Internet of Things Communication Reference Model

Adel H. Alhamedi
VŠB-Technical University of Ostrava
Ostrava - Czech Republic
ade0004@vsb.cz

Hamoud M. Aldosari
VŠB-Technical University of Ostrava
Ostrava - Czech Republic
mub0002@vsb.cz

Vaclav Snasel
VŠB-Technical University of Ostrava
Ostrava - Czech Republic
vaclav.snasel@vsb.cz

Ajith Abraham
VŠB-Technical University of Ostrava
Ostrava - Czech Republic
ajith.abraham@ieee.org

***Abstract*— The model we propose in this paper takes its roots from the OSI (ISO 1984) model, the TCP/IP model (US DoD4 1970), and the Internet model, but it puts its focus on *Internet of Things* (IoT) specific features and issues. All the previous models have a great value, going beyond any discussion, but simply they have not been conceived with the IoT issues and features in mind. IoT may need more than a computer network communication model! We developed a new model compatible with the prospects of IoT. It should also be noted that there are efforts in recent years to produce a new reference model for communications to keep pace with the world of Internet for everything. The most prominent of these attempts are produced by the IoT Architecture project (IoT-A 2013), which seems appropriate, but we further propose additions and modifications in this paper.**

Keywords- Internet of Things (IoT); IoT Architecture project; IoT Architectural Reference Model; IoT Communication Reference Model.

I. INTRODUCTION

It is no secret that there is a rapid global trend and growing with days towards the *Internet of Things (IoT)* and at all levels of government and commercial. Even the regular user now feels pleasure of technology after he was feel fear from it in the past. But it is strange that most of them do not realize the sheer scale of the challenges facing this trend! Thus placing a burden too big on the shoulders of researchers and developers. So we have to be prepared from this moment for this transition and radical changes in everything around us. Where should for all sciences, knowledge, and disciplines cooperate among each other to transform our lives easily and safely to *Internet for Everything* [2].

So we are facing a new field called the *Next Generation of Internet*, which is a very fertile area for scientific research because the supply are very few compared to what is needed (demand). The term "IoT" was initially used by Kevin Ashton in 1999, and became of widespread use thanks to the work of the Auto-ID Centre. However, the definition was not given at that time, and although there's a general agreement that IoT involves objects and connectivity, the precise wording is still to be found [3]. We provide a definition of IoT from our vision and point of view.

***Internet of Things (IoT)*:** Is the integration of *objects* with the world of Internet, by adding hardware or/and software to be smart and so be able to *communicate* with each other and participate effectively in all aspects of daily life.

The Internet of Things (IoT) in very simple and short meaning is the communication *'communicate'* between objects. '*Objects'* are we and all around us (physical or virtual!) so cannot be limited and are also heterogeneous. We urgently need to find or develop a reference model for communication between these heterogeneous objects to coexist with each other to reach the goal of the Internet of Things (IoT). The current models (like OSI and TCP/IP) are outdated and may not meet this new trend and growing needs. For all this, we need a new model to be a common ground among those *objects* and enable them to communicate with each other regardless of its nature. This simply is the subject of this article.

A. OSI and TCP/IP

We begin with a quick historical perspective on the current reference models, which are now considered outdated. One of the most important communication concepts to understand our paper is the Open Systems Interconnect (OSI) reference model and other models [4, 5].

When networks first came into being, computers could usually communicate only with computers from the same manufacturer. In the late 1970s, the Open Systems Interconnection (OSI) reference model was created by the International Organization for Standardization (ISO) to break through this barrier. This conceptual model, created in 1978 and revised in 1984, describes a network architecture that enables data to be passed between computer systems in seven layers. As shown in *Table 1*, the OSI reference model is built, bottom to top, in the following order: physical, data link, network, transport, session, presentation, and application. The physical layer is classified as Layer 1, and the top layer of the model, the application layer, is Layer 7.

OSI Layer	Major Function
Application (Layer 7)	Provides access to the network for applications.
Presentation (Layer 6)	Translates data from the format used by applications into one that can be transmitted across the network. Handles encryption and decryption of data. Provides compression and decompression functionality. Formats data from the application layer into a format that can be sent over the network.
Session (Layer 5)	Synchronizes the data exchange between applications on separate devices.
Transport (Layer 4)	Provides connection services between the sending and receiving devices and ensures reliable data delivery. Manages flow control through buffering or windowing. Provides segmentation, error checking, and service identification.
Network (Layer 3)	Handles the discovery of destination systems and addressing. Provides the mechanism by which data can be passed and routed from one network system to another.
Data link (Layer 2)	Provides error detection and correction. Uses two distinct sub-layers: the Media Access Control (MAC) and Logical Link Control (LLC) layers. Identifies the method by which media are accessed. Defines hardware addressing through the MAC sub-layer.
Physical (Layer 1)	Defines the physical structure of the network and the topology.

TABLE I. OSI MODEL SUMMARY

OSI Stack	TCP/IP DoD4	Internet
Application	Process	Application
Presentation		
Session		
Transport	Host to Host	Transport
Network	Internet	IP
Data Link	Network Access	Link
Physical		

TABLE II. TCP/IP AND INTERNET LAYERS SUITE IN RELATIONSHIP TO THE OSI REFERENCE MODEL

The OSI model does a fantastic job to outline how networking should occur and the responsibility of each layer. Unfortunately, TCP/IP predates this model in 1970 and has to perform the same functionality with only four layers. *Table 2* shows how these four layers line up with the seven layers of the OSI model. The Network Access layer is sometimes referred to as the Network Interface or Link layer and this is where Ethernet, FDDI, or any other physical technology can run. TCP/IP model is commonly nowadays known as Internet model with some changes in the layers names and its functions to suit with the Internet network and its job.

II. NEW TRENDS IN IOT COMMUNICATION MODELS

A. IoT Architecture Reference Model (IoT-ARM) [1]

IoT Architecture Project (IoT-A). IoT-A is a project funded by the European Union and conducted between 2010 and 2013. More than 50 scientists and researchers contributed to the development of an *"Architectural Reference Model" (ARM)* for the Internet of Things.

The Internet of Things concept has evolved rapidly in recent years. But past solutions in these years can still be seen as island solutions, implementing some sort of "INTRAnet of Things" rather than an "INTERnet of Things". After much discussion about the core concepts of the IoT for several years, a group of researchers joined forces to lay the foundation for the much needed common ground or a common "architecture" for the Internet of Things: the IoT Architecture project (IoT-A) was born. IoT-A has created an *"Architectural Reference Model" (IoT ARM)* as the common ground architecture for the Internet of Things. One of the most important achievements and output component of this project is create IoT Communication Reference Model, which is basically the starting point for this paper. We discuss this model in the next sub-section as an input to proposed model.

B. IoT-A Communication Reference Model [1]

IoT-A team decided to work on the Internet model (TCP/IP model) and its 4 layers to develop it to suit IoT environment and with OSI model as a guide. This model is not able to address the interoperability issues between heterogeneous objects; like security and quality of service etc. But this model can be layered on top of one another with our vision to form a new model. The IoT-A model is illustrated in *Figure 1* and functions of each layer are as follows:

Physical aspect: This interoperability aspect concerns the physical characteristics of the communication technologies used in the system. It is similar to the OSI Physical Layer.

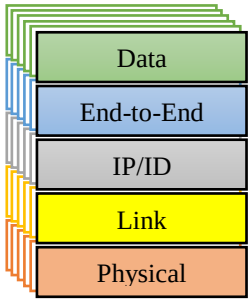

Figure 1. IoT-A Communication Reference Model and its Complexity Layers.

Link aspect: In order to address the heterogeneousness of networking technologies represented in the IoT field, the Link aspect requires special attention. In fact, most networks implement similar, but customized communication schemes and security solutions.

Network and ID aspect: This interoperability aspect combines two communication aspects: networking, which provides the same functionalities as the correspondent OSI layer; and identifiers, which are provided using resolution functionalities between locators and IDs.

End-to-end aspect: this aspect takes care of reliability, transport issues, translation functionalities, proxies/gateways support and parameter configuration when the communication crosses different networking environments. By providing additional interoperability aspects on top of those of the Network and ID aspect, this aspect provides the final component for achieving a global M2M communication model.

Data aspect: the topmost aspect of the IoT Communication Model is related to data definitions and transfers. The purpose of this aspect is to model data exchange between any two actors in the IoT.

C. *IoT Challenges*

We try to refer briefly to the most important challenges facing the Internet of Things, which is a source of inspiration to the idea of this paper: *Common Standards, Security Issues, and Quality of service (QoS).*

Common Standards: It is expected that the IoT will encompass different types of objects. These Objects will belong to different field networks and operate using different networking standards. In addition, these objects and networks will be expected inter-operate with each other [6]. The reader may think at first glance that we want to demonstrate that we need to create a special model for each class of *objects* of Internet of Things. On the contrary, we believe that we should create one common standard model and only one. Even do not fall into mistakes of the past and take the advantages of common standards. The current models are no longer sufficient for the world of Internet of things. Additional functionality for each layer of the previous models will not solve the problem, but would complicate matters more and more.

Figure 1 also illustrates how the model could become complicated if we faced all the challenges by adding a function for a layer from the model. It would be perfect if each layer from the model has its clear function or set of coordinated functions (not complex) at most. In the following Section we discuss about the rest of challenges faced by our new model *IoT Communication Reference Model*.

III. IoT Communication Reference Model

We propose the IoT Communication Reference Model with the prospects of IoT and its challenges in mind. The challenges that will need to be addressed when building IoT Communication Reference Model are include dealing with the security and quality of communication (quality of service) between objects.

A. *Additions and modifications*

Security Issues. The OSI security architecture reference model (ISO 7498-2) as illustrated in *Table 3* is also designed around seven layers (based on OSI reference model ISO 7498-1) [7, 8]. Although the security needs are well-recognized in traditional internet domain, it is still not fully understood how existing security protocols and architectures can be deployed in IoT [9]. If we want to apply this model for security of Internet of Things IoT, there must be protective measures at each layer in the OSI reference model like traditional networks! Taking into consideration that the Security Issues in IoT much larger, please see Figure 2 [7, 8].

OSI Layers (ISO 7498-1) Security Model (ISO 7498-2)

Application	Authentication
Presentation	Access Control
Session	Non-Repudiation
Transport	Data Integrity
Network	Confidentiality
Data Link	Assurance / Availability
Physical	Notarization / Signature

TABLE III. SECURITY MODEL

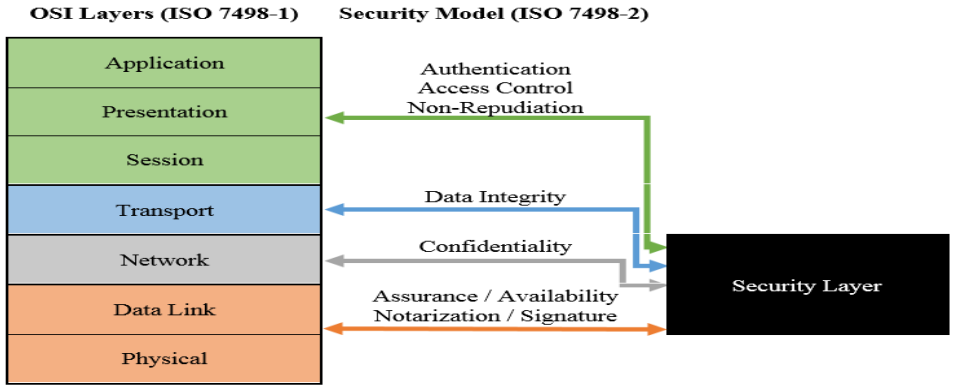

Figure 2. Security steps at each layer from OSI model.

It's time to create a separate layer specializing in Security Issues and add it to the model directly without needing for another model for security. We need to build solutions for all Security Issues in a single layer; which make Security Issues simpler and more powerful at the same time.

Quality of Service (QoS). The second issue that should take care of it in IoT is the Quality of Service (QoS). According to Cisco, Cisco's Internet Business Solutions Group (IBSG) predicts some 25 billion devices will be connected by 2015, and 50 billion by 2020 [10]. IoT will connects billions of objects to exchange information among them, the traffic and storages in the internet will also increase in an exponential way. Thus, any new proposed model for IoT needs to address many factors like QoS [11]. Of course, information explosion will happen in our world but probably in the presence of the same infrastructure! This requires extra attention for that issue. Unfortunately, with this significant increase there are no guarantees for the Quality of Service because *Objects* can have very different Quality of Service (QoS) requirements and working on many diverse protocols and a huge number of applications [12]. This means for example, a threat to human life if we talk about the Internet of Things in the field of medicine. The Quality of Service would then become more important than ever.

It's time to create a separate layer specializing in Quality of Service and add it to the model directly without distribution its functions on the different layers of the traditional model.

B. *New Communication Reference Model*

Basically, a reference model in IoT is a conceptual blueprint of how communications should take place. It describes how data and network information are communicated from an application on one *object* through the network media to an application on another *object*. It addresses all the processes required for effective communication and divides these processes into logical groupings called *layers*. There is no doubt that one of the most important processes or layers (which was distributed to layers and not a separate layer in the past) are the Security layer and Quality of Service layer. *Figure 3* illustrates the new model with two proposed layers; *Security layer* and *Quality of Service layer*.

Security layer in proposed model comes in logically arrangement between Link layer and Quality of Service layer for two reasons: First the data transmitted between source and destination through upper layers' devices. Second it is the most sensitive place in security vulnerabilities. We want to create an independent entity, which meets all security issues instead of dispersion quotient where the security process distributed over layers. One layer also could reduce various security steps, which are made at the level of the model's layers and makes it centered in a single layer. *This layer play the role of plug wall impervious to face any risks and walking with data wherever it go; which mean create a self-firewall in each frame of data; not per network nor per object but per frame (then we will achieve the ideal security).*

Quality of Service layer in the proposed model comes in logically arrangement between Security layer and Physical layer for this reason: To be the last process executed before sending data. In other words, to be the first process executed in receiving object; to be recognized the importance of data and how to handle it efficiently.

The IoT Communication Reference Model is hierarchical, and the same benefits and advantages can apply to any layered model. The primary purpose of all such models, especially in Internet of Things, is to allow different *objects* from different vendors with different nature to interoperate in environment of Internet. Advantages of using this model include, but are not limited to, the following:

- ✓ The model combines the Security processes into simpler and powerful layer, thus aiding security development at all levels.
- ✓ The model combines the Quality of Service processes into one layer, thus helping to attention by Quality of Service more than the past.
- ✓ These two lightweight layers are feasible to be run on small things (small objects: which owns Minimum CPU, memory, and energy depending on the budget and its role).

C. *Security Scenario from End-to-End*

IoT not only faces the traditional security risks in TCP/IP network, but also faces the new emerging risks. In recent years, there have been many discussions about the IoT security but some discussions just put forward the shortage of IoT mechanism and the others just provide strategic analysis [13]. In addition, users and a lot of specialists are more concerned about security issues in IoT; which may lead them to resist change rather than support it. We can apply everything from techniques that has been reached in the issue of security but in the same layer as a powerful shield. But there is an important question needs to be answered when talking on the security layer proposed by us. What the behavior of security layer with different objects, which operate on different layers and during the trip of data from transmitter to receiver? For a traditional scenario of communication from End-to-End [14, 15] please see *Figure 4*. We can classify objects to:

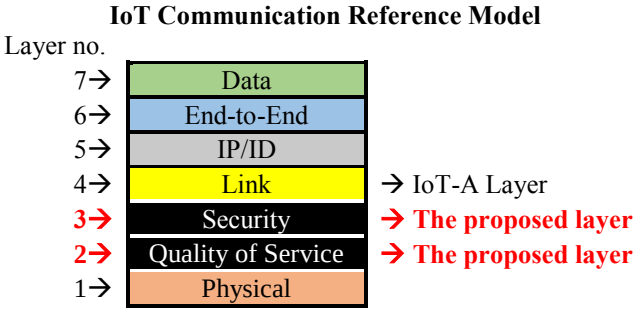

Figure 3. Proposed Model.

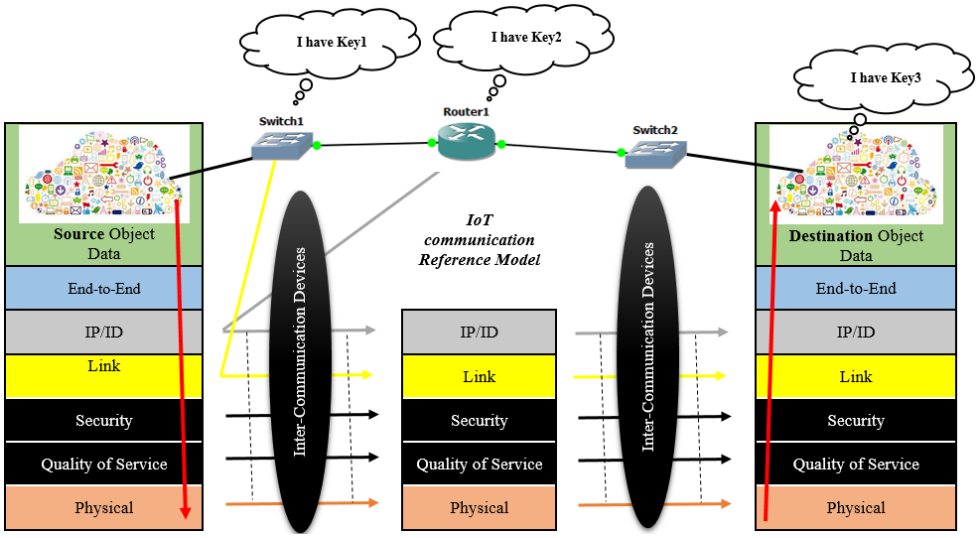

Figure 4. Security scenario from End-to-End.

1) Original Objects: Source and Destination of data.
2) Mediator Objects: IoT Inter-Communication devices. For example: Switch (Layer 2 device) and Router (Layer 3 device) etc.

Assume that this layer has what will called "Keys Chain". Keys Chain consists of: key1, key2, and key3. Key1 means; you have a permission to access to the fourth layer (link layer). Key2 means; you have a permission to access to the fifth layer (IP/ID layer). Key3 means; you have a permission to access to the upper layer [16] as illustrated in *Figure 4*.

For more protection you may construct objects required for all of these keys to access to upper layer and add some other security tools such as encryption to protect the remaining data from other objects, which does not have the rights of access. We should study the functions of that layer with more concentration. Does the concentration of security issues in a single layer will have a new dimension? This may cause a radical change in security issues.

D. Quality of Service Scenario from End-to-End

A fundamental concept in QoS is that quality of service' processes are performed at multiple layers of the OSI model to identify the traffic that is to be treated differently (either preferentially or differentially) [17]. Meanwhile, in Internet of Things the requirements of QoS must be guaranteed in all layers, which requires that all layers must come to the same comprehension to the requirements of QoS [18]. Moreover users in the past were waiting long minutes for internet services response but today users can no longer wait for fractions of a second [19]. So we deeply need to address it in a single layer. One of the nice advantages for one layer for QoS is the decreasing of a lot of coordination between layers during the implementation of QoS processes. We should study the functions of that layer with more concentration. For example: Is it appropriate with the Internet of Things to classified traffic to sixteen different type of classification like Quality of Service today?

But why this layer is the lower layer? Simply because this layer will determine the method of dealing with data, and its information do not constitute a security threat. As an advice we must not forget that we are heading to smart cities. In spite of various benefits participatory sensing brings along, there are tremendous research challenges when applying to the real life [20].

IV. CONCLUSIONS

This paper proposed a new IoT Communication Reference Model with the vision of communications “anytime, anywhere, anyone, and anything” [21]. The IoT Communication Reference Model is built, bottom to top, in the following order: Physical, Quality of Service, Security, Link, IP/ID, End-to-End, and Data. The two new layers: Quality of Service layer is classified as Layer 2 and the Security layer is classified as Layer 3. Advantages of using this model include, but are not limited to, the following:

- ✓ The model combines the Security processes into simpler and powerful layer, thus aiding security development at all levels.
- ✓ The model combines the Quality of Service processes into one layer, thus helping to attention by Quality of Service more than the past.
- ✓ These two lightweight layers are feasible to be run on small things (small objects: which owns Minimum CPU, memory, and energy depending on the budget and its role).

REFERENCES

[1] Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob van Kranenburg, Sebastian Lange, Stefan Meissner, Editors: Enabling Things to Talk, Designing IoT solutions with the IoT Architectural Reference Model. Springer Heidelberg New York Dordrecht London (2013).

[2] Cisco Internet of Everything (IoE), http://internetofeverything.cisco.com/

[3] Rob van Kranenburg, Alex Bassi: IoT Challenges. Van Kranenburg and Bassi Communications in Mobile Computing, SpringerOpen Journal (2012).

[4] Emmett Dulaney, Mike Harwood, Editors: CompTIA Network+ N10-005 Authorized (Fourth Edition). Pearson, Exam Cram (2012).

[5] Todd Lammle, Editor: CompTIA Network+ Study Guide (Second Edition). Sybex (2012).

[6] Oladayo Bello, Sherali Zeadally: Communication Issues in the Internet of Things (IoT) Springer-Verlag, London (2013).

[7] Glenn Surman: Understanding Security Using the OSI Model. SANS Institute InfoSec Reading Room (2002).

[8] Anton: Security and the OSI Model. Essays24.com (2010).

[9] Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S. Kumar, KlausWehrle, Security Challenges in the IP-based Internet of Things, Wireless Personal Communications: An International Journal, Volume 61 Issue 3, pp. 527-542, 2011.

[10] Cisco Internet Business Solutions Group, http://www.cisco.com/web/about/ac79/index.html .

[11] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, Shahid Khan, Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. IEEE 10th International Conference on Frontiers of Information Technology, pp. 257 – 260, (2012).

[12] Chong Han, Josep Miquel Jornet, Etimad Fadel, Ian F. Akyildiz: A cross-layer communication module for the Internet of Things. Computer Networks 57 (2013) 622–633 (2012).

[13] Xue Yang, Zhihua Li, Zhenmin Geng, and Haitao Zhang, Editors: A Multi-layer Security Model for Internet of Things. IOT Workshop Springer-Verlag Berlin Heidelberg (2012).

[14] Jeff Doyle, Editor: CCIE Professional Development, Routing TCP/IP, Volume I. CiscoPress (1998).

[15] Jeff Doyle, Jennifer DeHaven Carroll, Editors: CCIE Professional Development, Routing TCP/IP, Volume II. CiscoPress (2011).

[16] Emmett Dulaney, Editor: CompTIA Security+ Study Guide (Fifth Edition). Sybex (2011).

[17] Tim Szigeti, Christina Hattingh, Editors: End-to-End QoS Network Design Quality of Service in LANs, WANs, and VPNs. Cisco Press (2005).

[18] Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung, The Internet of Things: Vision & Challenges. IEEE 2013 Tencon, pp. 218-222, (2013).

[19] Jianbin Wei, Cheng-Zhong Xu, Measuring Client-Perceived Pageview Response Time of Internet Services. IEEE Transactions on Parallel and Distributed systems, 22 (5), 773-785, (2011).

[20] Ren Duan, Xiaojiang Chen, Tianzhang Xing, A QoS Architecture for IOT, International Conference on Internet of Things (iThings/CPSCom) and 4th International Conference on Cyber, Physical and Social Computing, pp. 717 - 720, (2011).

[21] Jiong Jin, Jayavardhana Gubbi, Tie Luo, Marimuthu Palaniswami, Network Architecture and QoS Issues in the Internet of Things for a Smart City. International Symposium on Communications and Information Technologies (ISCIT), pp. 956-961, (2012).