# Network Access Control for the IoT: A Comparison Between Cellular, Wi-Fi and LoRaWAN

Shanay Behrad, Stéphane Tuffin, Emmanuel Bertin
Orange Labs
France
{shanay.behrad, stephane.tuffin, emmanuel.bertin}@orange.com

Noel Crespi
Institut Mines-Telecom, Telecom SudParis, CNRS 5157,
France
noel.crespi@it-sudparis.eu

***Abstract*— The IoT (Internet of Things) is expected to encounter new business trends like wholesale wireless connectivity, due to the emergence of new user demands. These new business trends and demands will have a major effect on the entire IoT system and on the associated security needs. In this paper, we study the necessity of providing a new AC (access control) framework for IoT through a comparison of the AC architectures in the different communication technologies that are currently in operation for IoT. We consider cellular, Wi-Fi and LoRaWAN networks and their compatibility with the wholesale wireless connectivity concept.**

***Keywords— IoT; Access control; Wholesale wireless connectivity; Cellular systems; Wi-Fi; LoRaWAN;***

## I. INTRODUCTION

The IoT (Internet of Things) refers to billions of interconnected devices around us that are absorbed into the Internet and can communicate with each other with or without human intervention. These devices could be sensors, wearables, smart-phones, kitchen appliances, cars, industrial machines and anything we can imagine [1]. The applications and use cases of IoT will affect every aspect of our life from health care, smart homes and cities, and transportation to manufacturing and logistics. To become a reality, the IoT faces different challenges, including security ones. The security issues of the IoT devices are important in all of the IoT applications and use cases but in some of them, these issues become a vital factor. Auhenticating IoT devices and controlling their access to the network services and resources are key items to build such secured systems. Access control means authentication of IoT devices (clarifying their identities to the network) and checking their rights to do certain actions and to gain different types of services e.g. different types of connectivity and quality of services according to their subscriptions with the network. Considering the pervasiveness of the IoT in human life, negligence on security (especially on access control processes), may cause serious problems such as communication disruptions, financial losses, and even Life-threatening actions, e.g. in the medical sector [2, 3].

There are different communication technologies for enabling IoT applications and use cases. According to [4], we can consider them as three categories. Cellular technologies, Long-range networks like LoRaWAN and short-range networks like Wi-Fi. The entities that are involved in access control processes and the workflows between them are not the same in these different communication technologies. However, we can find a mapping between these entities and the common entities exist in all access control processes.

In designing access control mechanisms for the IoT, we should consider the application domains too. Because there are diverse IoT applications with different characteristics and requirements in different environments. All these differences impact the whole network, the associated security needs, and access control flow. For example, waste management application in smart city application domain is a delay tolerant application but patient's healthcare delivery and monitoring application in healthcare domain requires low latency [4]. In addition to these differences, there are also some common requirements in all IoT applications. Most of the IoT devices have low power capacity and cannot support strong access control procedures. They have also limitations in energy and battery life, therefore they could only support energy efficient procedures. In IoT, numerous devices may require accessing the network at the same time. The access control procedures should be correctly managed by the network to avoid DDOS attacks (distributed denial of services attacks) and high network access latency as well [5].

Among the above-mentioned requirements for designing IoT access control mechanisms, there is also a new concept calls "wholesale wireless connectivity". When we buy a connected device, we expect to have the wireless connectivity embedded inside it. Such devices and services (e.g. iPad+cellular; Kindle readers, future connected vehicles, future things for home automation and assisted living, etc.) are now believed to be best retailed when connectivity is directly commercialized with the device (better customer experience, better value proposal). Briefly said, connectivity providers sell connectivity to different verticals which in turn provide them to their own users, in a B2B2C business model (Business to Business to Consumer). Therefore, the wholesaling of wireless connectivity appears as a key issue. IoT use-cases targeting vertical sectors that are involving end-users (e.g. connected car occupants, patient remotely taken care of by the health industry) implies by defining a disintermediated business for connectivity provider, as the primary end-user relationship is handled by the vertical sector. The "wholesale wireless connectivity" has a significant impact on access control mechanisms that should be used in IoT.

In this paper, we will focus on access control mechanisms in cellular, Wi-Fi and LoRaWAN systems, to see that if they

978-1-5386-8336-1/19/$31.00 ©2019 IEEE

are in line with the "wholesale wireless connectivity" concept. The remainder of the paper is organized as follows. In section II, we explain the main concepts of an access control mechanism. In section III we study the access control mechanisms in the existing cellular, Wi-Fi and LoRaWAN systems. In section IV, we finally discuss whether these mechanisms could fulfill new requirements according to wholesale connectivity model.

## II. Basics of Authentication and Access Control

In this section, we introduce the general architecture of the access control systems, while in the next section we detail the implementations for various networks. Access control architectures and their associated entities may vary in different contexts but the general concepts remain similar. The main objectives are always to protect the subscribers and the resources and to apply billing rules for network usage [6, 7]. Access control usually consists of two steps: authentication and authorization. Authentication means verifying the user's identity by checking its credentials. Its purpose is to know who the user is [8]. Authorization means granting access to specific types of resources and services based on a user's access rights [9]. Its purpose is to specify what a user can do [8], which means controlling the access rights of users on the resources such as data, or even to IoT objects [10].

Access control (AC) architecture usually consists of two main functional entities; an Access Control server and an Access Control client. An AC server includes a database containing the users' data and it is responsible for managing the AC processes according to this database. An AC client is responsible for querying the AC server when users try to access the network through this entity [11]. The responsibilities of these two functional entities may be distributed in different physical entities for different systems. In some AC mechanisms, users are referred to by the 'peer' term. Figure 1 shows a typical network AC system.

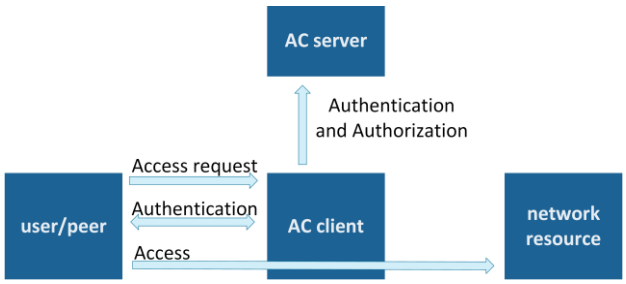


Fig. 1. Functions of AC systems.

## III. Access Control Implementation in Various Networks

To explain AC mechanism in network platforms, we consider the current cellular networks (mainly UMTS and LTE), the Wi-Fi and the IoT-focused LoRaWAN network.

### A. AC in cellular networks

Figure 2, depicts the AC systems in the current cellular networks. In summary, AC systems used in cellular networks, rely on a long-term secret key shared between:

- A hardware security module in the form of a UICC (universal integrated-circuit card) running a USIM (Universal Subscriber Identity Module) application inside the UE (User Equipment). This module calls SIM card.
- An AuC (Authentication Centre) that is integrated with an HLR (Home Location Register, the central database of subscribers' information in 3G architecture) or an HSS (Home Subscriber Server, the subscribers' database in 4G architecture) which is capable of authenticating the UICC.

Mobile networks use SDM (Subscriber Data Management) systems that consolidate previous silos of subscriber data (multiple HLR/HSS systems, AAA servers, etc.) into a single system. The authentication of the UICC by the core network of the operator (the connectivity provider) confirms the identity of the UICC at the cellular network provider level. The cellular network provider can then retrieve the subscription information which had previously been associated with this UICC identity at ordering time. The retrieved subscription information is then used by the cellular network provider to authorize which cellular service can be used and to bill the subscriber for the services consumed.

The main methods that are implemented in cellular networks (3G or UMTS and 4G or LTE) to fulfill AC requirements are UMTS-AKA, EPS-AKA, EAP-AKA and EAP-AKA'. They are all challenge– response authentication protocols with mutual authentication feature (the network authenticates the subscribers and the subscribers authenticate the network). UMTS-AKA and EPS-AKA are used to authenticate the subscribers connected across 3GPP access networks to the core network of 3G and 4G respectively. UMTS-AKA involves the USIM in the subscriber's mobile equipment, VLR/SGSN (Visitor Location Register/Serving GPRS Support Node, responsible for mobility management), and HLR in the core network.

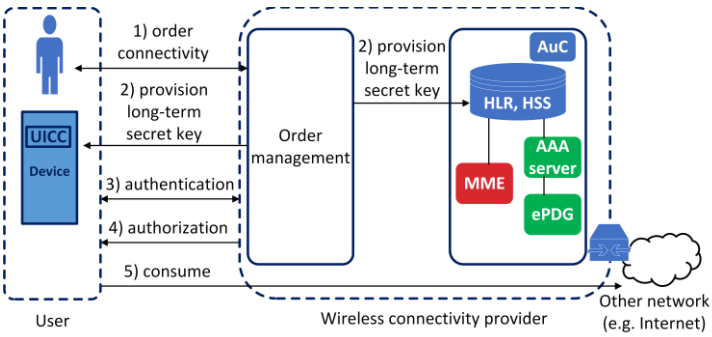


Fig. 2. Current mobile network AC model.

Authentication of the subscribers is based on their unique identity, IMSI (International Mobile Subscriber Identity) and a shared secret key K that is stored both inside the USIM and the HLR. This identity is provisioned by an order management module from the mobile network operator Information System while the subscriber buys a UICC from the operator (fig. 2) [12]. Considering the AC functional entities and the terminology that we have mentioned above, we can say that

both HLR and VLR/SGSN act as AC servers and that VLR/SGSN also acts as an AC client.

As with UMTS-AKA, EPS-AKA operates between the USIM, the MME (Mobility Management Entity, the main control node of the network) and the HSS. EPS-AKA is also based on IMSI and a shared secret key between the USIM and the HSS (previously provisioned by the order management module). So with AC terminology, HSS and MME jointly play the role of an AC server and MME also acts as an AC client. One of the important differences between the EPS-AKA and UMTS-AKA protocols is that EPS-AKA uses the serving network's identity in deriving the further keys in the key hierarchy (from the shared secret key K), to secure the connections between the network elements. The binding of the keys to the serving network identity reduces the probability of a serving network impersonation fraud. On the other hand, EAP-AKA and EAP-AKA' are responsible for the authentication of subscribers when they try to access a 3GPP core network via a non-3GPP access network (e.g., via a public or private Wi-Fi network). These two protocols belong to the EAP framework (Extensible Authentication Protocol). In EAP terminology, we have 'authenticators' and 'EAP servers'.

For matching the EAP and AC concepts, we can say that an authenticator is an AC client and an EAP server is an AC server. In EAP-AKA and EAP-AKA', the authentication process is based on NAI (Network Access Identifier, derived from IMSI) and a shared secret key as in UMTS-AKA and EPS-AKA. Performed between USIM (or any other application with a similar functionality. This part is left unspecified in 3GPP specifications because of the use of non-3GPP access networks), non-3GPP access network or ePDG (Evolved Packet Data Gateway) in core networks and a 3GPP AAA server along with HLR or HSS. The role of AC client is played by the access network (the exact entity may differ according to the type of access network) and by the ePDG. The role of AC server is obviously played by the 3GPP AAA server, along with HLR or HSS. The 3GPP AAA server chooses to use EAP-AKA or EAP-AKA' according to some conditions out of this paper's scope, but we can say that EAP-AKA' is stronger that EAP-AKA as it uses serving network identity in key derivation processes like EPS-AKA [13]. Table 1 summarizes the responsibilities of the different entities of the UMTS-AKA, EPS-AKA, EAP-AKA and EAP-AKA' methods in AAA systems terminology.

TABLE I. CELLURAR AC FUNCTIONS

| AC Entities | UMTS-AKA | EPS/AKA | EAP-AKA/EAP-AKA' |
|---|---|---|---|
| **user/peer** | UE | UE | UE |
| **AC client** | VLR/SGSN | MME | Access Network, ePDG |
| **AC server** | HLR, VLR/SGSN | HSS, MME | 3GPP AAA server, HSS/HSS |

## B. AC in Wi-Fi

Wi-Fi networks are one of the most widely spread networks. The main security mechanisms that are applied to these networks are WPA (Wi-Fi Protected Access) and WPA2 [14]. The entities that participate in the users' authentication process and establish secure connections are user devices, access points (acting as AC client) and an authentication server (acting as AC server). The WPA protocol uses IEEE 802.1x standard for users' authentication.

In home or small networks, it utilizes the personal mode in which a key is pre-shared between the users and the access point – anyone who holds the key can access the network. In this mode, the access points have the responsibilities of both AC client and AC server [15]. In a business network, the WPA protocol utilizes the enterprise mode in which there is no pre-shared key between the users and access points. It uses an EAP type protocol (choosing an EAP protocol is based on the existing authentication system) with an AC server (EAP server) as a separate entity of the access point. WPA2 was introduced to replace WPA. The users' authentication process is almost the same as in WPA. It improves the level of security by adding the requirement of proving an access point's identities with the authentication server (this part is out of our paper's scope). Figure 3 is the general workflow of a Wi-Fi access control system. After the devices provide their identities (user names) to the access point, they negotiate with the authentication server through the access point, about the type of EAP authentication method they want to use.

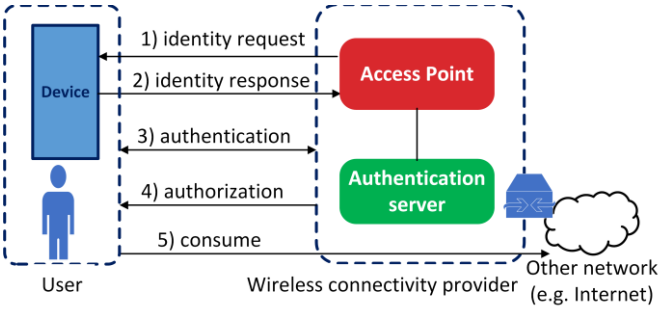


Fig. 3. Wi-Fi network AC model.

The entities of both WPA and WPA2's protocols are shown in AC systems' terminology in table 2.

TABLE II. WI-FI AC FUNCTIONS

| AC Entities | WPA/WPA2 personal networks | WPA/WPA2 business networks |
|---|---|---|
| **user/peer** | User's device | User's device |
| **AC client** | Access point | Access point |
| **AC server** | Access point | EAP server |

## C. AC in LoRaWAN

LoRaWAN networks are based on LPWA (low-power, wide-area) technologies that are suitable for transmitting low amounts of data through a wide area with low power consumption [16]. Its architecture has a star topology and contains: End-Devices (sensors that are connected to the gateways to have access to the network, this connection is a single-hop LoRa connection), Gateways (forwards received data from end-devices to the network server through an IP backhaul), a Network Server (the intelligent part of the network and the center of the star topology), a Join Server (manages end-device activation and connection to the network) and an Application Server (for application-specific processing) [17].

There are two types of end-device activation processes for connecting them to the network: ABP (Activation-by-Personalization) and OTA (Over-the-Air) [17]. Therefore, there are two types of access control in LoRaWAN. In the OTA activation process, the end-devices should introduce themselves to the network to obtain the necessary information to establish secure connections with the network (e.g. the session key between the end-device and the application server to encrypt the application-specific data messages). Each end-device in this process should have two unique identifiers and an AppKey, a shared secret key between the end-device and the joint server that controls the end-device. The AppKey is never sent to the other servers and is used to derive the further session keys with which to encrypt the communications and data [18]. As for identifiers, one of them, the DevEUI identifies the end-device (like a MAC address of a TCP/IP device) and the other, the JoinEUI (known as the AppEUI in the previous specifications of LoRa), identifies the join server that the end-device should refer to (the service provider of the device). An end-device should have an address, DevAddr, that identifies it in the current network. The join server should contain the devices' AppKey and DevEUI.

There are two scenarios for provisioning these identities in an end-device. In the first, the device manufacturer allocates the DevEUI and the AppKey to the end-device and sets the value of the JoinEUI to the service provider's join server identifier. In this scenario, the end-device belongs to the service provider but it can work in different networks in different countries because the service provider can register its join server identifier (JoinEUI) in different network operators (figure 4).

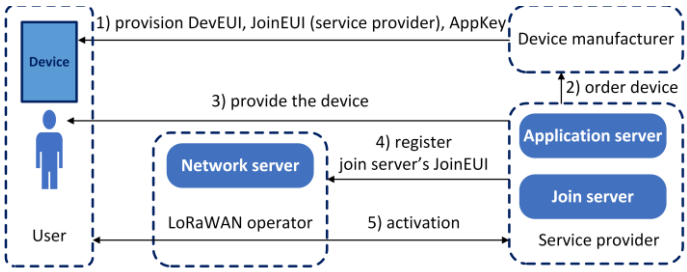


Fig. 4. LoRaWAN AC model with the first scenario of the OTA activation process. The device belongs to a specific service provider.

In the second scenario, as with the first, the device manufacturer allocates the DevEUI and the AppKey to the end-device but the device's JoinEUI is set to the identifier of a join server belonging to a trusted third party (and which knows the end-device's DevEUIs and its AppKeys). Therefore, the end-device can work with any service provider in the various networks (figure 5). In this scenario, end users buy these end-devices from any retail channel (they do not get the end-devices from the service providers).

In the ABP activation process, unlike the OTA activation process, the join server plays no role. Devices are personalized to work with a specific LoRaWAN network. All the necessary information and session keys required to establish a secure connection between the end-device and the network have already been configured in the end-device, the network server and the application server (figure 6). Therefore there is no need for remote authentication and access control and the end-device can exchange data with the network immediately.

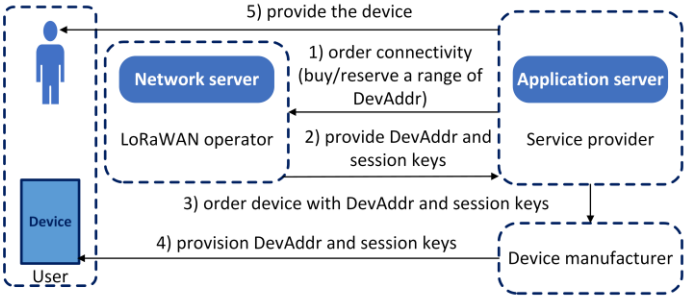


Fig. 6. LoRaWAN AC model with the ABP activation process.

As shown in table 3, the AC system entities do not make sense in the ABP activation process. In the OTA activation process the responsibilities of AC client and AC server are distributed among the network server, join server and application server, but the details of these responsibilities are different in the two OTA scenarios.

TABLE III. LORAWAN AC FUNCTIONS

| AC Entities | ABP | OTA |
|---|---|---|
| **user/peer** | No need for remote authentication | User's device |
| **AC client** | | The responsibilities are shared between network, join server and application server |
| **AC server** | | |

## IV. COMPARISON OF DIFFERENT AC MODELS FOR IOT NEEDS

In this section we examine AC models in the current cellular, Wi-Fi and LoRaWAN networks to determine if they can fulfil the new IoT wholesale connectivity requirement. As we see in section III part A, in the current cellular systems' AC mechanisms, the network operators (connectivity providers) have central role and act as both AC server and AC client. To fit the rising disintermediation depicted in the introduction, we can deform the design of the AC model in figure 2 by defining an intermediate player to obtain connectivity orders from the users. The verticals can play the

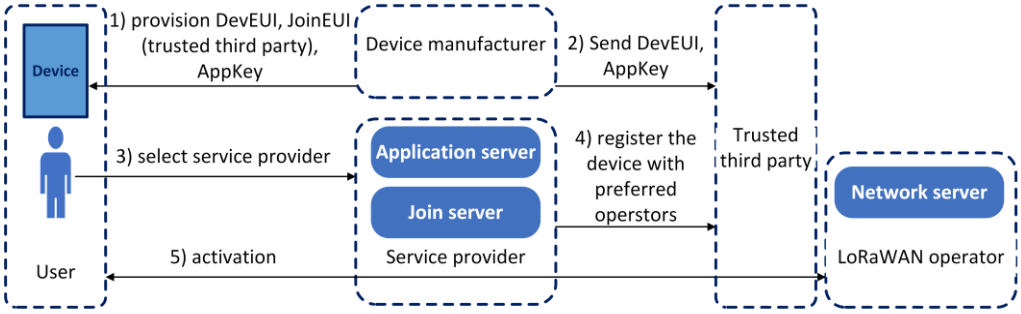


Fig. 5. LoRaWAN AC model with the second scenario of the OTA activation process. The device does not belong to a specific service provider and a user can buy it from any retail channel.

role of this intermediate player. This AC model is shown in figure 7 and is already being used by players like Apple for provisioning identities and keys in devices (e.g., iWatches) through embedded SIM mechanisms (eSIM).

Such an evolution (deforming current AC systems) is however questionable. It would generate redundancies at the disintermediating player and at the wholesale connectivity provider(s) because each must manage end-users/subscribers in their own information systems; while the wholesale connectivity provider would have no business incentive to do so (the wholesale connectivity provider is selling to the intermediate player, not to individual subscribers). Furthermore both the disintermediating player and the connectivity provider have to authenticate the end-users/subscribers at their own level. The intermediate player could use any means relevant to its own business while the connectivity provider would be restricted to authenticating an UICC and its assumed ownership by the end-user/subscriber that it does not directly know. These redundancies could generate extra costs and a lack of agility.

On the other hand, it is expected that, the next generation of mobile networks, 5G, will support heterogeneous and non-3GPP networks accesses like LoRaWAN and Wi-Fi. By these non-3GPP networks accesses, devices are not always equipped with an UICC and the connectivity provider doesn't always have a-priori knowledge (i.e. pre-provisioned in its information system) about the person/organization responsible for the network consumption of a given device. The connectivity provider still needs to provide ciphering and/or integrity protection keys to the device but this is done when the device is about to use a given network (e.g. activated) and without relying on long-term secret keys stored in the UICC and pre-provisioned in the information system (figure 3, arrows n°2 and 3). As 5G's core network will have to cope with heterogeneous access types, devices and business-cases, one cannot assume that a UICC-SDM based system is the panacea. In addition to all these problems, introducing the intermediate player to the wireless connectivity provider and providing mutual authentication between them, is another issue that should be taken into account. Since the intermediate player could be any vertical with different types of slices, their management is not possible with this AC model.

The AC model in Wi-Fi networks is relatively simple, and appears to not be very helpful for elaborating future IoT access control mechanisms. There is no contract (free or per user) and the authorization may be unrelated to the authentication. It does not fit to wholesale connectivity as well.

The AC system in LoRaWAN however, it does allow for several business models quite distinct from the retailing of cellular network subscriptions to end-users. As noted in the third section, by providing different possibilities to allocate the necessary information such as identities and keys to the end-devices, LoRaWAN could have different scenarios for the different actors' connections. In the OTA activation process, the end-devices work with a specific application provider on any network or they work with any (compatible) application provider on any network (through the mediation of an undefined Trusted Third Party player at device activation time).

LoRaWAN does not give a central role to network based AC systems. Instead the main players regarding authentication and authorization are recognized by the system architecture to be the device manufacturers and the application providers: in all the business cases considered the network provider is involved in the commissioning process, either by the application provider or by a yet-undefined trusted third party player (Considering the potential ecosystem evolutions where multiple Trusted Third Parties might attempt to take a central position in device activation and where the number of application provider and device provider could explode, this is probably a weak point of the LoraWAN architecture.). Moreover, endpoint/application keys are learned by the network provider before the usage phase (i.e. involving an "ordering" process in the information systems similar to traditional SDM based systems) only in the ABP activated end-devices case. Otherwise, the network (i.e. the network server, not a subscription management system) learns about endpoint/application at first use-time i.e. during over-the-air activation.

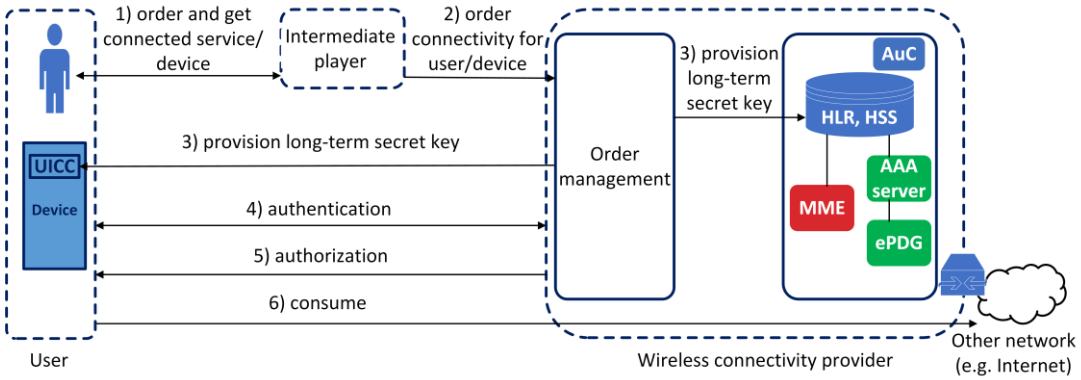


Fig. 7. Deformation of current mobile network AC model for disintermediation.

## V. CONCLUSION

Access control of devices in IoT has a key importance, for their own security as well as for the network one. Along with a better quality of experience for the users like high data rates and low energy consumptions, some new requirements appear in this context (e.g. wholesaling wireless connectivity business trends and willingness to provide and manage the IoT concept in a more efficient manner). In this paper we study the suitability of the current AC mechanisms of cellular, Wi-Fi and LoRaWAN networks for this new requirement. The current AC mechanisms in cellular networks, the deformation form of them and AC mechanisms in Wi-Fi do not fit the wholesale wireless connectivity model. But as AC mechanism in LoRaWAN does not give a central role to the connectivity provider, it may however show an alternative way of designing AC for wholesale connectivity in IoT.

Future works will focus on studying the entities that will participate in IoT's AC mechanisms and the exact responsibilities of each: which entities will be under the control of wholesale connectivity provider and which of them will be under the control of verticals. In addition to the wholesale connectivity concept, IoT brings some additional requirements that should be considered too. For example linking multiple objects to the same subscription and separating the subscriber authentication from the device authentication because of the changes in the ownership of the devices that may happen during their lifecycles.

## REFERENCES


[1] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things: New Perspectives and Research Challenges," *arXiv preprint arXiv:1803.05022*, 2018.

[2] Kelsey D. Atheron, Popular Science, "Hackers Can Tap Into Hospital Drug Pumps To Serve Lethal Doses To Patients," available at: http://tinyurl.com/qfscthv, 2015.

[3] Darren Pauli, ITNews, "Hacked Terminals Capable of Causing Pacemaker Deaths," http://tinyurl.com/ycl4z9xf, 2015.

[4] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[5] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[6] S. Wong, N. Sastry, O. Holland, V. Friderikos, M. Dohler, and H. Aghvami, "Virtualized authentication, authorization and accounting (V-AAA) in 5G networks," in *Standards for Communications and Networking (CSCN), 2017 IEEE Conference on*, 2017, pp. 175–180.

[7] M. Koutsopoulou, A. Kaloxylos, A. Alonistioti, L. Merakos, and K. Kawamura, "Charging, accounting and billing management schemes in mobile telecommunication networks and the internet," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 1, 2004.

[8] T. Velte and A. Velte, *Cisco: a beginner's guide*. McGraw-Hill, Inc., 2006.

[9] C. Metz, "AAA protocols: authentication, authorization, and accounting for the Internet," *IEEE Internet Computing*, vol. 3, no. 6, pp. 75–79, 1999.

[10] S. Gusmeroli, S. Piccione, and D. Rotondi, "IoT access control issues: a capability based approach," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, 2012, pp. 787–792.

[11] A. E. Yegin and F. Watanabe, "Authentication, Authorization, and Accounting," *Next Generation Mobile Systems 3G and Beyond*, pp. 315–343, 2005.

[12] 3GPP, "Security Architecture," *TS 33.102*, Tech. Spec. V14.1.0, 2017.

[13] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE security*. John Wiley & Sons, 2012.

[14] LoRa Alliance Technical Committee, "LoRaWAN™ 1.1 Specification", Tech. Spec. V1.1, 2017.

[15] M. Mathews and R. Hunt, "Evolution of wireless LAN security architecture to IEEE 802.11 i (WPA2)," in *Proceedings of the fourth IASTED Asian conference on communication systems and networks*, 2007.

[16] M. Khasawneh, I. Kajman, R. Alkhudaidy, and A. Althubyani, "A survey on Wi-Fi protocols: WPA and WPA2," in *International Conference on Security in Computer Networks and Distributed Systems*, 2014, pp. 496–511.

[17] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*, vol. 3, no. 1, pp. 14–21, 2017.

[18] LoRa Alliance Technical Committee, "LoRaWAN™ Backend Interfaces 1.0 Specification", Tech. Spec. V1.0, 2017.