

Proposta de auto-registro de serviços pelos dispositivos em ambientes de IoT

Caio C. M. Silva, Francisco L. de Caldas, Felipe D. Machado, Fábio L. L. Mendonça e Rafael T. de Sousa Jr.

Resumo— Este artigo apresenta uma abordagem de auto-registro de serviços de dispositivos em ambientes de IoT. Em contraponto a trabalhos em que a iniciativa de registro cabe a entidades centrais do *middleware*, a proposta estrutura-se para que o próprio dispositivo seja capaz de registrar seus serviços e, usando sensibilidade ao contexto, o dispositivo especifique as informações dos serviços que devem ser propagadas na IoT. Com a proposta desenvolvida em termos de especificação de informações de contexto do dispositivo e do fluxo de interação entre o dispositivo e o *middleware* de IoT, resultados experimentais são obtidos comparando o desempenho da abordagem proposta com relação à abordagem centrada no *middleware*.

Palavras-Chave— Internet das coisas (IoT), Serviços de IoT, Abstração de Dispositivos, Sensibilidade ao contexto.

Abstract— This article presents an approach to self-registration of device services within IoT environments. In counterpoint to works in which the registration initiative lies to *middleware* core entities, the proposal is structured so that the device itself is able to register its services and, using context awareness, the device specify services information that should be propagated in the IoT. With the proposal developed in terms of device context information specification and interaction flow between the device and the IoT *middleware*, experimental results are obtained which compares the performance of the proposed approach to the *middleware*-centric approach.

Keywords— Internet of Things (IoT), IoT Services, Device Abstraction, Sensitivity to Context.

I. INTRODUÇÃO

A quantidade de dispositivos de Internet das Coisas (IoT) está em contínuo crescimento, apontando para uma magnitude de milhões de dispositivos em um futuro próximo. Tal número, associado à variedade de serviços providos por tais dispositivos, pode constituir um cenário impeditivo para o gerenciamento desses dispositivos e serviços, caso não sejam utilizadas abordagens avançadas para o seu registro e organização em uma rede IoT.

A bem da exatidão, devemos nos referir não apenas a uma única, homogênea e coesa Internet das Coisas, mas às várias encarnações ou instâncias de Internet das Coisas. A Figura 1 ilustra uma situação comum de um dispositivo celular multifuncional transportado por uma pessoa que

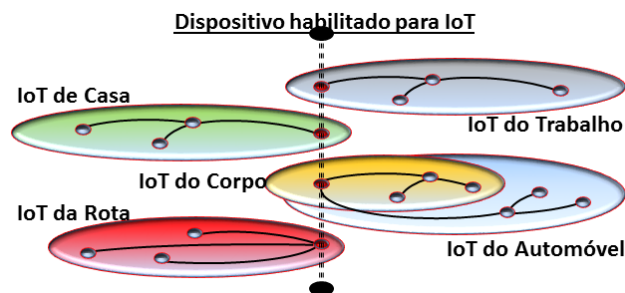


Fig. 1. Diferentes contextos para um dispositivo de IoT

dirige um veículo entre sua casa e o trabalho. Tal dispositivo participa simultaneamente de diversas instâncias de IoT, sendo cada instância na verdade uma rede sobreposta (*overlay network*) sobre a infraestrutura fixa e móvel da Internet. O dispositivo tem diferentes papéis em cada instância de IoT e a situação se modifica continuamente em função de diversos fatores, em particular o movimento.

Assim, além das instâncias de IoT envolvendo aplicações com dispositivos estáticos, de limitada e fixa capacidade de armazenamento, processamento e comunicações, evidencia-se que se apresentam cenários com aparelhos móveis inteligentes (por exemplo: celulares multifuncionais, acessórios pessoais, controladores de bordo em veículos e dispositivos embarcados), cada um deles podendo estar presente simultaneamente em diversas instâncias de IoT. Tais instâncias envolvem potencialmente diferentes plataformas de hardware e sistema operacional, *middleware* de IoT, protocolos de comunicação, modelos de dados, políticas de segurança, tipos de aplicações, etc.

Em vista disso, um determinado dispositivo pode ter simultaneamente diversos papéis, desde o de sensor simples sob controle de outra entidade, ou a operação como par idempotente de outro dispositivo, até atuar como o próprio controlador principal de uma aplicação completa de IoT. Nessa situação, podendo simultaneamente ofertar diversos serviços, sob condições diferenciadas, e que podem se modificar a qualquer instante (por exemplo, em função da mobilidade, ou da capacidade energética restante, ou de decisões de usuários, etc.), é importante haver sensibilidade ao contexto tanto pelo dispositivo, quanto pelas possíveis aplicações em que esteja contribuindo.

De fato, concordamos com [1] quando afirma que, do ponto de vista conceitual, a Internet das coisas refere-se a entidades que atuam como fornecedores e/ou consumidores de dados relacionados com o mundo físico, ou seja, a IoT tem foco em dados e informação, em vez de tecnologias de comunicações e protocolos. Se, por um

Caio C. M. Silva, Francisco L. de Caldas, Felipe D. Machado, Fábio L. L. Mendonça e Rafael T. de Sousa Jr., Laboratório de Tecnologias da Tomada de Decisão, Faculdade de Tecnologia, Universidade de Brasília, DF, Brasil, E-mails: {caio.silva, francisco.lopez, felipe.duarte, rafael.desousa, fabio.mendonca}@redes.unb.br. Os autores agradecem à Agência de pesquisa, desenvolvimento e inovação FAPDF (Protocolo 11454.54.34054.17052016), e à Defensoria Pública da União (Acordo de Cooperação 30/2014 DPU-FUB), pelo suporte ao presente trabalho.

lado, entende-se IoT como um sistema altamente dinâmico e distribuído em rede, onde um número muito grande de objetos inteligentes produzem e consomem informação, por outro lado, há uma perspectiva cuja questão principal consiste em relacionar e integrar as funcionalidades e recursos fornecidos pelos objetos inteligentes, compondo-os na forma de serviços e correspondentes de fluxos de dados gerados.

Conforme analisa [2], o trato da heterogeneidade e da escalabilidade são fundamentais em um sistema complexo e dinâmico como esse, levando à necessidade de pouca intervenção humana, devendo os dispositivos oferecer auto-capacidades, notadamente elevado grau de autonomia configuração, auto-organização e auto-adaptação a vários cenários, auto-reação a eventos e estímulos, e auto-processamento de enormes quantidades de dados trocados. No presente artigo, propomos atribuir responsabilidades dessa ordem ao dispositivo de IoT, valendo notar, ainda de acordo com [2], que o uso de contexto é necessário para a operacionalização de serviços eficientes capazes de funcionar em ambientes dinâmicos e compostos por grande quantidade de nodos que podem ser mover, causando repentinos aparecimentos ou desaparecimentos dos serviços, a qualquer tempo.

Já [3] propõe um novo paradigma de IoT cognitiva, em que coisas físicas ou virtuais são interconectadas e interagem segundo um ciclo percepção-ação sensível ao contexto, mas o próprio artigo adverte sobre a necessidade de fazer a ponte entre a teoria e a prática desse paradigma. O presente artigo tem justamente o propósito de desenvolver a ideia de registro por iniciativa do dispositivo, a ponto de concretizar experimentos de avaliação dos resultados, o que é feito utilizando um middleware de IoT existente [4].

Por outro lado, a IoT pode ser vista a partir de duas perspectivas, centrada na rede e centrada na coisa (objeto ou dispositivo), a primeira com foco em serviços providos pela rede usando dados providos pelos dispositivos e, a segunda, com foco em serviços de dispositivos inteligentes [5]. No presente artigo, argumentamos que a perspectiva centrada no dispositivo é mais adequada para o registro de serviços dos dispositivos, argumento este sustentado em evidências empíricas obtidas pelos resultados da avaliação experimental da proposta concebida e implementada.

O artigo [6] afirma que as aplicações sensíveis ao contexto são capazes de se adaptar continuamente a ambientes e funções muito complexas e dinâmicas, na presença de movimento e de dispositivos e sistemas heterogêneos, o que requer a percepção de processos e conteúdo de duas formas de contexto, físico e virtual. Os contextos físicos envolvem percepções de dispositivos sensores, como velocidade, aceleração, pressão, luz, localização, movimento, som, tato e temperatura. Os contextos virtuais são especificados pelos usuários ou capturados a partir das interações dos usuários, suas preferências, interesses, objetivos e tarefas. Neste artigo, propomos que o dispositivo participe ativamente na integração das duas visões, oferecendo, na forma de serviços, sua capacidade operacional e a informação adequada para cada instância de aplicação de IoT. Nesta proposição, o dispositivo atua na fase de

aquisição do contexto dentro do ciclo de vida do contexto [7] usado pela aplicação ou instância de IoT.

Embora evidencie-se que a segurança é um requisito imprescindível na participação de um dispositivo em uma ou várias instâncias de IoT, seguimos neste artigo o argumento de [8] segundo o qual a lógica de funcionamento da aplicação deve ser separada das políticas de execução da segurança. Assim, este artigo é dedicado à investigação de uma proposta de funcionalidade para o dispositivo de IoT, de modo a permitir o teste da efetividade e do desempenho dessa funcionalidade, considerando para outro estudo o aspecto da segurança.

Tendo em vista tais considerações, neste artigo é proposta uma abordagem para que o próprio dispositivo possua o controle sobre os serviços que disponibiliza, e tome a iniciativa de atualizar a rede sobre novas informações relativas a cada um de seus serviços, visando aumentar a escalabilidade da rede, além de possibilitar um melhor controle sobre a heterogeneidade dos dispositivos.

O trabalho está organizado da seguinte forma: a seção II traz uma breve discussão sobre os trabalhos relacionados à pesquisa. O processo de auto-registro do dispositivo e o conjunto de informações de contexto utilizadas são apresentados na seção III. Na seção IV são apresentados os resultados experimentais. Finalmente, conclusões e trabalhos futuros são apresentados na seção V.

II. TRABALHOS RELACIONADOS

Alguns trabalhos de pesquisa em IoT adotam uma abordagem orientada a serviço para atender os requisitos de topologias de rede dinâmicas. Enquanto alguns projetos focam na abstração dos dispositivos na forma de serviços de rede [9] [10] [11] [12], outros dedicam atenção às abstrações de informações/dados e sua integração com os serviços [13] [14] [15].

Um desafio comum para as diversas soluções supracitadas é o desconhecimento da topologia utilizada, questão usualmente tratada com processos de descoberta (*discovery*) de serviços/dispositivos em grande parte com base nas abordagens tradicionais utilizadas na Internet, ou em ambientes ubíquos e redes de sensores e atuadores sem fio [16] [17]. Por exemplo, SOCRATES [12] provê a descoberta em dois níveis, designados como nível do dispositivo e nível do serviço, neles utilizando ou o WS-Discovery para serviços web (*web services* - WS) ou um mecanismo de descoberta RESTful (para serviços *representational state transfer* - REST). Nos citados trabalhos, também é possível identificar que a abordagem para descoberta dos serviços disponíveis é realizada sob responsabilidade de uma entidade central da rede.

Em contraposição, o presente artigo propõe a ideia de que um dispositivo deva realizar o seu auto-registro em uma rede IoT, de modo que cada dispositivo possa atuar de forma autônoma na rede, realizando requisições somente para os nós com os quais haja interesse de interação. Para que seja possível habilitar a operação de auto-registro, cada dispositivo deve ser capaz de entender o contexto computacional em que está inserido, podendo este contexto ser entendido como o conjunto de todos os aspectos técnicos relacionados às capacidades e recursos computacionais [18].

Mais especificamente, o contexto computacional possui dois objetivos principais, um deles sendo expressar a heterogeneidade que normalmente está presente em ambientes de IoT, inclusive as diferentes capacidades computacionais dos dispositivos e os aspectos de conectividade [19] [20]. Já o segundo objetivo é considerar os diferentes recursos que um dispositivo de IoT encontra enquanto está em *roaming* [21]. Isso posto, a utilização de informações de contexto permite que o dispositivo possa reduzir a quantidade de dados comunicados [22] sem prejuízo ao funcionamento da rede IoT.

Assim, a abordagem de auto-registro do dispositivo com sensibilidade ao contexto favorece a escalabilidade da rede IoT, dado que tem o efeito resultante de diminuir o tráfego de dados na rede, além de contribuir para descoberta dos dispositivos e serviços.

III. PROPOSTA DE AUTO-REGISTRO DE SERVIÇOS

Nesta seção é apresentada a proposta de auto-registro de serviços pelos dispositivos em ambientes de IoT, sendo apresentadas as contribuições e as respectivas subseções onde são tratadas no artigo. Primeiramente, discrimina-se o conjunto de informações de contexto que habilitam o processo de auto-registro, servindo para estabelecer a identificação e os serviços do dispositivo em uma rede IoT, conforme detalhado na subseção III-A. Em seguida, define-se o fluxo de informações para o registro de serviços em uma rede IoT, cujos passos são apresentados na subseção III-B.

A. Informações de contexto

Nesta subseção são apresentadas as informações de contexto relevantes para permitir o registro de serviços em um ambiente de IoT. Cada conjunto de informações foi organizado como um “documento” que deve ser enviado pelo dispositivo para a rede IoT. Foram definidos três tipos de documentos: **documento de identidade**, **documento de registro** e **documento de atualização**.

É importante ressaltar que os documentos foram definidos utilizando o padrão JSON, dado que esse formato utiliza uma menor quantidade de bytes para representar uma informação se comparado com outras abordagens como, por exemplo, XML [4].

1) *Documento de identidade*: O documento de identidade possui as informações relativas ao contexto computacional do dispositivo IoT. Este dispositivo deve ter a capacidade de obter essas informações, através de um algoritmo operante em seu próprio contexto, e compô-las em um documento de identidade, um exemplo do qual sendo apresentado no trecho de código em formato JSON III-A.1. As informações de **Chipset ID**, **Processor ID** e **Mac address**, são compostas e utilizadas pela rede IoT para gerar um ID único do dispositivo para a rede. Já o **host name** é utilizado pela rede para enviar informações ao dispositivo quando necessário, e para permitir (ou negar) envios de requisições do dispositivo para a rede.

```
{id_cps : 4C4C4544004731108047B4C04F4C3232,
 id_prc : 51 06 04 00 FF FB EB BF,
 hd_srl : W761TTGL, driver : ethernet,
 mac : 74:e6:e2:ce:23:6d, host : rpy-iot}
```

As informações sobre as tecnologias de comunicação são utilizadas pela rede IoT para identificar a tecnologia mais adequada para realizar a troca de informações, além de permitir uma maior disponibilidade do dispositivo. É importante ressaltar que por princípio uma rede IoT deve ser capaz de comunicar uma determinada informação independentemente da tecnologia de comunicação utilizada. Como discutido em [23], ambientes de IoT devem suportar diferentes formas de comunicação de maneira transparente para os clientes.

O dispositivo deve primeiramente enviar o documento de identidade para a rede IoT, recebendo em resposta um *id token* que será utilizado nas interações seguintes. Nestas, o dispositivo deve informar, com o *idtoken*, o endereço físico (mac) para que seja possível identificar por qual interface de comunicação a requisição foi enviada.

2) *Documento de registro*: O dispositivo IoT deve informar quais são os serviços que ele deseja oferecer para a rede, realizando o registro dos serviços através do documento de registro. Neste, cada serviço é caracterizado por quatro informações: nome, tipo da informação, unidade da informação e descrição. Um exemplo desse documento encontra-se no trecho de código JSON III-A.2.

```
{id_token : 11768768, mac : 74:e6:e2:ce:23:6d,
 services:[{name : get_temp, type : float,
 unit : celsius, desc : temp sensor}]}
```

Podendo um determinado dispositivo oferecer mais de um serviço, no documento de registro deve estar inserida uma lista com todos os serviços que o dispositivo deseja oferecer para o middleware. Além da coleção de serviços, é necessário que seja inserido no documento o *id token* válido e o *MAC* do dispositivo. O *MAC* deve ser enviado para que seja verificado se um determinado dispositivo trocou sua interface de rede, podendo essa troca ser caracterizada como um comportamento suspeito.

Na resposta ao envio do documento de registro, a rede vai informar o identificador de cada serviço cadastrado, bem como o tempo de envio das informações para cada serviço requisitado ao dispositivo.

3) *Documento de atualização*: Este terceiro documento serve ao envio das informações coletadas pelo dispositivo, ou seja, para cada serviço cadastrado, o dispositivo deve enviar as pertinentes informações coletadas. Por exemplo, caso o dispositivo tenha cadastrado um serviço para informar a temperatura, outro para informar a humidade e outro para enviar informações de autenticação de RFID, tal dispositivo deve usar um documento de atualização para enviar a temperatura atual, a humidade a atual e se houve alguma tentativa de autenticação por RFID. Um exemplo de um documento de registro encontra-se no trecho de código JSON III-A.3.

```
{id_token : 11768768, mac : 74:e6:e2:ce:23:6d
 services:[{id_serv : 001, value: 24}]}
```

O dispositivo sabe quando deve enviar uma informação relativa a um serviço, pois a rede IoT terá fornecido esse parâmetro na operação de registro do serviço.

B. Processo de registro

O processo de registro entre o dispositivo e a rede IoT, com a separação de seus componentes e interações, é apresentado na figura 2.

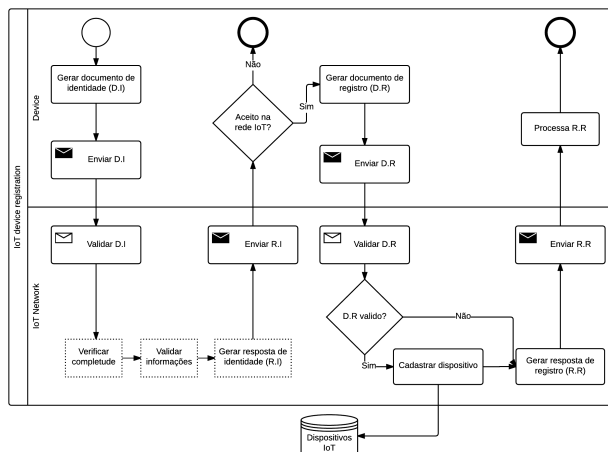


Fig. 2. Processo de auto-registro de serviços para dispositivos IoT

O processo se inicia com o próprio dispositivo gerando o documento de identidade, o que requer capturar suas informações, inseri-las no documento de identidade e enviar este último para a rede IoT. A rede recebe o documento e realiza o processo de validação (PV) do documento, em três fases fundamentais:

- **Verificar completude:** Nesta fase é verificado se todas as informações necessárias para gerar a identidade do dispositivo estão disponíveis no documento. Caso alguma informação não tenha sido enviada, o dispositivo não será aceito na rede IoT. Avaliar a completude é um dos requisitos fundamentais para se garantir a qualidade de contexto [24].
- **Validar as informações:** É verificada a validade de cada informação, processo este que ocorre através de definições de políticas de contexto [22]. Cada informação possui um conjunto de políticas que a definem como válida ou não.
- **Gerar resposta de identidade:** A resposta de identidade contém um código informando se a operação foi bem sucedida ou não, na forma de uma mensagem especificando o código e o *id token* caso o dispositivo tenha sido aceito na rede. Um exemplo dessa resposta é apresentado no trecho de código JSON III-B.

```
{code : 200, id_token : 11768768}
```

Tendo a rede gerado e enviado a resposta para o dispositivo, este será responsável por interpretar o documento e avaliar se foi aceito ou não pela rede. Caso não tenha sido aceito, o dispositivo deve iniciar todo o processo novamente. Porém, se o documento de identidade foi validado pela rede, o dispositivo deve assumir o *id token* como seu identificador único, e gerar o documento de registro, este informando a especificação de cada um dos serviços que o dispositivo deseja realizar na rede IoT. Após gerar o documento de registro, o dispositivo deve enviá-lo à rede, que, ao receber o documento, realiza o respectivo processo de validação. Caso o documento de registro seja válido, os serviços são registrados em um banco de dados do middleware de IoT. Caso contrário, o pedido é desconsiderado, sendo gerada uma resposta negativa para o dispositivo.

O documento de resposta de registro contém um código informando se a operação foi realizada com sucesso ou não, e, em caso de sucesso, uma lista de serviços que discrimina, para cada serviço informado pelo dispositivo, o nome do serviço, o id do serviço e o *refreshing time*. O nome na lista é o mesmo nome provido pelo dispositivo, o id do serviço representa o identificador único do serviço gerado pela rede, e o *refreshing time* é o intervalo de tempo requisitado ao dispositivo para envio das informações relativas ao serviço. O trecho de código JSON III-B apresenta um exemplo de resposta para documento de registro.

```
{code : 200, services:[{name : get_temp,
id_serv : 001, timing : 60}]}
```

Por fim, após receber uma resposta de sucesso da rede IoT, o dispositivo está registrado na rede com seus serviços associados e, a partir desse momento, passa a enviar os documentos de atualização dentro da especificação de *refreshing time* fornecida pela rede.

IV. EXPERIMENTOS E ANÁLISE DOS RESULTADOS

Com a finalidade de validar a proposta, foram realizadas duas implementações do *middleware* de IoT, ambas configuradas em um equipamento servidor e respectivamente denominadas **servidor ativo** e **servidor passivo**. Para efeito dos testes, no caso ativo, o servidor é responsável pela descoberta dos serviços, enquanto, no caso passivo, são os dispositivos que devem enviar ao servidor as informações sobre os serviços. O ambiente experimental é apresentado na tabela I.

Verifica-se então o tempo de resposta do servidor à medida que cresce o número de dispositivos registrados no *middleware*. Para realizar os testes, foi utilizada a ferramenta JMeter. O cenário de teste se inicia com o regitro de um dispositivo e a cada segundo seguinte registra-se outro dispositivo continuamente, até o limite de trezentos mil dispositivos. Cada dispositivo envia informações no intervalo de [1, 2] segundos. Para cada requisição, coleta-se o tempo de resposta do servidor passivo e do ativo. A figura 3 apresenta o valor médio do tempo de resposta à medida que cresce o número de dispositivos na rede.



Fig. 3. Relação entre número de dispositivos e tempo de resposta

Os resultados indicam que, com o aumento no número de dispositivos registrados na rede, o tempo de resposta aumenta para ambas as abordagens, mas o servidor ativo

TABELA I
ESPECIFICAÇÃO DO AMBIENTE EXPERIMENTAL

Nó	SO	Processador	Memoria	Armazenamento	Simulador
Dispositivos	Ubuntu 14.04	Intel i5 2.5GHz	4GB	1TB	JMeter
Middleware	CentOS 6	Intel XEON 2.79GHz	32GB	4TB	Apache

tem tempo de resposta até 42% maior que a servidor passivo. De fato, a diferença no tempo médio de resposta entre duas abordagens está no intervalo de [-1.2, 1358] ms, ou seja, a abordagem por iniciativa do dispositivo é até 1,3s mais rápida em média.

Além disso, à medida que aumenta a escala do sistema, evidencia-se o aumento gradativo na diferença entre as duas abordagens, tendo os experimentos indicado, para cenários com mais de trinta mil dispositivos, que a abordagem por iniciativa do servidor tem tempo de resposta 38% pior, no melhor dos casos. Assim, há indicador de que tal abordagem pode ser impeditiva para ambientes IoT com uma magnitude estimada de milhões de dispositivos.

Em síntese, há evidência de que a utilização de uma abordagem onde o dispositivo informa seus serviços e seu estado corrente ao middleware de IoT, isto é, quando o dispositivo realiza seu auto-registro, contribui com a escalabilidade desse middleware de IoT.

V. CONCLUSÕES E TRABALHOS FUTUROS

Este artigo propõe uma abordagem para auto-registro de serviços pelos dispositivos em ambientes de IoT, argumentando que os dispositivos de IoT devem ser sensíveis ao contexto e ser capazes de identificar seus próprios serviços e enviá-los à rede. Para tanto, os dispositivos devem enviar documentos de identificação, registro e atualização, documentos estes que possuem informações de contexto sobre o ambiente em que o dispositivo se encontra.

Resultados experimentais coletados da implementação indicam que a abordagem proposta favorece a escalabilidade da rede IoT, tendo em vista os tempos de resposta das requisições serem até 42% menores em relação a abordagem onde tal iniciativa cabe a uma entidade central do middleware, especialmente em cenários em que aumenta a quantidade de dispositivos na instância de IoT.

Para trabalhos futuros, sugere-se o refinamento do modelo de contexto, para caracterizar todo o ambiente em que um dispositivo de IoT está inserido. Além disso, objetiva-se realizar processamentos de filtragem no próprio dispositivo para que a quantidade de informações por ele veiculadas na rede seja ainda mais reduzida.

REFERÊNCIAS

- [1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
- [2] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.
- [3] Q. Wu, G. Ding, Y. Xu, S. Feng, Z. Du, J. Wang, and K. Long, "Cognitive internet of things: a new paradigm beyond connection," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 129–143, 2014.
- [4] C. C. de Melo Silva, H. G. C. Ferreira, R. T. de Sousa Júnior, F. Buiati, and L. J. G. Villalba, "Design and evaluation of a services interface for the internet of things," *Wireless Personal Communications*, pp. 1–38.
- [5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [6] D. Zhang, H. Huang, C.-F. Lai, X. Liang, Q. Zou, and M. Guo, "Survey on context-awareness in ubiquitous media," *Multimedia tools and applications*, vol. 67, no. 1, pp. 179–211, 2013.
- [7] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.
- [8] A. Rizzardi, S. Sicari, D. Miorandi, and A. Coen-Porisini, "Aups: An open source authenticated publish/subscribe system for the internet of things," *Information Systems*, 2016.
- [9] M. Eisenhauer, P. Rosengren, and P. Antolin, "Hydra: A development platform for integrating wireless devices and sensors into ambient intelligence systems," in *The Internet of Things*. Springer, 2010, pp. 367–373.
- [10] W. Zhang and K. M. Hansen, "Semantic web based self-management for a pervasive service middleware," in *Self-Adaptive and Self-Organizing Systems, 2008. SASO'08. Second IEEE International Conference on*. IEEE, 2008, pp. 245–254.
- [11] M. Presser, P. M. Barnaghi, M. Eurich, and C. Villalonga, "The sensei project: integrating the physical world with the digital world of the network of the future," *Communications Magazine, IEEE*, vol. 47, no. 4, pp. 1–4, 2009.
- [12] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services," *Services Computing, IEEE Transactions on*, vol. 3, no. 3, pp. 223–235, 2010.
- [13] D. Massaguer, B. Hore, M. H. Diallo, S. Mehrotra, and N. Venkatasubramanian, "Middleware for pervasive spaces: Balancing privacy and utility," in *Middleware 2009*. Springer, 2009, pp. 247–267.
- [14] J. Honkola, H. Laine, R. Brown, and O. Tyrkko, "Smart-m3 information sharing platform," in *The IEEE symposium on Computers and Communications*. IEEE, 2010, pp. 1041–1046.
- [15] K. Aberer, M. Hauswirth, and A. Salehi, "Infrastructure for data processing in large-scale interconnected sensor networks," in *Mobile Data Management, 2007 International Conference on*. IEEE, 2007, pp. 198–205.
- [16] F. Zhu, M. W. Mutka, and L. M. Ni, "Service discovery in pervasive computing environments," *IEEE Pervasive computing*, no. 4, pp. 81–90, 2005.
- [17] E. Meshkova, J. Riihijärvi, M. Petrova, and P. Mähönen, "A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks," *Computer networks*, vol. 52, no. 11, pp. 2097–2128, 2008.
- [18] G. Chen, D. Kotz *et al.*, "A survey of context-aware mobile computing research," Technical Report TR2000-381, Dept. of Computer Science, Dartmouth College, Tech. Rep., 2000.
- [19] A. Bartolini, M. Ruggiero, and L. Benini, "Visual quality analysis for dynamic backlight scaling in lcd systems," in *Proceedings of the Conference on Design, Automation and Test in Europe*. European Design and Automation Association, 2009, pp. 1428–1433.
- [20] S. Ceri, F. Daniel, M. Matera, and F. M. Facca, "Model-driven development of context-aware web applications," *ACM Transactions on Internet Technology (TOIT)*, vol. 7, no. 1, p. 2, 2007.
- [21] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," in *Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on*. IEEE, 1994, pp. 85–90.
- [22] C. Silva and M. Dantas, "Quality-aware context provider: A filtering approach to context-aware systems on ubiquitous environment," in *WiMob*, 2013, pp. 422–429.
- [23] H. Kopetz, "Internet of things," in *Real-time systems*. Springer, 2011, pp. 307–323.
- [24] Y. Kim and K. Lee, "A quality measurement method of context information in ubiquitous environments," in *Hybrid Information Technology, 2006. ICHIT'06. International Conference on*, vol. 2. IEEE, 2006, pp. 576–581.