UDC 629.735.018.7.015.3.025.1

V.M. Korchan, PhD, I.V. Morozova
(National Aviation University, Ukraine)

Methods of identification of IoT devices

There are various identification methods cannot used by many devices of the Internet of Things for a number of objective reasons. Very important property is the fixed ratio an identifier with the actual device of the Internet of Things, as well as versatility in the application of the identifier in various industries. The promise of vast new markets has created an array of alliances and consortia to develop competing standards and protocols for the Internet of Things (IoT). The ITU - DONA Foundation alliance is one such example. DONA's Digital Object Architecture (DOA), a name-attribute binding service for managing distributed databases, presents itself as a potential solution for IoT challenges. But this proposed solution has been greeted with intense political opposition.

The DOA identifier structure

In the DOA architecture, the resolution system is two-tier. The first the resolution level is the global register (GHR, from the English Global Handle Registry); the second level is a set of local registries (LHR, from the English Local Handle Registry) or local services (LHS, from the English.Local Handle Service). For permission identifier in this subsystem, first there is an appeal to the global registry GHR, which reports information about the local LHR, which contains necessary information about the digital object. Schematically this process is shown in Figure 1.

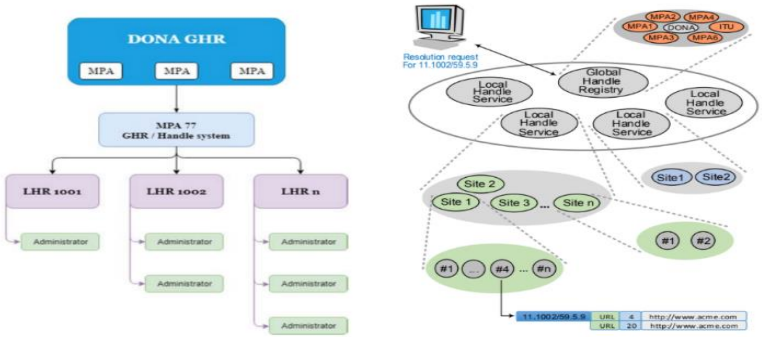

Fig. 1. Structure of the Handle system

The DOA identifier structure itself also follows a two-level system. The first part is called the prefix; the second part is a suffix. The prefix allows to establish

information about the local register of the LHR digital object. This the correspondence of the prefix and information about the administrator is stored in the global the GHR registry. The suffix already uniquely identifies a specific object, and this information linking the suffix to a specific object is stored in local LHR registry.

The interaction of elements within DOA involves communication between distributed LHR servers located in different countries. But distribution leads to an increase in network latency, the value of which can unacceptable for services and applications requiring ultra-small delays in 5G / IMT-2020 communication networks. Thus, one of the characteristics of the system resolution, critical for identifying the Internet of Things, is the average time serving one request.

To minimize network latency, it is proposed to split the resolution system, by introducing intermediate level registers between GHR and distributed LHR – Middle Handle Register, MHR. Each MHR can be tied to a specific geographic region on the world map, taking into account density and quantity devices located there, as well as the density of the manufacturers (i.e. the density LHR). LHR communicates with the nearest MHR instead of the remote GHR, which reduces the distance of data transmission over communication channels and, as a result, reduces network delay.

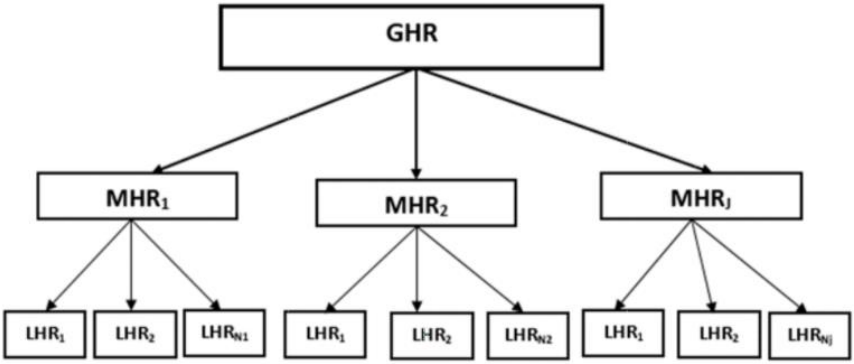

Fig. 2. The main components of DOA with an intermediate level of interaction

DOA and the Handle System were initially conceived with something else in mind: the management of libraries and digital documents. The Handle System is, in fact, a very efficient means of achieving what it was originally designed to do: act as a library repository and information retrieval system with persistent identifiers. Even the IETF and Internet Society (ISOC) use it for those purposes. Once you bring that mix into the IoT space, however, the scale changes by many orders of magnitude, and concerns such as security, privacy, and efficiency become paramount. In other words, there are many reasons to continue ignoring it. Although most industry players regard the idea of having globally unique identifiers as a means of trusted authentication for

IoT as a good one, as far as we know no private sector software company is currently considering applying DOA to Internet of Things solutions. Major global industry standards bodies have developed their own specialized tagging platforms and have rejected the use of DOA to combat counterfeiting. The currently preferred method of secure resolution is that of 802.1AR "Secure Device Identity" that leverages Certificate Authorities (CA). Although this method is far from perfect as CAs are susceptible to spoofing, they are often supplemented with different schemes such as including hardware-level signature to establish a chain of trust.

Conclusion

A method for identifying devices and applications of the Internet of Things has been developed in heterogeneous communication networks based on the architecture of digital objects, which allows identification of IOT devices and applications on a global scale. Methods for integrating DOA identifiers into Internet devices are considered things that support various technologies for wireless data transmission and presents the structure of metadata that can be used in the architecture digital objects for IoT devices to validate originality combined with traditional identifiers.

References

1. Digital identification of objects: technology and not only / Ed. M.A.Medrisha. Moscow: Scientific Review, 2016.228p. ISBN978-5-9906425-4-6.
2. Evans D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. CISCOWhitePapers.2011.
3. Berners-Lee, T., Fielding, R., Masinter, L. RFC 3986. Uniform Resource Identifier (URL): Generic Syntax. URL: https://www.ietf.org/rfc/rfc3986.txt.
4. Kirichek R., Kulik V., Koucheryavy A. False Clouds for Internet of Things and Methods of Protection // 18th International Conference on Advanced Communication Technology (ICACT). 2016.pp. 201–205.
5. Danilov K., Kirichek R., Kulik V. Methods for Detection of Internet of Things in the Global Network // Telecom IT. 2015. Vol. 4 (12). pp. 48–56.