Context Based Service Discovery in Unmanaged Networks Using mDNS/DNS-SD

Milosh Stolikj, Pieter J. L. Cuijpers, Johan J. Lukkien, *Senior Member, IEEE*, and Nina Buchina
Dept. of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands

***Abstract*—We propose an extension of the mDNS/DNS-SD service discovery protocol, which enables service clients to discover and select services based on their context. The extension improves scalability in large networks, which is of particular importance in future Internet of Things deployments.**

I. Introduction

The penetration of *Internet of Things* (IoT) is gradually changing the consumer market. The explosion in number of devices woven into our physical world, and embedded with communication and processing capabilities, enables many novel applications, like smart homes, home automation systems, connected wearables etc. In a future where the number of devices with which an end-user can interact, grows at an astounding rate, a crucial step is the discovery of such devices and the services they provide in an automatic fashion.

Figure 1 depicts the process and goal of service discovery: service clients discover service providers in a distributed context where neither one knows the existence of the other. Service discovery protocols achieve this goal by defining 1) a language for describing services and selection criteria; 2) a protocol for exchanging service descriptions; 3) rules for matching service descriptions with selection criteria.

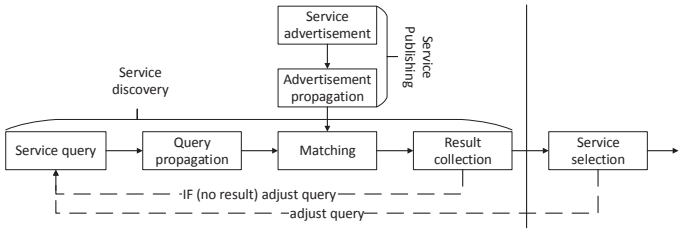


Fig. 1. The service discovery process. The service clients issues a query that is matched by the service advertisement of the service provider. In a distributed context, these tasks can be performed by different entities.

The focus in the IoT is on protocols which are confined to the local network scope and do not require central management. Furthermore, the protocols should be standardized by the Internet Engineering Task Force (IETF), in order to guarantee wide acceptance. Previous studies [1] [2] have identified Multicast Domain Name System (mDNS) [3] with DNS-Based Service Discovery (DNS-SD) [4], a standards-based protocol, with light footprint, good scalability and wide usage, as a potential solution for service discovery in the IoT. In this work, we extend the protocol with a context-based model for describing and discovering services, which enables better scalability in large networks.

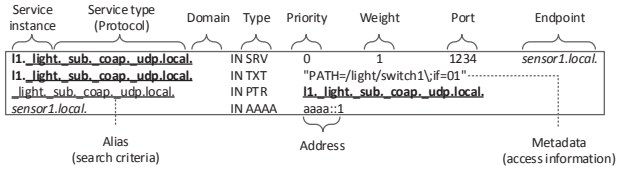


Fig. 2. DNS-SD description of a light sensor service. The four RRs are connected through the name of the service.

II. Service Discovery using mDNS/DNS-SD

mDNS/DNS-SD is a combination of protocols for distributed service discovery in zero-configuration networking. It consists of two components: a communication protocol defined by mDNS, and a service discovery and service description protocol defined by DNS-SD. mDNS foresees a distributed environment, where resolution information is stored locally on each device within the local network, and each device directly answers to incoming name resolution queries. In that sense, every participating device acts both as a server and a client. DNS-SD is a protocol for describing and resolving services using DNS Resource Records (RR). DNS-SD defines how a client can leverage DNS queries to discover service instances within a logical domain using the service type as selection criterion. DNS-SD describes service instances using four RRs, as in Figure 2. Services are distinguished by their structured name, in the form *"<Name>.<Type>.<Domain>"*. The first part of the name is a unique identifier of the service instance. The service type is formed by concatenating the application protocol and the transport protocol used for accessing the service instance. Lastly, the domain defines the service scope.

In the current standard, the only available selection criterion is the service type, with additional descriptions added in text (TXT) RRs. Therefore, for selecting a service with specific context, a client must gather the descriptions of all services of the same type, and then select the most appropriate one. This reduces the scalability of the protocol in large networks, where many service instances of the same type may co-exist.

III. Context Based Service Discovery for mDNS/DNS-SD

Two approaches to improve the protocol have been proposed. The first approach [5], customizes DNS-SD for building control, where services are selected based on location and sub-protocol. Location information is added as part of the domain name, while the sub-protocol is added via the type/subtype options. The second approach [6], uses TXT RRs inside

978-1-4673-8364-6/16/$31.00 ©2016 IEEE

queries as a way to impose constraints for service selection. TXT RRs contain key-value pairs of features requested by the client. Service providers respond only if their own TXT RRs contain all entries from the query TXT RR.

While both approaches are an improvement over the current DNS-SD standard, neither is ideal. The former approach lacks flexibility and is tightly coupled with location as the primary discriminator, and the latter approach imposes additional overhead in the size of the queries. Therefore in [7], an analysis is performed on different design choices for including context in the DNS-SD protocol. Here, we present the most promising solution, which is a mixture of the previous two approaches.

We define that any given service instance can be associated with a set of context tags. A context tag is an atomic descriptor of one context property. The presence or absence of a context tag indicates whether or not the associated service instance has that specific context. These context tags are pre-configured at commissioning time, or are learned from the environment at run time. Service discovery then consists of sending one or more queries, listing a combination of wanted/unwanted context tags. As a response, a set of descriptions is expected, whose sets of tags satisfy the queries. We use boolean logic to express the queries, using conjunction ($\wedge$, denoted by '*'), disjunction ($\vee$, denoted by '.') and negation ($\neg$, denoted by '-') operators. Finally, after the combination of context tags, we add the service type and the logical domain.

Our approach reduces the number and the size of the messages required for discovery, at the expense of increased processing complexity. However, due to the simplicity of the query language, this should have limited impact on the discovery time. Furthermore, the context tags are stored in compact form, and require less memory space than both storing fully qualified domain names, and storing key-value pairs, as used in the other two approaches.

IV. Comparison

We compare the three approaches using the following scenario. Assume a network of one client and two service providers (Table I). The client searches a light switch for blue lights in office 1. For the first approach (Figure 3a), one additional RR is created, which contains the location in the domain name. The light color is part of the TXT RR. The client first discovers all light switches for office 1, and from the received TXT responses, finds the correct instance.

When TXT RRs are used as part of the query, all context features are encoded inside a new TXT RR (Figure 3b). The client sends the TXT RR as part of the query. Only responses that satisfy this query are expected.

Finally, with our approach, only one PTR RR is sent as a query, containing all requested context (Figure 3c) with a similar effect as the previous.

V. Conclusion

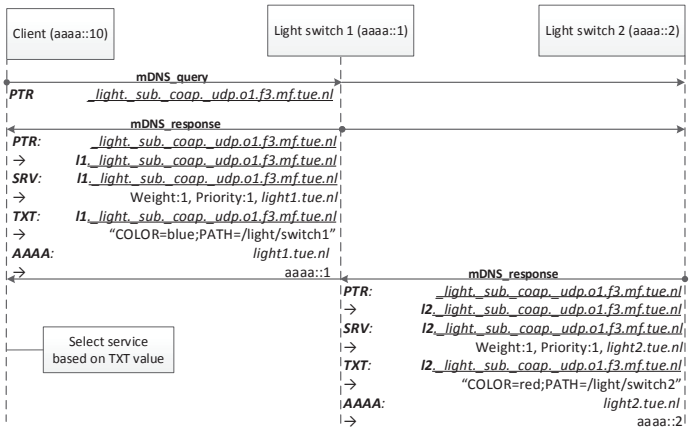
In this paper we presented an extension of the mDNS/DNS-SD protocol for service discovery, which enables services to be described and discovered based on their context. Compared to other similar approaches, the extension is backward compatible with the existing standard, has a well defined structure and has more expressive power. The extensions improves the protocol's scalability in large networks, which is of particular importance for large scale IoT deployments.

Acknowledgments

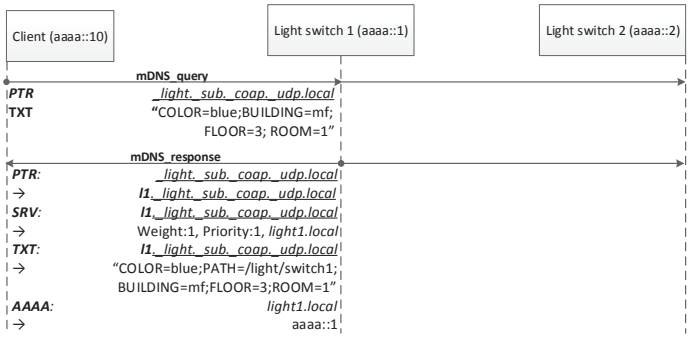
This work is supported in part by the Dutch P08 SenSafety Project, as part of the COMMIT program.

TABLE I
Description of test scenario.

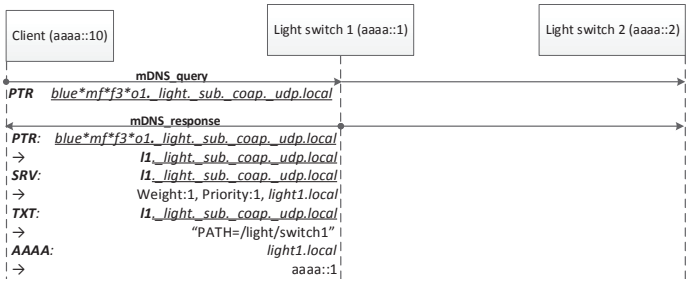
Property	Light switch 1	Light switch 2
Service type	_light._sub._coap._udp.local	
Location	MetaForum (**mf**), Floor 3 (**f3**), Office 1 (**o1**)	
Color	blue	red
Resource path	/light/switch1	/light/switch2



(a) Location in domain name.



(b) TXT records as part of queries.



(c) Context-based model.

Fig. 3. Approaches to context-based mDNS/DNS-SD service discovery.

978-1-4673-8364-6/16/$31.00 ©2016 IEEE

REFERENCES

[1] R. Klauck and M. Kirsche, "Bonjour Contiki: A Case Study of a DNS-based Discovery Service for the Internet of Things," in *Ad-hoc, Mobile, and Wireless Networks*, ADHOC-NOW, pp. 316–329, 2012.

[2] M. Stolikj, R. Verhoeven, P. J. Cuijpers, and J. J. Lukkien, "Proxy support for service discovery using mDNS/DNS-SD in low power networks," in *World of Wireless, Mobile and Multimedia Networks*, WoWMoM, 2014.

[3] S. Cheshire and M. Krochmal, "RFC 6762: Multicast DNS." http://www.ietf.org/rfc/rfc6762.txt, 2013.

[4] S. Cheshire and M. Krochmal, "RFC 6763: DNS-Based Service Discovery." http://www.ietf.org/rfc/rfc6763.txt, 2013.

[5] P. van der Stok and K. Lynn, "CoAP Utilization for Building Control." http://tools.ietf.org/html/draft-vanderstok-core-bc, 2012.

[6] A. Aggarwal, "Optimizing DNS-SD query using TXT records." http://tools.ietf.org/html/draft-aggarwal-dnssd-optimize-query, 2014.

[7] N. Buchina, "Extending service discovery protocols with support for context information." Master Thesis, TU Eindhoven, 2014.

978-1-4673-8364-6/16/$31.00 ©2016 IEEE