DOA-based IoT
A system for anti counterfeiting

Albahri Mahmood
Department of Communication and Data Networks
State University of Telecommunication
St. Petersburg, Russia
albahri.89@hotmail.com

Abdelhamied A. Ateya
Electronics and Communications Engineering dep.
Zagazig University
Zagazig, Egypt
a_ashraf@zu.edu.eg

Ammar Muthanna
Applied Probability and Informatics Department
Peoples' Friendship University of Russia (RUDN University)
Moscow, Russian
ammarexpress@gmail.com

Ruslan Kirichek
Department of Communication and Data Networks
State University of Telecommunication
St. Petersburg, Russia
kirichek@sut.ru

Aleksey Borodin
Representation PJSC Rostelecom in the International Telecommunication Union (ITU)
Moscow, Russia
alexey.borodin@rt.ru

***Abstract*— There is no doubt that the IoT is a big revolution that has a great impact on our life. IoT provides the communication network for connecting physical objects (i.e. sensors and embedded systems). With the massive increase of IoT devices and the very high society impacts of the IoT including the wide range of applications predicted, the anti counterfeiting becomes an important issue. In this work, we mainly focus on this issue. DOA is a global system that enables the generation of digital objects with unique identifiers. Using DOA, we can identify any information and store it using a unique global identifier. We provide a framework for enabling and facilitating the use of DOA in IoT for anti counterfeiting. The system provides a unique identifier for each IoT device and enables the end user to check the device information and specifications through the identifier. Moreover, the identifier can be used to identify the device in the network. The user can extract the identifier of the device by using a proper technology interface.**

Keywords—Internet of Things, DOA, handle, anti counterfeiting, prefix

I. INTRODUCTION

Internet of Things (IoT) represents the third wave in the Internet technology evolution came after the revolution of the Mobile Internet. IoT is the dawn of machine interaction, since it represents the main framework for the machine to machine (M2M) communication [1]. With this revolution, a massive number of applications in various fields are presented that with no doubts push the world to a new life, certainly with the nearly release of the fifth generation of cellular system (5G). Applications such as smart cities, smart homes, industrial automation and e-health are considered [2].

With the recent development of system-on-chip and wireless devices, the number of connected devices to the Internet exceeds the global human population and this number is increasing dramatically. By 2020, it is expected that the number of connected devices will be in the range of 50 billion with a market volume of range of 7.5 trillion dollars [3], [4]. IoT is the communication paradigm that covers the connection and interaction among this growing number of devices in a smart way. The number of IoT connected devices around the world raise exponentially; Fig.1 illustrates the actual and the predicted number of IoT devices in billions from 2015 to 2025 with the market impact [5].

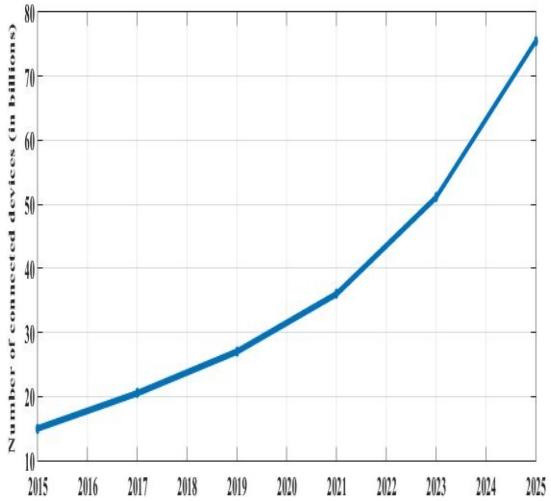

Fig. 1. Number of IoT connected devices (2015 – 2025) in billions [5].

Counterfeited devices may introduce series problems for all market sectors, starting from the end user and moving to vendors. Moreover, adverse consequences of counterfeit devices could affect governments and private sectors [6]. There some regional and global organizations that care for combat counterfeiting and intellectual property rights enforcement, the main one is the Anti-Counterfeiting Trade Agreement (ACTA) [7]. There are lots of counterfeit solutions developed for various technologies or goods; however these solutions are a product dependent. This means that an industry uses a method for counterfeit a certain product, while other products and industries may deploy different ways. Considering electronic devices, there are many ways developed for anti counterfeiting such as Electronic product code (EPC) and International mobile equipment identity (IMEI) [8]. The IMEI is a unique number allocated for each mobile device and used as the mobile equipment identifier in the network. This helps to prevent counterfeited devices from being used as even if the user don't recognize when getting a counterfeited mobile device, no cellular network would accept the device [9].

One of the key solutions recommended to combat counterfeiting in IoT devices is the digital object architecture (DOA) system. Using DOA each IoT device can get a unique identification, which can be used to map to the original device information and also may be used to identify the device in the network. The device information is set by the vendors and can be accessed by the user once getting a device through the device identifier. The identifier is implemented in the device by the manufacturer through the DOA system and can be extracted by the user by means of a prober interface.

In this work, we provide a DOA-based system that can be used in IoT for anti counterfeiting. In (Sec. II), a general description of the DOA system is introduced including the mechanism of handle system. In (Sec. III), a framework for the DOA based system for IoT is presented.

II. BACKGROUND AND RELATED WORKS

A. *DOA system*

The idea behind DOA was first originated by a research group released by National Research Initiatives (CNRI) in a project funded by the Defense Advanced Research Projects Agency (DARPA) in 1993 [10]. DOA is a system used for various purposes, generally for store and retrieve information for an Internet based system.

DOA is a system considering information and digital material storing, accessing and managing. The digital object is information or digital material that contains two main components; the data and the metadata. The metadata consists mainly of the handle which is a global unique identifier for the digital object and may contain other fields that may come up for special purposes [11].

A general structure of the DOA system and the process involved is illustrated in Fig.2. The first part of the system is the originator, which is the user who requests the service. The originator has a data and wants to form it in the shape of a digital object. For this purpose the originator communicate with handle generator asking for a handle to form a digital object for his data. The handle generator responds with a handle, which is a unique identifier that is independent of the logical or physical system [12]. The originator forms a digital object using the received handle with the digital data, and then forwards the data to a certain repository or a group of repositories.

A repository is a system used mainly for storing digital objects, services and management information. It works based on a repository access protocol which enables and manages the accessing and depositing mechanisms. The depositing mechanism is responsible for adding new digital objects and the accessing mechanism is used to control and manage the availability and accessing a certain repository [10]. Each repository has a unique name and an IP address which assigned by a local naming authority, which in contact with a global naming authority. Repository may define some services and properties to facilitate managing and controlling the stored data. An example of these properties is the record property, which allow collecting and gathering all data associated with the same digital object.

Once a digital object is stored in a repository, the repository name or IP and the digital object's handle are transmitted to the handle servers system for registration purposes [13]. up on the user demand and the nature of the information, the originator can ask for the name of the repository and dedicated network or even the group of repositories incase of the digital object is stored in multi-repositories by sending the handle of the digital object to the handle servers system. The handle servers system responds to the request by the name of the repository where the user's data is available.

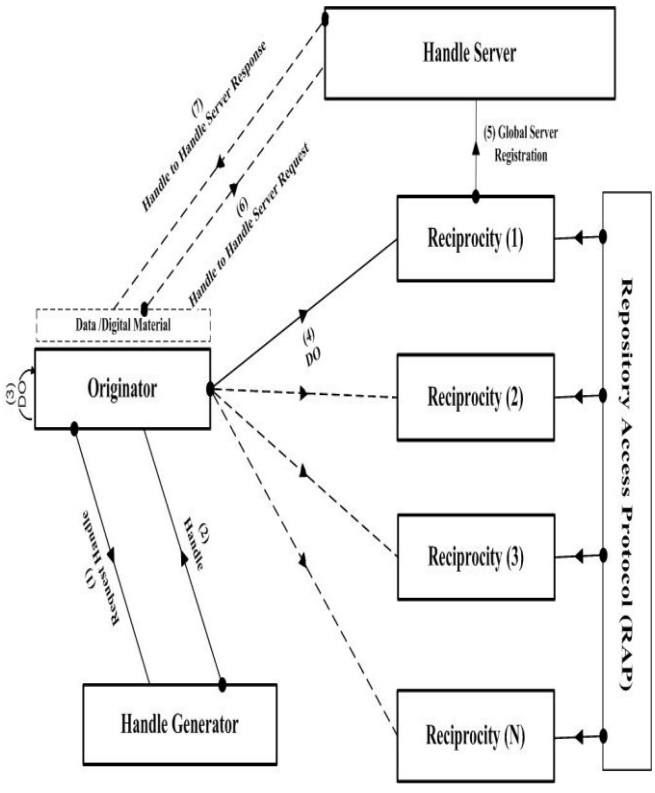

Fig. 2. General structure for the DOA system.

The handle is now supported by the DONA foundation (DONA), which is a nonprofit foundation established for general purposes associated with handles of digital objects [14]. In 2014, ITU has performed a memorandum of understanding (MOU) with the DONA organization to work with the CNRI as a step for transition from CNRI to DONA. In 2015, DONA took the responsibility of the GHR [14]. DONA provides various services include management and development for all issues concerned with the DOA (i.e. technical coordination, evolution and applications). DONA has the authority to provide all tasks associated with the handle system identifier, registration and resolution services, this include admission, coordination and maintenance.

B. *Handle system*

The handle system is built on the base of location mapping, since the handle system can resolve any handle of a digital object to its location. The handle consists with two main parts; prefix and suffix. The prefix is a global identification administrated at the global handle registry (GHR). GHR maintain prefixes for different handles and mapping information to the local handle service (LHS) dedicated with each prefix. LHS is responsible for managing the second part of the handle or the suffix. In another word, the handle system can be viewed as a group of handle services rooted to GHR and each of them may employ one or more sites, with one or multiple servers for each site [15]. A general overview of the handle system structure is illustrated in Fig.3.

III. DOA-IOT SYSTEM

The past international telecommunication Union‘s (ITU) world telecommunication standardization assembly (WTSA 16) in Tunisia had discussed many issues concerned with the IoT. These issues vary from technical perspectives to economic and security matters. One of the main issues discussed was the DOA as announced by the proceedings of the WTSA 16 [16]. Based on the WTSA 16 proceedings, there are a number of proposal works discussing the DOA for IoT provided by three main alliances; the Arab States Administrations (Arab States), the Russian Communications Commonwealth (RCC) and the African Telecommunication Union (ATU) [16], [17].

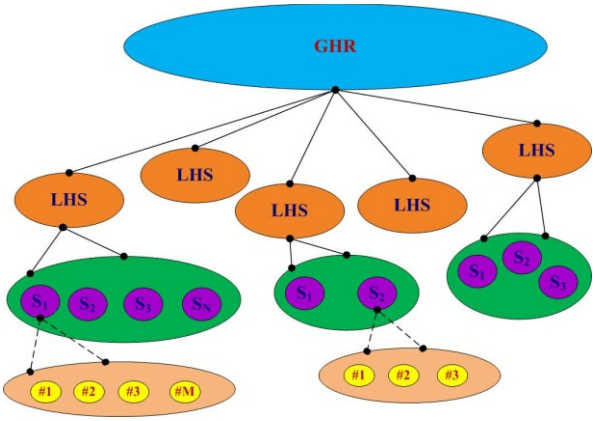

Fig. 3. Handle system structure.

Employing DOA for IoT devices, will assign each IoT device a handle. The handle will mainly used to identify and map to the device identification information. The handle‘s prefix should indicate the country and the main region, while the suffix will point to the IoT device information. Using the handle’s prefix we can enter the GHR to estimate the corresponding LHS, where we can enter with the suffix to get all information associated with the IoT device labeled by this handle (prefix + suffix). The GHR is a global registry serve for all distributed LHSs. LHS may be dedicated with a vendor and located within its vicinity, or may serve for multi-vendors. The preliminary purpose for deploying DOA for IoT is to anti-counterfeiting in IoT products.

The user can check the IoT device specifications and make sure of them through the handle system. The user can extract the handle prefix using a proper technology, and sends the handle prefix to the GHR asking for the LHS contains the dedicated information of the IoT device. The GHR responds with a message contains the address of the intended LHS. The device receives the message containing the LHS and sends a request message to the LHS contains the handle. The LHS respond with the stored data for the handle, this data contains all information about the IoT device approved and modified by the device vendor. Figure 4 indicates the structure and procedures for the IoT device checking the counterfeiting using DOA system.

A. *Handle interface reader*

The handle should be hardware implemented in the IoT device. One way is to build an IoT module in each IoT device that acts as the hardware identifier or the device passport. The handle may be stored in a non-volatile read-only-memory (ROM) in the IoT module and can be red and extracted by the user through an interface technology circuit. The user can check the counterfeiting of an IoT device by using a prober interface supported by the IoT module in the device to get the handle.

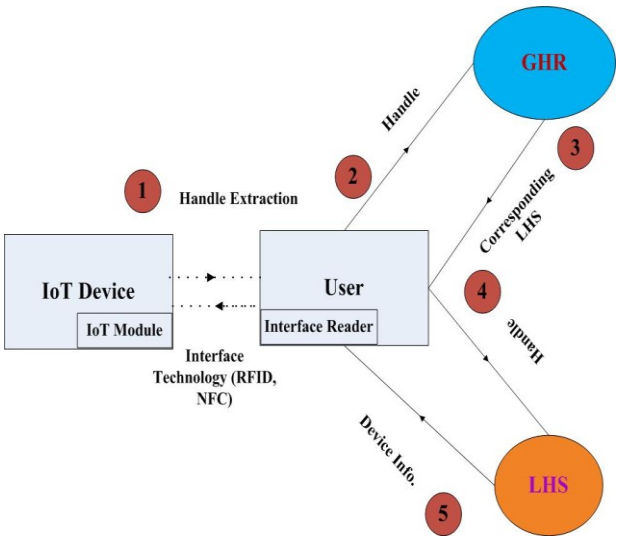

Fig. 4. DOA-IoT system.

RUDN University Program 5-100, Moscow, Russian

There many secure technologies that can be deployed as a user interface; we mentioned some of them in the following:

1- Near field communication (NFC) technology interface:

   The IoT device can support NFC tag, which can be read by any other devices that supports the read/write mode of NFC technology. An example of such devices is the mobile device supports NFC technology [18].

2- Radio frequency identification (RFID) technology interface:

   A passive RFID tag can be implemented in the IoT device which map to the handle. The RFID tag can be read using any RFID reader device. A mobile device with an operating system supports a built in RFID reader can be used [19].

B. Handle implementation

The IoT handle is used to map to the device information and specifications. Once the user gets the device handle, he can extract the device information via the previous illustrated procedures. The device information is organized in a three main parts; the general information, the technical information and the software and application information as a three illustrated in Fig.5. The general information part contains information associated with the device manufacturer and a general description of the device including the device shape. The fields deployed in this part may include the following:

1- Product name,

2- Product type,

3- Manufacturer name,

4- Data assembled,

5- Dimensions and packaging,

6- Associated certificates, and

7- Guarantee and maintenance validity.

The second part is the technical information, which contains all information associated with the hardware specifications. This part may include the following fields:

1- Storage specifications,

2- Power specifications,

3- Processing specifications, and

3- Communication standard supported.

The last part contains information about the software supported by the IoT device. This includes the operating system specifications (i.e. type and version). Also, a list of applications and use cases of the IoT device including the deployment scenarios may be include [20].

C. How it works

The GHR allocate the handle prefix to the IoT devices manufacturers upon their request. Then the manufacture asks the LHS for the suffix to form the handle for a certain device

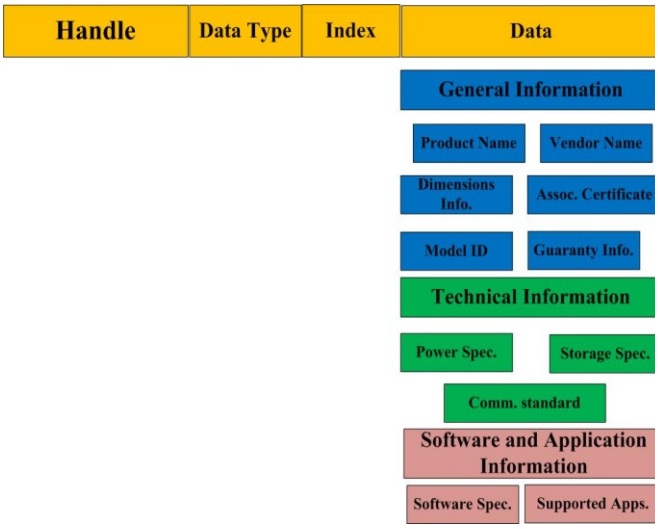

Fig. 5. Device information and handel data structure.

and once the handle is obtained and data is registered the GHR should be informed.

Using handle as the IoT device identifier achieves various benefits. The handle system can be used to anti counterfeit of IoT devices; moreover the IoT device can use the handle as the device identification when registered in a network. All IoT networks and associated ones may deploy a register for the IoT device identifiers include the authorized devices.

Deploying DOA for IoT still politically controversial, however there is a great demand from many governments raise the hand to this topic. This made the ITU opens the work and claims for developing a framework cover the DOA employment for IoT devices. The work dedicated with this subject is under the study group level now. Last point to be mentioned is that DOA for IoT devices can be used as an alternative way to the IPV6, since the IPV6 facilitates allocating a unique address to each device. Thus, each device could have a handle and an IPV6 that can map to each other.

IV. EXPERIMENTAL WORK

We perform a simple experiment to identify an IoT device and provide a user friendly interface to read the device‘s identifier. For this purpose, we connect a NOR flash memory (Atmel - AT26DF161 – SU) to the ESP32 board. The board is considered as the IoT device that is target to be identified. The flash memory is used as a register for the identifier. The flash memory is connected to the ESP32 board and the identifier is written to the memory using the operating system of Mongoose OS. A computer based interface is provided to enable reading the device identifier as illustrated in Fig.6. Once the device identifier is extracted, it can go through the DOA system and provide the data associated with the identifier.

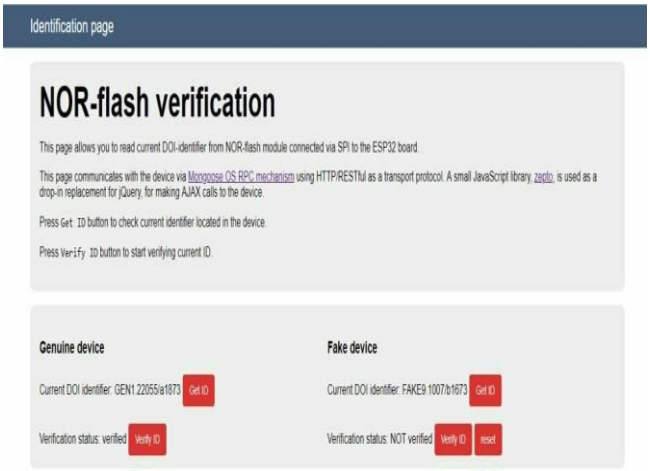

Fig. 6. Device identifier detection.

V. Conclusion

DOA can be deployed for the IoT to achieve various benefits, mainly for combating counterfeit of IoT device. The work provides the structure of the DOA system for IoT, in which each IoT device is allocated a handle that represents the device identifier. The handle is implemented in the device on a non-writable memory embedded with the device. The handle is global unique identifier provided by the DOA system. The handle is used to map to the original device specifications and information. The device information includes; general information, technical information and software and application information. The user can extract the handle from the device via a prober interface.

Acknowledgment

The publication has been prepared with the support of the "RUDN University Program 5-100"

References

[1] Ammar, M., Russello, G. and Crispo, B., 2018. Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, pp.8-27.

[2] Mihovska, A. and Sarkar, M., 2018. Smart Connectivity for Internet of Things (IoT) Applications. In New Advances in the Internet of Things (pp. 105-118). Springer, Cham.

[3] Nordrum, A., 2016. Popular internet of things forecast of 50 billion devices by 2020 is outdated. IEEE Spectrum, 18.

[4] D. Lund, C. MacGillivray, V. Turner, M. Morales, "Worldwide and Regional Internet of Things (IoT) 2014–2020. Forecast: A Virtuous Circle of Proven Value and Demand," International Data Corporation (IDC), Tech. Rep., 2014.

[5] Statistics on "Internet of Things (IoT)" [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ [Accessed: March. 2018].

[6] Guan, W., 2018. Copyright Anti-Circumvention & Free Trade. Journal of World Trade, 52(2), pp.257-279.

[7] Wang, J., 2018. Copyright Limitations and Exceptions for Education and Research: Unity in Diversity. In Conceptualizing Copyright Exceptions in China and South Africa (pp. 49-89). Springer, Cham.

[8] Nath, B. and Kushwaha, R., Mformation Software Technologies Llc, 2015. Providing dynamic group subscriptions for M2M device communication. U.S. Patent 8,942,191.

[9] Lindholm, F. and Hallenstål, M., Telefonaktiebolaget LM Ericsson, 2015. Terminal identifiers in a communications network. U.S. Patent 9,026,082.

[10] Kahn, R. and Wilensky, R., 2006. A framework for distributed digital object services. International Journal on Digital Libraries, 6(2), pp.115-123.

[11] Hoang, T. and Yang, L., 2013, April. Scalable and transparent approach to media archive using digital object architecture. In Proceedings of the 46th Annual Simulation Symposium (p. 6). Society for Computer Simulation International.

[12] Jerez, H.N., Khoury, J., Abdallah, C. and Piovesan, J., 2018. The internet transient network architecture: A comparative description. Google Scholar.

[13] Berber, F. and Yahyapour, R., 2017, August. A High-Performance Persistent Identifier Management Protocol. In Networking, Architecture, and Storage (NAS), 2017 International Conference on (pp. 1-10). IEEE.

[14] "The DONA Foundation." [Online]. Available: https://dona.net/ [Accessed: March. 2018].

[15] Proceedings of the World Telecommunication Standardization Assembly (Hammamet, 2016)

[16] "Digital Object Architecture for IoT." [Online]. Available: http://www.wileyconnect.com/home/2016/11/8/what-governments-decided-on-digital-object-architecture-for-iot [Accessed: March. 2018].

[17] Dory, J.R., Hanes, D.H. and Dowdy, J.G., Hewlett-Packard Development Co LP, 2018. Near Field Communication (NFC) Data Transfer. U.S. Patent Application 15/717,429.

[18] Ahson, S.A. and Ilyas, M., 2017. RFID handbook: applications, technology, security, and privacy. CRC press.

[19] Skarmeta, A., Hernández-Ramos, J.L. and Bernabe, J.B., 2015, December. A required security and privacy framework for smart objects. In ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015 (pp. 1-7). *IEEE*.