been proposed by researcher and organizations to facilitate and simplify the difficulty of development and maintenance. The groups with most contribution to IoT such as World Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF), they provide practical and reliable protocols that currently supporting the operation of the IoT.

In this paper, these protocols is categorized into 3 group: Application protocols, Service Discovery protocols and Infrastructure protocols.

<table>
<tr><td>Application Protocol</td><td>CoAP</td><td>DDS</td><td colspan="2">AMQP</td><td>MQTT</td><td>MQT
T-SN</td><td>XMPP</td><td>HTTP REST</td></tr>
<tr><td>Service Discovery</td><td colspan="4">mDNS</td><td colspan="4">DNS-SD</td></tr>
<tr><td rowspan="4">Infrastructure Protocols</td><td>Routing Protocol</td><td colspan="7">RPL</td></tr>
<tr><td>Network Layer</td><td colspan="4">6LoWPAN</td><td colspan="3">IPv4/IPv6</td></tr>
<tr><td>Link Layer</td><td colspan="7">IEEE 802.15.4</td></tr>
<tr><td>Physical Layer</td><td colspan="2">LTE-A</td><td>EPCglobal</td><td colspan="2">IEEE 802.15.4</td><td colspan="2">Z-Wave</td></tr>
</table>

Constrained Application Protocol (CoAP)

The constrained application protocol is an application layer protocol that designed by IETF for the constrained-resource devices. It defines a web transfer protocol based on REpresentational State Transfer (REST) on top of HTTP functionalities and it is interoperable with HTTP. REST represents a simpler way to exchange data between clients and servers over HTTP. ([15] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, M. Dohler)

CoAP changes some HTTP functionalities so that it meets the IoT requirements such as low power consumption and functioning under lossy and noisy links. Thus, the objective of CoAP is to support tiny devices with low power, computation and communication capabilities to utilize RESTful interactions.

CoAP is binding to UDP so that the overall implementation is lightweight. To meet the reliability, CoAP owns some features. In the header, the message type and Quality of Service are represented in two bits. The message types are:

1. Confirmable: message that requires ACK.
2. Non-confirmable: message that does not need ACK.
3. Acknowledgement: to confirm the message is received.
4. Reset: the message cannot be read.

Besides, to achieve the reliability, a Stop-and Wait transmission method is used to transmit the messages with 16 bits header field that contains Message ID. Therefore, the message transmission is un-duplicates.

CoAP has Datagram Transport Layer Security (DTLS) to protect the message. DTLS is a security protocol that runs on the top of UDP. It offers authentication, data integrity, confidentiality, automatic key management, and cryptographic algorithms ([14] Thamer A. Alghamdi, Aboubaker Lasebae, Mahdi Aiash).

Message Queue Telemetry Transport (MQTT)

Message Queue Telemetry Transport is designed for M2M communications and was introduced by IBM in 1999 and was standardized in 2013 at OASIS ([16] D. Locke). It is an application layer protocol that runs on top of TCP. It is a publish/subscribe protocol which does not need clients to request updates, so the network bandwidth resources are saved and the computational resources is less needed.

MQTT consists of three components: subscriber, publisher, and broker. A target device is registered as a subscriber for specific topics. When the publishers publish topics of targets, the subscriber will be notified by the broker. In addition, the security is achieved by the broker to validate authorization of the publishers and the subscribers ([17] U. Hunkeler, H. L. Truong, and A. Stanford-Clark).

The features of MQTT would be the sparingly usage of the bandwidth and battery. MQTT ensures reliability by providing three QoS levels:

1. Fire and forget: Send a message once, no require of the ACK.
2. Delivered at least once: Send a message at least once, require the ACK.
3. Delivered exactly once: Use four-way handshake mechanism to make sure the message is exactly delivered once.

Despite the MATT is running on top of TCP, it is designed to be low overhead comparing with other TCP-based protocols ([18] Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, Colin Keng-Yan Tan). Because of the publish/subscribe architecture, it is more preferable than most of other protocols for the IoT.

Extensible Messaging and Presence Protocol (XMPP)

XMPP is used for multi-party chatting, voice and video calling and telepresence. It allows users to communicate with each other by sending instant messages on the Internet no matter which operating system they are using. The protocol allow the instant message to achieve authentication, access control, privacy measurement, hop-by-hop and end-to-end encryption, and compatibility with other protocols. Since XMPP has been standardized over fifteen years ago, this protocol has been widely applied in the Internet. Due to the fact that it fail to support the new application data, Google already stopped supporting the XMPP standard.

XMPP is an asynchronous publish/subscribe application layer protocol that runs on TCP. It also support synchronous request/response messaging systems. Due to the use of small message footprint and low latency message exchange, it provides near real-time communication ([22] S. Bendel, T. pringer, D. Schuster, A. Schill, R. Ackermann, M. Ameling). As the protocol name mentioned, XMPP is extensible and its functionality can be increased by the specification of XMPP Extension Protocols (XEP).

Due to the less support of QoS, this protocol is impractical for M2M communications. This drawback only can be remedied by the inherited mechanisms of TCP. In addition, XMPP uses XML messages so that it causes more computation due to the tags. In the other hand, the support of publish/subscribe architecture actually make it more suitable for the IoT comparing to CoAP.

Advanced Message Queuing Protocol (AMQP)

Advanced Message Queuing Protocol is an open standard application layer protocol for the IoT. AMQP focuses on message-oriented environments. It supports reliable communication via message delivery guarantee primitives.

AMQP defines two types of messages: 1) bare message: supplied by the sender. 2) Annotated message: seen by the receiver. The header of the message contain three parts: frame header, extended header, and frame body. The header contain parameters including priority, time to live, durability, first acquirer, and deliver count. [26]

Data Distribution Service (DDS)

DDS is a publish/subscribe architecture application layer protocol that designed for real-time M2M communications. In contrast to other publish/subscribe application layer protocols such as MQTT or AMQP, DDS relies on a broker-less architecture and uses multicasting to bring excellent Quality of Service (QoS) and high reliability to its applications. DDS's broker-less publish/subscribe architecture suites well to read-time constraints for IoT and M2M communications. [27]

DDS defines two layers:

Data Centric publish/subscribe (DCPS): to delivery information to subscribers.

Data Local Reconstruction layer (DLRL): is served as interface to DCPS functionalities.

3.2 Service Discovery Protocols

Multicast DNS (mDNS)

mDNS is such a service that can perform the task of unicast DNS server. mDNS is flexible due to the fact that the DNS namespace is used locally without extra expenses or configuration. mDNS is an appropriate choice for embedded internet-based devices due to these three reasons: ([28] S. Cheshire and M. Krochmal)

- There is no need for manual reconfiguration or extra administration to manage devices
- It is able to run without infrastructure
- It is able to continue working if failure of infrastructure happens.

DNS Service Discovery (DNS-SD)

The pairing function of required services by clients using mDNS is called DNS-based service discovery (DNS-SD). Using this protocol, clients can discover a set of desired services in a specific network by employing standard DNS messages. DNS-SD like mDNS, is part of the zero configuration aids to connect machines without external administration or configuration.

3.3 Infrastructure Protocols

Routing Protocol for Low Power and Lossy Networks (RPL)

The IETF aimed to standardize a link independent routing protocol based on IPv6 for resource-constrained devices. RPL is designed to support minimal routing requirements through building a robust topology over lossy links. This routing protocol supports simple and complex traffic models like point-to-point, point-to-multipoint, and multipoint-to-point.

PRL uses a Destination Oriented Directed Acyclic Graph (DODAG) to represent the routing diagram of nodes. Each node in the DODAG is aware of its parents but they have no information of their children. For this diagram, RPL keeps at least one path for each node to the root and preferred parent to pursue a faster path to increase performance ([23] T. Clausen, U. Herberg, and M. Philipp).

Low power Wireless Personal Area Networks (6LowPAN)

Low power Wireless Personal Area Networks is the specification of mapping services required by the IPv6 over Low power WPANs to maintain an IPv6 network. ([6] M. R. Palattella et al.) The standard provides header compression to reduce the transmission overhead, fragmentation to meet the IPv6 Maximum Transmission Unit (MTU) requirement, and forwarding to link-layer to support multi-hop delivery ([7] J. W. Hui and D. E. Culler). To meet the requirement of the IoT, 6LowPAN removes many IPv6 overheads in such a way that a small IPv6 datagram can be sent over a single hop in the best case.

IEEE 802.15.4

The IEEE 802.15.4 protocol was designed to specify a sub-layer for Medium Access Control (MAC) and a physical layer (PHY) for low-rate wireless private area network ([24] LR-WPAN). Due to its specifications such as low power consumption, low data rate, low cost, and high message throughput, it also is utilized by the IoT, M2M, and WSNs. It provides a reliable communication, operability on different platforms, and can handle a large number of nodes. It also provides a high level of security, encryption and authentication services.

LTE-A

Long Term Evolution - Advanced encompasses a set of cellular communication protocols that fit well for machine-Type Communications (MTC) and IoT infrastructures especially for smart cities where long term durability of infrastructure is expected. ([4]

M. Hasan, E. Hossain, and D. Niyato) Moreover, it outperforms other cellular solutions in terms of service cost and scalability.

At the physical layer, LTE-A uses orthogonal frequency division multiple access (OFDMA). LTE-A also employs a multiple-component carrier (CC) spread spectrum technique that allows having up to five 20-MHz bands.

The architecture of LTE-A network relies on two essential parts. The first one is the Core Network (CN) which controls mobile devices and deals with IP packet flows. The other part is the Radio Access Network (RAN) which handles wireless communication and radio access and establishes user plane and control plane protocols.

EPC-global

EPC-global just like EPC as previous introduced. It is a unique identification number which is stored on an RFID tag and is used basically in the supply chain management to identify items. The underlying architecture uses Internet based RFID technologies along with cheap RFID tags and readers to share product information. The specification of this technology is introduced in the section 2.1.1 (RFID). This architecture is recognized as a promising technique for the future of the IoT because of its openness, scalability, interoperability and reliability beyond its support to the primary IoT requirements such as objects IDs and service discovery ([25] E. C. Jones and C. A. Chung).

Z-Wave

Z-Wave, known as a low-power wireless communication protocol for Home Automation Networks (HAN), has been used widely in the remote control applications in smart homes as well as small-size commercial domains. Z-Wave convers about 30 meters point-to-point communication and is specified for applications that need tiny data transmission like light control, household appliance control, smart energy and HVAC, access control, wearable health care control, and fire detection ([29] C. Gomez and J. Paradells).

In its architecture, there are controller and slave nodes. Controllers manage the slaves by sending commands to them. For routing purposes, a controller keeps a table of the whole network topology. Routing in this protocol is performed by source routing method in which a controller submits the path inside a packet.

Conclusion

The world is changing much faster than ever before, but with the IoT come to our life, it is going to be even faster. IoT technologies will be applied into any aspect of our life and help us to improve the efficiency, quality and decisions. With so much benefits the IoT can bring to us, we should give more effort on researching this technology and solve the downside problems which is one of the major reason that blocks it from being widely applied.

In this paper, I have presented the concept of IoT with some applications in daily life and different aspects of analysis, the technologies of IoT that connect heterogeneous smart objects and bring into Internet, and the protocols of IoT that support different applications working reliably and meet specific requirements.

References

1. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: a survey. Computer Networks, v. 54, n. 15, p. 2787 – 2805, 2010. ISSN 1389-1286. DOI.10.1016/J.COMNET.2010.05.010.
2. MEDAGLIA, Carlo Maria et al. Services, Use Cases and Future Challenges for Near Field Communication. In: THE STOLPAN PROJECT, DEPLOYING RFID CHALLENGES, SOLUTIONS, AND OPEN ISSUES, DR. CRISTINA TURCU (ED.). 2011. Retrieved May 30, 2013.
3. D. Evans, “The Internet of things: How the next evolution of the Internet is changing everything,”CISCO, San Jose,CA, USA,White Paper, 2011.
4. M. Hasan, E. Hossain, and D. Niyato, “Random access for machineto-machine communication in LTE-Advanced networks: Issues and approaches,” IEEE Commun. Mag., vol. 51, no. 6, pp. 86–93, Jun. 2013.
5. IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802. 15. 4-2011, 2011.
6. M. R. Palattella et al., “Standardized protocol stack for the Internet of (important) things,” IEEE Commun. Surveys Tuts, vol. 15, no. 3, pp. 1389–1406, 3rd Quart. 2013.
7. J. W. Hui and D. E. Culler, “Extending IP to low-power, wireless personal area networks,” IEEE Internet Comput., vol. 12, no. 4, pp. 37–45, Jul.Aug. 2008.
8. VILMOS, A.; MEDAGLIA, C. M; MORONI, A. NFC Technology and its application Scenarios in a future of IOT. STOLPAN Project, 2011.
9. NFC. Near Field Communication, Security Concerns with NFC Technology. 2013. Retrieved May 14, 2013.
10. DYE, S. Machine-to-Machine Communications. 2008. Retrieved March 28, 2008.
11. Shinho Lee, Hyeonwoo Kim, Dong-kweon Hong, Hongtaek Ju, Correlation Analysis of MQTT Loss and Delay According to QoS Level, International Conference on Information Networking (ICOIN), 28-30 Jan. 2013, pp. 714-717.
12. Sven Bendel, Thomas pringer, Daniel Schuster, Alexander Schill, Ralf Ackermann, Michael Ameling, A Service Infrastructure for the Internet of Things based on XMPP, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 18-22 March 2013, pp. 385-388.

13. Bipin Upadhyaya, Ying Zou, Hua Xiao, Joanna Ng, Alex Lau, Migration of SOAPbased Services to RESTful Services, 13th IEEE International Symposium on Web Systems Evolution (WSE), 30 Sept. 2011, pp. 105-114.
14. Thamer A. Alghamdi, Aboubaker Lasebae, Mahdi Aiash, Security Analysis of the Constrained Application Protocol in the Internet of Things, Second International Conference on Future Generation Communication Technology (FGCT), 12-14 Nov. 2013, pp. 163-168.
15. Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, Mischa Dohler, Standardized Protocol Stack for the Internet of (Important) Things, Communications Surveys & Tutorials IEEE 15(3), 2013, pp. 1389-1406.
16. D. Locke, “MQ telemetry transport (MQTT) v3. 1 protocol specification,” IBM developerWorks, Markham, ON, Canada, Tech. Lib., 2010.
17. U. Hunkeler, H. L. Truong, and A. Stanford-Clark, “MQTT-S—A publish/subscribe protocol for wireless sensor networks,” in Proc. 3rd Int. Conf. COMSWARE, 2008, pp. 791–798.
18. Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, Colin Keng-Yan Tan, Performance Evaluation of MQTT and CoAP via a Common Middleware, IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 21-24 April 2014, pp. 1-6.
19. ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: a survey. Computer Networks, v. 54, n. 15, p. 2787 – 2805, 2010. ISSN 1389-1286. DOI.10.1016/J.COMNET.2010.05.010.
20. ETSI. European Telecommunications Standards Institute. 2013. Retrieved May 14, 2013, from <http://www.etsi.org>.
21. Ala A, M. Guizani, M. Mohammadi, Mohammed A, M. Aledhari, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015
22. S. Bendel, T. pringer, D. Schuster, A. Schill, R. Ackermann, M. Ameling, A Service Infrastructure for the Internet of Things based on XMPP, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 18-22 March 2013, pp. 385-388.
23. T. Clausen, U. Herberg, and M. Philipp, “A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL),” in Proc. IEEE 7th Int. Conf. WiMob, 2011, pp. 365–372.
24. IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802. 15. 4-2011, 2011.
25. E. C. Jones and C. A. Chung, RFID and Auto-ID in Planning and Logistics: A Practical Guide for Military UID Applications. Boca Raton, FL, USA: CRC Press, 2011.

26. “OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0,” Adv. Open Std. Inf. Soc. (OASIS), Burlington, MA, USA, 2012.
27. Data distribution services specification, V1.2, Object Manage. Group (OMG), Needham, MA, USA, Apr. 2, 2015.
28. S. Cheshire and M. Krochmal, “Multicast DNS,” Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6762, 2013.
29. C. Gomez and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” IEEE Commun. Mag., vol. 48, no. 6, pp. 92–101, Jun. 2010.