
Method for identifying network services in a network having Internet-of-Things network subscribers

The present invention relates to a method for identifying network services in a network with Internet-of-Things network subscribers.

In the field of Internet-of-Things (IoT), network subscribers (e.g. sensors and/or actuators) are typically connected to a network via cables or wirelessly to allow communication with services in the network. A communication between the network subscribers (e.g. sensors and/or actuators) and the services in the network can be based on an IP protocol, for example. For example, the search for a service on the network can be performed by a domain name system DNS-based service discovery according to the IETF RFC6763 standard. The IoT network subscribers (e.g. sensors/actuators) are typically configured so that they can communicate with a fixed network service. If the address of the network service is changed, all IoT sensors/actuators connected to it must be reconfigured, resulting in considerable effort upon each address change of the network service.

In the German patent application giving rise to a right of priority, the German Patent and Trademark Office has examined the following documents: US 2015/0341446 A1, US 2016/0127305 A1 und US 2015/0142968 A1.

It is an object of the present invention to provide a method for identifying services in a network having Internet-of-Things sensors/actuators, which enables an improved and more effective identification.

This object is achieved by a method for identifying services in a network having Internet-of-Things sensors/actuators according to Claim 1.

A method is thus provided for identifying network services in a network having at least one host which provides each network service with a network service identifier, having at least one Internet-of-Things sensor/actuator based on domain name system service discovery DNS-SD via a multicast domain name system mDNS. A domain name system service discovery DNS-SD compliant request for a network service or network service

type is sent by a network subscriber (e.g., Internet-of-Things sensors/actuators) to a network having at least one host which provides network services. The host can itself represent an IoT device. At least one domain name system service discovery DNS-SD compliant response from one of the hosts to the request is received by the sensor/actuator. The response from the hosts contains a text field with a network service identifier of the network service that matches the requested network service type on the application layer. A connection request is sent by the Internet-of-Things sensor/actuator to the host that offers the desired network service and which has a network service identifier that matches the application of the sensor/actuator. This enables a standard-compliant, simple and efficient means of providing a decentralised search for network services. By specifying the network service identifier in the text field, a filtering option for the relevant services is made possible.

According to one aspect of the invention, the network service identifier represents an identifier, an identifier of the Internet-of-Things network subscriber and/or of the associated network service on the application layer. Optionally, the identifier can be freely or substantially freely selected by the user when setting up a system. The user thus determines the name of the network service identifier and/or of the associated IoT network subscriber on the application layer. This enables improved addressing of the respective network service identifiers and/or the respective IoT network subscribers.

According to one aspect of the invention, the domain name system service discovery DNS-SD compliant response comprises, in addition to the host address information consisting of host URL and a port number, an application-layer service identifier in the TXT field, which according to the standard is only optional. With the aid of these, the IoT sensor/actuator can dynamically identify the service associated with it independently and distinguish it from other similar services in the local network. In other words, instead of a modifiable, purely structural address (IP address or host name), the identification can be performed on a static identifier on the application layer without the need to use or maintain a mapping table.

This allows the IoT network subscribers, e.g. IoT sensors/actuators, to independently identify those hosts that offer the network service required by the IoT sensors/actuators and connect to them via the IP protocol, so that the IoT sensors can transmit their data via the network to the network service. This leads to significantly reduced configuration effort and the IoT sensors/actuators carry out the search, the identification and the connection to the network services independently. This is made possible by suitably enrich-

ing the response of the host with IoT application-specific information. In a response in a DNS SD over mDNS the text field TXT indicates the IoT application to which a network service belongs. With this information, a remote station can dynamically learn how to address the network service being sought, which is assigned to an IoT application, in order to enable communication.

According to one aspect of the invention, a distributed identification of central network services of a distributed IoT application can take place in the local network. The network service is identified by an entry in a text field TXT of an mDNS-SD compliant response. The entry in the text field can have an application-layer identifier.

According to another aspect of the invention, the multicast domain name system mDNS optionally represents a wide-area mDNS. The network services can thus also be identified in distributed local networks.

According to another aspect of the invention, the Internet-of-Things sensors/actuators and/or the hosts are optionally addressed based on IPv6 link local addresses. This leads to a further reduction in the effort involved in configuring the IoT sensors/actuators.

According to one aspect of the invention, the IoT sensors/actuators themselves can be service providers in an IoT application, e.g. an IoT temperature sensor can offer a thermometer service. Thus, IoT sensors/actuators simultaneously act as hosts. Furthermore, there are many other conceivable services on hosts in the network, e.g. a web-based status display (dashboard), which displays the data from the IoT sensors/actuators. The method is suitable for identifying any kind of local IoT services and thus allows all combinations of the identification, which is also optionally mutual, of IoT sensors/actuators and hosts.

According to one aspect of the invention, distributed IoT network subscribers can identify entries by means of the application identifier of the components in the text field TXT of the announced mDNS-SD. Further actions can then be performed, such as a software update or a firmware update.

Further embodiments of the invention are the subject matter of the dependent claims.

Advantages and exemplary embodiments of the invention are elucidated below with reference to the drawing.

Fig. 1 shows a schematic view of a process sequence of a search for services in a network according to a first exemplary embodiment of the invention, and

Fig. 2 shows a schematic view of DNS-SD information when searching for services in a network.

5

The invention relates to an Internet-of-Things (IoT) infrastructure, in which a plurality of IoT network subscribers (e.g. IoT sensors, actuators, wireless transmitters/receivers etc.) can communicate over a network (e.g. the internet or a local network) with other components, such as hosts that provide network services. The communication of the sensors, actuators and/or the wireless transmitters/receivers with a network as well as with hosts in the network is based on an IP protocol. As an option, IoT network subscribers (IoT sensors/actuators and/or wireless transmitters/receivers) can act as hosts. The search, for example, by the IoT network subscriber for an associated network service uses DNS-SD over mDNS (domain name system-service discovery via multicast domain name system, see standard: IETF RFC 6762). The IoT network subscriber requires a network service to be able to communicate and transmit data or measurements to the network service. The network service, in turn, is used to receive this data and optionally to control or transmit commands to the IoT network subscriber.

According to one aspect of the present invention, specific names or individual identifiers can be assigned to the respective IoT network subscribers or the associated network services. For example, the identifiers can represent TI211-temperature collector input. Optionally, the identifiers or the descriptors or names of the respective IoT network subscribers can be defined by the user.

Fig. 1 shows a schematic representation of a process sequence of a search for services according to a first exemplary embodiment of the invention. According to the first exemplary embodiment, a service discovery, i.e. a search for a network service, is performed based on mDNS. An IoT network subscriber 100 (e.g. sensor/actuator) sends a request 1 (mdns request) for a network service of a specific type 11 into the connected network 300. A plurality of hosts 210, 220, 230 that provide network services are connected to the network 300. If any of the hosts 210, 220, 230 provides the network service of the requested type 11, the host 210, 220 responds with an mDNS-SD announcement 2, 3. The request 1 and the responses 2, 3 are made in a service discovery phase SDP. Each response 2, 3 (mDNS announcement) comprises the address information consisting of network name 13 (consisting of host name 13a and domain 13b) and port 14, as well as

25

30

the service identifier on the application layer 12, where the latter is contained in a text field TXT of the response 2, 3. The application identifier 12 can be used to identify the associated network service that is sought. If the IoT network subscriber (e.g. sensor/actuator 100) has identified the correct network service using the application identifier 12, a connection request 4 is made in a Service Using Phase SUP from the IoT sensor/actuator 100 to the corresponding host 210 providing the required network service. The IoT Sensor 100 uses the address information from the mDNS-SD announcement consisting of network name 13 and port number 14.

This allows an IoT sensor/actuator 100 to achieve an independent and dynamic connection to a desired network service. Advantageously, configuration of IP addresses, for example, is no longer necessary.

According to one aspect of the present invention, a user can identify the IoT network subscribers 100 and/or the associated network services in their system with their own identifiers. These specific identifiers can appear in the text field TXT so that a user can directly recognize IoT network subscribers and/or the associated network services in their identifier structure (naming system of the IoT network subscribers and/or the associated network services). This is advantageous because it means the user does not need a mapping table (application identifier to the IP address; infrastructure address or structural address). In addition, a mapping table of a bus address is thus required in non-IP-based systems.

For example, an identifier for an IoT temperature sensor and/or the associated network service can be represented by Tlxxx. For example, the identifier for a valve can be represented by Vxxx. Optionally, the user can implement the respective identifier for the IoT network subscribers/network service on the basis of a system diagram or a system structure, which is to be enabled by its being controlled by the IoT network subscribers.

According to one aspect of the invention, IPv6 link local addresses are used in the allocation of the IP addresses. This allows the hosts 210 - 230 and the network subscriber 100 to allocate or assign the IP addresses themselves. This is again advantageous, as it no longer requires central administration.

Fig. 2 symbolically shows the mDNS-SD request by means of an available mDNS user program. In line (1) the request is made as to which hosts offer the service of type 11, and then the program displays a list (lines 2 and 3) with information on hosts that re-

sponded to the request with an announcement, including the server name (13a) and the domain (13b). In line 5, the mDNS user program is prompted to display further information about the found host that is known from the announcement. This includes the network name 13, the port number 14, and the service identifier on the application layer
5 12 (i.e., its own identifier for the respective IoT network subscriber). The latter was transmitted in the text field TXT of the mDNS-SD announcement.

According to one aspect of the present invention, the IoT network subscriber can be configured as a wireless transmitter/receiver or a wireless client.

The wireless transmitter/receiver can perform IP-based communication with the network
10 based on a WiFi protocol, LTE protocol, 5G protocol, or a Bluetooth protocol.

Claims

1. Method for identifying network services (210 - 230) in a network (300) having at least one host which provides each network service with a network service identifier (12), and with at least one Internet-of-Things network subscriber in the form of at least one Internet-of-Things sensor/actuator and/or wireless sender/receiver (100) based on domain name system service discovery DNS-SD via a multicast domain name system mDNS, having the steps:

transmitting a domain name system service discovery DNS-SD compliant request (1) for a network service type (11) from an Internet-of-Things network subscriber (100, 210, 220, 230) to the network (300) having the at least one host that provides network services;

receiving at least one domain name system service discovery DNS-SD compliant response (2, 3) from one of the hosts (210 - 230) to the request (1),

wherein the response (2, 3) comprises a text field (TXT) having a network service identifier (12) of the network service corresponding to the requested network service type, and

transmitting a connection request (4) from the Internet-of-Things network subscriber (100) to the host (210 - 230) to which the network service identifier (12) in the response is assigned and which provides the desired network service.

2. Method for identifying network services in a network according to Claim 1, wherein the network service identifier in the text field (TXT) corresponds to an identifier of the Internet-of-Things network subscriber (100, 210, 220, 230) and/or to the associated network service on the application layer.

3. Method for identifying network services (210 - 230) in a network (300) according to Claim 1 or 2, wherein address information of the searched for host, which comprises a network name (13) and a port number (14) of the host (210 - 230), is not known to the requesting network subscriber in advance.

4. Method for identifying network services (210 - 230) in a network (300) according to Claim 1, 2 or 3, wherein the multicast domain name system mDNS is a wide-area mDNS.

5. Method for identifying network services (210 - 230) in a network (300) according to any one of Claims 1 to 4, wherein
the Internet-of-Things network subscribers (100) and/or the hosts (210 - 230) are
5 addressed based on IPv6 link local addresses.
6. Method for identifying network services (210 - 230) in a network (300) according to any one of Claims 1 to 5, wherein
the host (210, 220, 230) can represent one of the Internet-of-Things network sub-
10 sscribers (100).