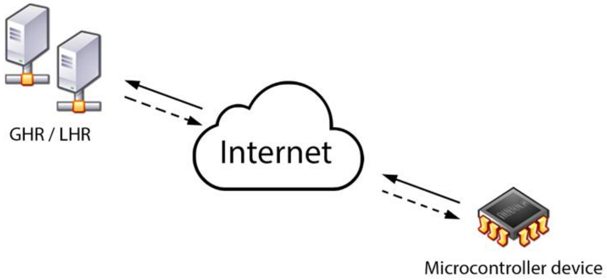
UDC 621.396

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

Approbation of methods of identification of devices of Internet things on the basis of architecture of digital objects

To test the detection of Internet of Things devices based on the architecture of digital objects, a laboratory bench was developed, which was allocated to a specific object of the identified device using a Handle server via the Internet. During the experiment, a device identification scenario was considered using intermediate verification device.



.

Fig. 1. Schematic representation of the interaction of elements in the identification of IoT devices based on DOA (traditional approach)

The laboratory stand for identification of IoT devices was developed with the introduction of a new component (in contrast to the traditional approach) - the level of object verification in the DOA system. The stand consist of the following components (Fig. 2):

1) Handle-server containing information about the identified device;
2) the Internet as a network infrastructure;
3) end device (IoT device or identifiable entity); any other;
4) an additional level of object verification in the Digital Object Architecture system.

Considering the differences between the main components of the system, it is worth noting the combination of the Global Handle Register and Local Handle Register into one object for testing on a laboratory bench, the study participants were given access to the DOA test zone with the “11.test” prefix, which allows them to place their own identifiers in the existing system Digital Object Architecture. In the future, this makes it possible to evaluate many characteristics of the developed system at the application level.

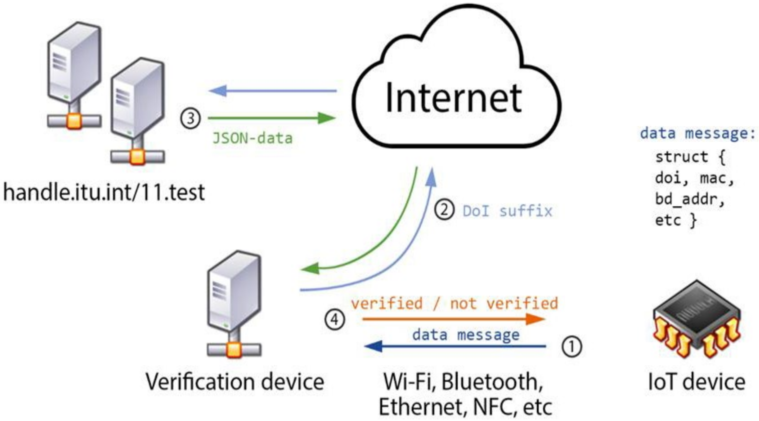


Fig. 2. The modernized concept of the DoA-based device identification system using the verification level

The verification level was represented by a software and hardware complex with a set of network interfaces that allow connecting many different devices, both through direct physical interaction (NFC technology) and through network interaction (BLE, WiFi).

The end device can be either an IoT device or a regular object, the verification of which is necessary in some context.

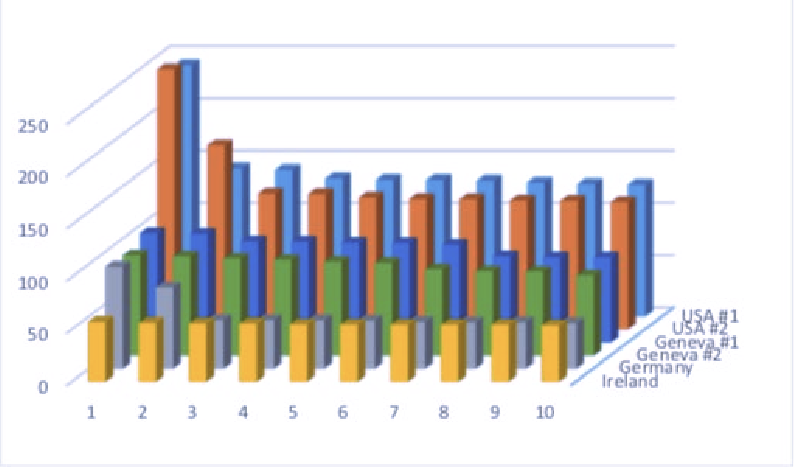
The process of verifying a device with a DOA identifier occurs in stages:

1) using one of the available interfaces, an appeal is made to the verification device, which includes the transfer of a data array containing the digital identifier of the object, as well as data that directly checks the validity of the object - MAC address, BLE address, date of sale of the product , unique product number, etc.;
2) the verification device determines the required server for the request, sends a request to the specified object identifier;
3) The handle-server responds to the request with a JSON array containing the necessary fields, including the fields responsible for checking the object for compliance;
4) the verification device compares the received data according to the given fields, gives the result of the check (both to the output means and directly to the device being verified).

Analysis of the results of a natural experiment

Introducing the traditional verifier scheme will allow the average system access time to the DOA server to be determined and provide the status of the verifier. Accessing the verification device using certain technologies such as NFC or BLE introduces additional delays on the interfaces, but this is not the target scenario for this study.

Fig. 3. Graph of network delay when sending a request to different countries



Delays were measured in two cases:

1) using the CNRI proxy server system, a set of web servers, who understand the processing protocol. The system consists of four different web servers located in three different geographical areas;
2) using the main GHR server hosted in Geneva.

Table 1. Contains the latency for each server and the average latency based on ten experiments. Each request was made using the REST API, which makes it possible to process requests in JSON format. The timeslots were obtained using the packet capture software Wireshark.

Table 1.

Results of measuring the delay using different handle-servers

Location	Delay, ms										
	1	2	3	4	5	6	7	8	9	10	Average
USA #1	140,2	240,4	141,7	132,0	130,6	126,6	126,0	129,9	128,0	130,5	142,6
USA #2	249,2	130,0	123,2	121,9	176,4	126,2	123,4	124,7	129,6	124,8	142,9

Germany	97,6	43,6	44,4	77,6	46,4	45,9	46,2	46,5	44,4	44,8	53,7
Ireland	53,8	57,3	54,6	54,6	54,7	54,8	55,7	55,7	54,6	56,2	55,2
Geneva #1	81,5	82,5	95,2	103,9	93,5	95,4	81,5	104,5	96,8	96,5	93,1
Geneva #2	80,4	93,0	91,5	88,7	94,9	95,9	89,8	76,7	80,8	82,6	87,4

As can be seen from Table, the best latency value is observed when communicating with a server located in Germany, and the worst value is observed with a server located in the USA. Based on these values, we can conclude that in order to minimize latency, it is necessary to optimize routes for accessing GHR servers.

The composition of factors influencing the identification of the Internet of things is analyzed. The main features of identification for the Internet of Things are defined and summarized.

A full-scale experiment was carried out to study the delay in data transmission in the architecture of digital objects system. The laboratory stand was developed with the introduction of a new component (in contrast to the traditional approach) - the level of object verification in the DOA system, which allows you to connect many different devices, both through direct physical interaction (NFC technology) and through network interaction (BLE, WiFi).

Analysis of the results of a field experiment showed that the best value of the delay is observed when exchanging data with a server located in Germany, and the worst value - with a server located in the USA.

Conclusion

Thus, the device is checked through strictly defined DOA servers, protected from direct access for ordinary users, without issuing data by the requested identifier. This approach limits the possible scenarios for counterfeiting devices with a digital ID, while simultaneously offloading the end device. The resulting system in a stationary version (in the form of a stand) also makes it possible to visually demonstrate the speed of the identification process, the route of service traffic, and other parameters.

References

1. Інтернет ресурс - https://azure.microsoft.com/ru-ru/solutions/iot/iot-technology-protocols/
2. Identifiers of Internet of Things. Jurgen Heiles, Henri Barhel. 1-34p. Alliance of IoT Innovation. February 2018. Інтернет ресурс: https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf
3. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, Wei Zhao. (Internet of Things JOURNAL). Macau. 1-17p. https://ieeexplore.ieee.org/ielaam/6488907/8059894/7879243-aam.pdf