Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 370-380
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

Segurança em Infraestrutura para Internet das Coisas

Infrastructure Security for Internet of Things

Airton A. de Jesus Junior[1], Edward David Moreno[1]

[1]Universidade Federal de Sergipe, UFS, Brasil

Correspondência: Airton A. de Jesus Junior, Endereço: DCOMP/PROCC. Av. Marechal Rondon, s/n Jardim Rosa Elze - CEP 49100-000 - São Cristóvão/SE. E-mail: airton2junior@gmail.com

Recebido: 14 de outubro de 2015 Aceito: 26 de março de 2016 Publicado: 09 de maio de 2016

Resumo

O conceito de Internet das coisas (*Internet of Things* - IoT) pressupõe que objetos comuns possam estar interligados à Internet, de modo a dotá-los da inteligência necessária para interagir e, de algum modo, auxiliar a vida das pessoas por meio da coleta de dados físicos, processamento e promoção de respostas através de atuadores eletromecânicos. Além do desenvolvimento de tecnologias há de se efetuar a pesquisa e o tratamento dos aspectos de segurança aplicáveis em infraestrutura para Internet das coisas. Dessa forma, este artigo visa primeiro repassar os conceitos teóricos básicos sobre os elementos que compõe a infraestrutura para Internet das Coisas, com destaque para rede de sensores sem fio, *middleware* e computação em nuvem. Em seguida o trabalho faz um levantamento e discute os desafios e soluções adequadas para a segurança em infraestrutura para Internet das Coisas, em específico a necessidade de manutenção da privacidade dos usuários como também a busca pela interoperabilidade entre os diversos dispositivos inteligentes. Ao final o estudo realiza uma comparação de algumas implementações em infraestrutura para Internet das Coisas em termos de atendimento aos requisitos de segurança da informação: confidencialidade, integridade, disponibilidade, autenticação, controle de acesso e não repúdio e registra os desafios e trabalhos futuros na área.

Palavras-chave: Desafios; segurança; infraestrutura; Internet das coisas; *Framework*.

Abstract

The concept of Internet of things (Internet of Things - IoT) assumes that ordinary objects can be linked to the Internet in order to provide them with the necessary intelligence to interact and, somehow, help people's lives through the collection Physical data processing and promoting responses through electromechanical actuators. Besides developing technologies imperious the research and treatment of the safety aspects applicable to Internet of Things infrastructure. Thus, this article aims to first pass the basic theoretical concepts about the elements that make up the Internet of Things infrastructure, especially wireless sensor network, middleware and cloud computing. Then the work is a survey and discusses the challenges and solutions designed for security infrastructure for Internet of Things, in particular the need to maintain the privacy of users as well as the search for interoperability between different smart devices. At the end of the study makes a comparison of some implementations in infrastructure for the Internet of Things in terms of compliance with information security requirements: confidentiality, integrity, availability, authentication, access control and non-repudiation and records the challenges and future work in the area.

Keywords: Challenges; security; infrastructure; Internet of Things; Framework.

1. Introdução

Até o presente, podemos considerar que a principal forma de comunicação da Internet ocorre entre seres humanos, todavia, alguns estudiosos afirmam que a nova tendência da rede será a implantação da Internet das coisas (*Internet of Things*, IoT). A Internet das coisas promoverá a conectividade de todos e de tudo (KHAN et al, 2012).

Para proceder esta mudança de paradigma na Internet, de computadores interconectados para coisas interligadas, faz-se necessária a pesquisa e a simplificação quanto ao processo de desenvolvimento e a operação de aplicações e serviços de tecnologia da informação. De modo a direcionar os esforços dos desenvolvedores para o que essencialmente importa: o enfrentamento da demanda dos usuários, poupando tempo e recursos com questões de

infraestrutura. *Middleware* visa enfrentar este desafio, ao prover uma abstração da infraestrutura (CHAQFEH et al., 2012).

Dentre as tecnologias a serem integradas no contexto da infraestruturua para IoT tem-se destaque para a rede de sensores sem fio (*Wireless Sensor Network* - WSN) e a plataforma de computação em nuvem (*Cloud computing* - Cloud). A adoção conjunta destas tecnologias decorre do antagonismo e da complementaridade existente entre ambas (LEITÃO et al., 2012). Ademais, o modelo de computação em nuvem vem se tornando adequado para suportar as demandas, naturalmente dinâmicas, geradas por aplicações que trabalham com monitoramento e modelagem de ambientes naturais (LEE et al., 2010).

Da mesma forma que mais facilidades são oferecidas pela computação em nuvem, tais como a computação sobre demanda e a modalidade de pagamento sobre o que efetivamente se usa, algumas questões de segurança, privacidade e interoperabilidade comprometem a credibilidade desta plataforma computacional. A justificativa encontra-se no fato do consumidor não possuir o domínio dos ativos computacionais, de modo a implementar os controles que julgar conveniente (ALMORSY et al., 2011). Por outro lado, estudos apontam a necessidade de se implementar maiores níveis de proteção em rede de sensores sem fio antes de se adotá-la de forma irrestrita (KUMARI et al., 2010).

Este artigo visa, em princípio, analisar alguns dos recentes trabalhos que abordam os desafios de segurança em infraestrutura para IoT, de forma a acentuar os principais aspectos de segurança a serem atendidos quanto à especificação e o desenvolvimento de soluções para Internet das coisas. Este estudo está dividido nas seguintes seções: segunda seção apresenta-se os fundamentos teóricos em infraestrutura para Internet das Coisas; terceira seção dedica-se a levantamento dos trabalhos correlatos; quarta seção discutiu-se os aspectos e tratamentos de segurança nos trabalhos encontrados; quinta seção identifica-se desafios e trabalhos futuros e na sexta faz-se a conclusão.

2. Fundamentação Teórica

Para o avanço da Internet das coisas exige-se o enfrentamento de alguns desafios. Dentre estes, destacam-se a interoperabilidade e a segurança em infraestrutura para IoT, de modo a promover a fácil e segura integração entre os diversos dispositivos inteligentes. Por exemplo, faz-se necessária a elaboração de novos modelos de representação da informação contextual (CASTELLI et al., 2007), assim como o desenvolvimento de abstrações capazes de facilitar o desenvolvimento de aplicações e serviços suportados por pequenos objetos heterogêneos, tendo-se em vista facilitar a vida das pessoas (MCEWEN e CASSIMALLY, 2013). Para tanto, faz-se necessário repassar alguns conceitos utilizados na infraestrutura da Internet das Coisas, especialmente: rede de sensores, middleware e computação em nuvem.

2.1. Internet Das Coisas

A idéia de Internet das coisas (*Internet of Things* - IoT) sugere a ampliação da habitual perspectiva de termos apenas dispositivos de computação portáteis, tais como: *tablets*, *laptops*, *smartphones* interligados à Internet. Neste novo contexto vislumbra-se a possibilidade de termos um enorme conjunto de dispositivos do cotidiano (roupas, espelho, sapatos, geladeira, bracelete) munidos de limitado processamento, todavia, aptos a interagir no ambiente em que se encontram, graças a intercomunicação que possuem com a rede mundial de computadores, Internet.

Dentre as possibilidades de aplicação da Internet das coisas temos o desenvolvimento de serviços para coleta e comunicação de dados existentes no meio ambiente. Por exemplo, em serviços públicos temos aplicação para as áreas de transporte, saúde, educação e segurança, como também em ambientes privados: domicílio e escritórios, permitindo, inclusive, o emprego nos diversos domínios econômicos e sociais, tais como: indústria, comércio e defesa (KHAN et al., 2012).

A Internet atual utiliza a pilha de protocolos TCP/IP para prover a comunicação entre inúmeros hosts em rede. Esta tecnologia foi idealizada para um contexto restrito, a intercomunicação de computadores institucionais (TAN e WANG, 2010). Todavia, com a presente perspectiva de conectar bilhões de objetos que, por sua vez, elevarão o tráfego e a necessidade de armazenamento dos dados, emerge a necessidade de se especificar um modelo computacional adequado a esta realidade. A arquitetura de comunicação proposta deve enfrentar alguns fatores, tais como: escalabilidade, interoperabilidade, confiabilidade, QoS etc (KHAN et al, 2012).

A arquitetura de infraestrutura para Internet das Coisas proposta pelos autores Tan e Wang (2010) e Wu et al. (2010) é basicamente dividida em cinco camadas:

a) camada de percepção (*device layer*): responsável pelo levantamento dos aspectos físicos e interação com o meio, formada de objetos, sensores e atuadores;

b) camada de rede (*transmission layer*): camada que transmite, de forma segura, a informação coletada no estrato anterior para os sistemas de processamento apropriados;

c) camada *middleware*: esta camada visa abstrair a especificidade tecnológica subjacente, provê o gerenciamento

dos serviços e a ligação com a estrutura de armazenamento de dados;

d) camada de aplicação: faz o gerenciamento global dos serviços providos pela camada de *middleware* nas áreas de saúde inteligente (*smart health*), cidade inteligente (*smart city*) etc;

e) camada de negócio: responsável pela gestão de toda a infraestrutura para IoT.

Para efeitos de simplificação deste estudo, consideraremos as camadas da infraestrutura para IoT sob três perspectivas: rede de sensores (camadas de percepção e rede), *middleware* e computação em nuvem (camadas de aplicação e negócio).

2.2 Redes de Sensores Sem Fio

Um dos dispositivos obrigatórios para emprego na camada de percepção da infraestrutura para IoT é o sensor, ou também conhecido como nó de sensor, elemento pequeno e autônomo responsável pela coleta e comunicação dos dados físicos do ambiente (CHAQFEH et al., 2012).

O sensor é basicamente um dispositivo eletrônico, leve e minúsculo, dotado de restrita capacidade de processamento, reduzida memória, memória *Flash* ou EEPROM, um minúsculo sistema operacional e outros utilitários, um ou mais sensores, propriamente dito, um fraca unidade de transmissão/recepção (*transceiver*), bateria ou unidade de captação de energia solar e, opcionalmente, um módulo de locomoção (DWIVEDI e VYAS, 2010).

Uma rede de sensores sem fio (*Wireless Sensor Network* - WSN) é o emprego de uma elevada quantidade de sensores geograficamente dispersos num ambiente físico, sem o apoio de qualquer infraestrutura física estabilizada. Pressupõe-se que os nós de sensores serão individualmente capazes de monitorar o meio, coletar o dado para, quando possível, processá-lo localmente e, em seguida, enviá-lo a um ou mais pontos de coleta: *gateway*, *sink* ou estação base, por meio da comunicação sem fio, *wireless* (DWIVEDI e VYAS, 2011).

A distribuição dos sensores no ambiente depende dos requisitos da aplicação e do espaço geográfico de interesse. A dispersão pode ser normal, quando planejado e fixo, ou aleatória, quando os nós são aleatoriamente posicionados no espaço, e, por fim, móvel, quando os nós possuem meios de locomoção. Esta informação torna-se importante devido ao fato de que a distribuição influencia diretamente no desempenho e na escolha do protocolo de roteamento dos sensores, e, consequentemente, no consumo de energia (DWIVEDI e VYAS, 2011).

Alguns estudos visam otimizar o roteamento e o tempo de vida da rede de sensores: (DWIVEDI e VYAS, 2010), (SHARMA e THAKUR, 2014) e (LIU, 2012). Entretanto, restam alguns obstáculos que merecem ser solucionados, dentre os quais se tem destaque para a segurança e a privacidade das informações coletadas, sem, no entanto, elevar de forma considerável a consumo de energia e a sobrecarga de processamento numa rede de sensores sem fio (KUMARI et al., 2010).

2.3 *Middleware* Para Internet Das Coisas

A infraestrutura para Internet das coisas, como visto, pressupõe a integração de dispositivos inteligentes, a exemplo do sensor, com camadas de maior generalização, a saber: aplicação e negócio. Para tal, duas camadas precisam de esforços de pesquisa e desenvolvimento: rede e *middleware*. Em termos de *middleware* para Internet das Coisas alguns *survey* foram identificados: (CHAQFEH et al., 2012), (BANDYOPADHYAY et al., 2011) e (ATZORI et al., 2010).

Num dos *middleware* para Internet das coisas: *SicsthSense* (MCANAMARA, 2014), os autores elaboraram uma solução aberta (*open source*) implantada em nuvem com o propósito de distribuir e armazenar fluxos de dados capturados a partir de dispositivos de limitado poder computacional. Com *SicsthSense* os dispositivos serão registrados, descobertos, configurados e programados através da plataforma de computação em nuvem, ou por meio de uma interface Web via rede local ou, ainda, de uma API de máquina para máquina, M2M.

O princípio básico da proposta (MCANAMARA, 2014) é a criação de repositório de recursos Web no qual usuários podem periódica e arbitrariamente consultar os dados coletados a partir dos dispositivos, estratificados em forma de fluxos (*streams*), acessíveis por uma URL e um website. A proposta diz também que os dados serão historicamente mantidos para fins de consulta, por exemplo, intencionando subsidiar pesquisas Big Data¸ como também poderá ser concedido e revogado o acesso conforme o interesse do usuário/proprietário.

A infraestrutura *SicsthSense* é estruturada através de interface RESTful, de modo a simplificar o projeto e desenvolvimento de aplicações cliente. A infraestrutura foi projetada tendo em vista que dispositivos IP possuem limitado poder computacional, como um nó Contiki (DUNKELS et al., 2004), usando 6LoWPAN (MULLIGAN, 2007) e RPL (KO et al., 2011). Os autores (KO et al., 2011) citam a existência de outras arquiteturas comerciais similares, como: Xively (COSM), Open.sen.se e ThinkSpeak.com, que tarifam pelo acesso aos dados ou firmam assinaturas de serviço.

O trabalho *Browsing the World* (CASTELLI et al., 2007) considera possível "navegar" ou "inquirir" informações a partir dos diversos entes/seres localizados no espaço, quer sejam animados ou inanimados. Todavia, para

tornar-se possível faz-se necessária a construção de uma representação informacional do espaço, suas entidades, processos e vida social.

A proposta vislumbra uma realidade em que os usuários poderiam a partir de dispositivos pessoais interligados (*smartphones*, luvas inteligentes etc) inquirir e recuperar dinamicamente qualquer tipo de informação dos seres a sua volta ou mesmo de qualquer outra parte do mundo. Em termos de comunicação M2M este conceito tornará possível a consciência dos objetos e a sua auto adaptação ao contexto. Neste sentido, os autores (CASTELLI et al., 2007) desenvolveram uma infraestrutura computacional baseada na modelagem de dados "W4".

Esta representação pressupõe que a maioria das informações sobre a realidade dos seres poderá ser representada através de quatro simples perguntas: *Who* (Quem), *What* (O quê), *Where* (Onde) e *When* (Quando). O modelo de representação informacional "W4", segundo os autores (CASTELLI et al., 2007), encontra-se apto a resolver estes desafios, pois muitos dos tópicos que envolvem o pensamento humano passam por estas quatro perguntas: quem é o sujeito? O que ele está fazendo? Onde e quando a ação e/ou o sujeito se encontra?

Ao final, os autores (CASTELLI et al., 2007) afirmam que, possivelmente, haverá o interesse de se explorar as diversas "redes inteligentes", das quais poderão inferir um "novo conhecimento" e, consequentemente, produzir uma determinada reação. Os autores apresentam um protótipo desta solução e exemplificam a utilização da infraestrutura e do modelo de representação "W4" no contexto dos seres (pessoas/objetos) presentes no ambiente da própria universidade. Exibem a interface de acesso a sensores e etiquetas RFID através de websites e do aplicativo Google Earth.

Numa terceira proposta de middleware, *NaturalCloud* (LEITÃO et al., 2012), os autores desenvolveram uma plataforma escalável para integração de rede de sensores sem fio com qualquer provedor computacional em nuvem. Os autores projetaram e desenvolveram uma plataforma, *NaturalCloud*, que visa atender aos critérios que julgaram necessários para solucionar o problema da integração existente entre rede de sensores sem fio e computação em nuvem.

A solução *NaturalCloud* (LEITÃO et al., 2012) foi desenvolvida basicamente em três módulos: *gateway*, nuvem e aplicação que interagem entre si bidirecionalmente. O primeiro módulo se chama módulo *gateway*, instalado junto a rede de sensores, mais precisamente na estação base (*gateway*), tem como principal função integrar uma nova rede de sensores à estrutura *NaturalCloud*. A partir da conclusão do processo de integração, passa a ser possível a troca de informações entre os módulos *gateway* e nuvem, consequentemente, o módulo nuvem passa a conhecer informações sobre cada um dos nós da rede (id, fabricante, atributos suportados) e, finalmente, os dados são compartilhados, permitindo o seu acesso através de consultas efetuadas pelo módulo nuvem.

Para demonstrar a aplicabilidade da plataforma (LEITÃO et al., 2012), efetuou-se um estudo de caso que analisou o contexto de redes de radares de trânsito existentes em três cidades e com densidade distintas: Cidade A (40 sensores); Cidade B (60 sensores) e Cidade C (90 sensores). Em seguida, efetuaram-se os testes de carga com os dados provenientes da captura de tráfego (fluxo), imagens e vídeos nos sensores. Ao final, os autores discutiram os resultados e demonstraram a eficiência e a flexibilidade da solução proposta.

2.4 Computação Em Nuvem

Outra tecnologia igualmente importante para implantação das camadas da infraestrutura IoT é a computação em nuvem, do inglês *cloud computing*. Trata-se de uma metáfora para a plataforma computacional utilitária em destaque, principalmente em virtude da expansão do acesso à banda larga, da popularização da computação móvel (*tablets* e *smartphones*), da intercomunicação de objetos inteligentes, IoT, e da disseminação de serviços e aplicativos *on-line* (LEITÃO et al., 2012).

Computação em nuvem tem se tornado uma área de grande interesse da pesquisa científica, por tratar-se da evolução e da convergência de diferentes tendências da tecnologia da informação: entrega de serviços pela Internet, pague pelo quanto se usa, elasticidade, virtualização, computação em grade, computação distribuída, armazenamento, terceirização de conteúdo, segurança e tecnologias Web 2.0 (PALLIS, 2010). Dada a dificuldade de definição, haja vista comportar tantas possibilidades de uso como também o emprego de diversas tecnologias, opta-se pela conceituação do NIST (RUSCHEL, et al., 2010, p. 4):

> *Computação em nuvem é um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (p. ex., redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e liberados com mínimo esforço gerencial ou interação com o provedor de serviços.*

Para melhor compreensão do termo, o NIST (MEL e GRANCE, 2009) também propõe que a infraestrutura de computação em nuvem possui cinco características essenciais: serviço de autoatendimento sob demanda; acesso por meio de banda larga; pool de recursos computacionais (processamento, memória, rede e armazenamento); rápida elasticidade com o propósito de prover maior escalabilidade de serviços e medição transparente da utilização dos recursos/serviços.

A computação em nuvem, por fim, apresenta três modelos de serviço: software como serviço (SaaS), plataforma como serviço (PaaS) e infraestrutura como serviço (IaaS). Como também pode ser implantada em quatro configurações: privada, comunitária, pública e híbrida (MEL e GRANCE, 2009). O detalhamento destas características e tecnologias fogem do escopo do presente estudo, mas pode ser examinada nas referências anteriormente citadas: Leitão et al. (2012), Pallis (2010), Petar (2012), Ruschel et al. (2010) e Mel e Grance (2009).

Vale destacar que a computação em nuvem trouxe, em abordagem via Internet, a possibilidade de diferentes usuários compartilharem um mesmo *pool* de recursos computacionais: memória, processador, rede, armazenamento, banco de dados, aplicações e serviços a um preço bastante atrativo. Grandes indústrias da tecnologia da informação, como Amazon, Microsoft e Google aproveitaram a oportunidade de negócio e disponibilizaram a própria infraestrutura de computação em nuvem. Esta pluralidade de provedores de serviços, no entanto, restringiu a integração e a portabilidade das aplicações hospedadas nos provedores de nuvem distintos (ZHANG, et al., 2013).

Dessa forma, a ampla adoção da plataforma em nuvem depende da superação de desafios em segurança, interoperabilidade e portabilidade (MEL e GRANCE, 2009). A razão para a demanda de interoperabilidade em nuvem varia desde: estratégia de negócio, independência de fornecedor, oscilação de preços no mercado, descumprimento no acordo do nível de serviço ou a necessidade de rápida resposta a incidente de segurança (EMEAKAROHA, et al., 2013).

3. Trabalhos correlatos

Nesta seção avaliam-se trabalhos correlatos que também discutiram os aspectos de segurança em infraestrutura para Internet das Coisas. Ao mesmo tempo, vislumbram-se algumas soluções para o adequado gerenciamento da segurança em infraestrutura para IoT.

3.1 Aspectos De Segurança Em Rede De Sensores Sem Fio

Dado que sensores manipulam informações sensíveis, tais como a intimidade, parâmetros de saúde etc, emerge a necessidade de se prover mecanismos de proteção, de modo a se garantir a manipulação dos dados sem a interferência não autorizada de terceiros.

Na pesquisa (KUMARI et al., 2010), os autores realizam a revisão bibliográfica de estudos no campo da segurança aplicada em rede de sensores sem fio. Citam o trabalho (WALTERS, et al., 2007) que elaboraram um *survey* sobre segurança em rede de sensores e também (KARLOF e WAGNER, 2003) que propuseram um modelo de roteamento seguro. Em acréscimo, Kumari et al. (2010) ressaltam alguns obstáculos estruturais na rede de sensores sem fio que dificultam o desenvolvimento de protocolos seguros, em essência a acentuada limitação de recursos: reduzida memória, pouco espaço para o código e limitada fonte de energia.

Kumari et al. (2010) denotam que a comunicação entre os sensores não ocorre de forma confiável, seja pela fragilidade inerente ao meio de comunicação, seja pela possibilidade de conflitos, ou ainda, pela latência que dificulta a sincronização de chaves criptográficas entre os dispositivos. Ressaltam as dificuldades de gerenciamento e operação da rede, como a elevada probabilidade de ataques físicos e a dispersão geográfica que dificultam a gerência remota e centralizada.

Em acréscimo, Kumari et al. (2010) destacam as principais ameaças de caráter físico e exemplificam aquelas que se apresentam em cada uma das subcamadas de comunicação: a) subcamada física: *Jamming*; b) de ligação: *Denial of Service* (DoS); c) de rede: *Selective Forwarding*, *Black hole/Sinkhole*, *Hello Flood*, *Wormhole*, *Sybil Attack*; d) de transporte: *Flooding Attack*; e) de aplicação: invasão e comprometimento dos dados da rede de sensores.

Após este levantamento, o estudo (KUMARI et al., 2010) define alguns requisitos de segurança para a rede de sensores sem fio, tais como: confidencialidade, autenticação, integridade, atualidade, disponibilidade, auto-organização, sincronização temporal e localização segura. Dentro desses requisitos enumera os possíveis ataques suscetíveis a redes de sensores sem fio, como também os correspondentes esquemas de segurança propostos na literatura.

Por fim, Kumari et al. (2010) ressaltam a adoção da abordagem holística como forma de se alcançar um maior nível de segurança, longevidade e efetividade na comunicação entre sensores, tenha ou não havido mudança no ambiente. E afirma que se garantida à segurança física deve-se proteger através de uma abordagem holística todas as subcamadas de comunicação.

No estudo Sharma et al. (2009) propõem-se a implantação transversal de uma plataforma de segurança multicamadas para o módulo de comunicação desenvolvido para rede de sensores sem fio. O trabalho ao fazer uma revisão bibliográfica do tema percebeu que a maioria das propostas se atém a uma única camada de comunicação. E, por isso, se especializou na prevenção de um único ataque. Após a avaliação destes estudos propõem a integração das soluções disponíveis em uma única plataforma de segurança escalável. Para a solução

proposta sugerem a inclusão de um novo componente, *Intelligent Security Agent* (ISA), responsável pelo provisionamento transversal de serviços de segurança entre as camadas de comunicação.

O componente ISA (*Intelligent Security Agent*) monitora o nível de segurança do sistema, avaliando se o nível projetado encontra-se de acordo com o efetivamente implantado, elimina, portanto, a falsa percepção de segurança ao identificar os riscos que precisam de atendimento. ISA sugere e aplica as contramedidas de forma efetiva e adequada, preserva intacto o protocolo de comunicação e reduz overheads. O ISA ao promover a segurança adaptativa visa incrementar o tempo de vida da rede de sensores, pois a implementação completa dos serviços de segurança nem sempre se torna apropriada ao contexto da aplicação em uso (SHARMA et al., 2009).

Sharma et al. (2009) avaliam que a abordagem holística de segurança provoca sobrecarga na rede de sensores ao promover a redundância de serviços em cada subcamada de comunicação. Exemplifica que no caso do ataque *black hole* haverá serviços redundantes tanto na subcamada de rede como na de enlace. Reafirmam que sem uma visão sistemática de segurança ter-se-á o desperdício de recursos em cada subcamada, e promoverá, até de forma não intencional, o ataque SSDoS (*Security Service DoS*). Finaliza que embora tenha observado uma evolução nas soluções de segurança em WSN, ainda prevalece a desconexão entre os resultados.

Diante deste cenário, Sharma et al. (2009) sugerem um modelo de segurança transversal e escalável com o propósito de cumprir os seguintes objetivos: robustez, simplicidade e flexibilidade. Enumeram como requisitos de segurança: robustez e confiabilidade, liderança em eleição, arquitetura de distribuição de chaves, protocolo de comunicação adaptativa e sistema de detecção de intrusão.

Para demonstrar a aplicabilidade da solução, Sharma et al. (2009) efetuam a simulação do modelo de segurança proposto sob as ferramentas Castalia e Omnet++ em três cenários distintos: Sistema de vigilância militar, monitoramento doméstico e administração agrícola, correspondendo, respectivamente, aos ambientes de elevado, médio e baixo nível de proteção. Considerou-se adequado aquele que obteve menor consumo de energia. Em cada cenário de testes adotou-se no primeiro caso a abordagem rígida de segurança, TinySec, enquanto no segundo utilizou as diretivas de segurança indicadas pelo componente ISA. Os resultados apontaram que sob cada cenário houve uma redução no consumo de energia quando se adotava a solução proposta.

3.2 Aspectos De Segurança Em *Middleware* Para Internet Das Coisas

Das propostas de middleware para IoT encontradas: *SicsthSense*, *Browsing the World* e *NaturalCloud*, muito pouco em termos de tratamento aos requisitos de segurança foi implementado, limitando-se a adoção do controle de acesso ou ao uso de criptografia na camada *WebServices*. Vê-se que estas abordagens são insuficientes para tratamento de todas ameaças existentes na infraestrutura de Internet das coisas. Principalmente devido a necessidade de se tratar as questões de segurança e privacidade dos usuários (UKIL et al., 2011).

Há um aplicativo Android, SCANDROID (*Security Certifier for anDroid*) (SCANDROID, 2015), que automatiza a certificação dos requisitos de segurança dos demais aplicativos instalados. Este sistema avalia e analisa o fluxo de dados entre as demais aplicações Android e, desse modo, pode decidir e realizar algumas ações de proteção para todo o sistema. Alternativamente, o sistema assiste o usuário na tomada de decisões relevantes para segurança do sistema (UKIL et al., 2011).

O sistema Contiki (CASADO e TSIGAS, 2009), voltado para sistemas operacionais de dispositivos inteligentes, propõe uma solução de segurança para a camada de rede de WSN, todavia, os trabalhos encontram-se ainda em desenvolvimento (DUNKELS, 2014) e, portanto, ainda iniciam a proteção dos dispositivos que gerenciam.

Adicionalmente, foi encontrado um *survey* específico de segurança em *middleware* para IoT (FREMANTLE e SCOTT, 2015). Neste estudo fizeram, primeiramente, um mapeamento dos desafios de segurança em três áreas distintas da infraestrutura para IoT: dispositivo, rede e nuvem.

Fremantle e Scott (2015) identificaram e discutiram cada uma dessas áreas de acordo com os critérios de segurança propostos no modelo CIA+ (SIMMONDS et al., 2004). Avaliaram os diversos aspectos de segurança e tratamentos adotados em vinte e dois *middleware* para IoT.

3.3 Aspectos De Segurança Na Computação Em Nuvem

O principal objetivo dos provedores de computação nuvem é facilitar a alocação de recursos de infraestrutura aos consumidores, que, por sua vez, migram dados e aplicação para a plataforma e os remuneram pela utilização dos serviços prestados. Deste modo, o consumidor ignora detalhes de infraestrutura para se concentrar nos requisitos do negócio (LEITÃO et al., 2012).

No entanto, esta situação oferece elevados riscos à segurança, na medida em que o consumidor deposita toda a confiança sobre os dados e serviços alocados unicamente no provedor de computação em nuvem. Estudos como (FERNANDES et al., 2014) avaliam esta realidade através de um levantamento das pesquisas na área da segurança em plataforma de computação em nuvem, tendo em vista a necessidade de esclarecer certas questões antes da adoção ampla desta tecnologia.

Fernandes et al. (2014) trataram de vários tópicos chave, notadamente vulnerabilidades, ameaças e ataques, propondo uma taxonomia para a classificação destes, bem como discutiram vários tópicos ainda abertos para estudo. Os autores relatam que *o National Institute of Standards and Technology* (NIST) identifica: a segurança, a interoperabilidade e a portabilidade como as maiores barreiras para uma adoção mais ampla da computação em nuvem.

Esta preocupação tem instigado a academia e a indústria na busca de soluções para os diversos problemas relatados nas pesquisas sobre o tema. A metodologia utilizada no trabalho (FERNANDES et al., 2014) foi a revisão bibliográfica de estudos desenvolvidos na indústria e na academia, a exemplo do trabalho (ZHOU et al., 2010) que elaborou um *survey* sobre segurança e preocupações com privacidade de alguns provedores de computação em nuvem. Ademais, foram discutidos brevemente problemas relacionados com o armazenamento compartilhado entre consumidores de computação em nuvem (*multi-tenancy*).

Fernandes et al. (2014) sugerem a adoção de *Virtual Private Cloud* (VPC) combinado com a possibilidade de implantação da *Intercloud*, rede interoperável de provedores de computação em nuvem, de modo a possibilitar a configuração mais adequada de segurança nesta plataforma computacional. Os autores sublinham que desta abordagem surgem perspectivas para desenvolvimento de topologias, protocolos padronizados de comunicação, modelos de confiança, identidade e gerenciamento de acesso, criptografia e gerenciamento de chaves, além de considerações a respeito da governança.

Os autores (FERNANDES et al., 2014) tratam de conceitos de segurança em nuvem, contextualizando de acordo com as diversas tecnologias que suportam este ambiente computacional: virtualização de servidores, aplicações para a Web, *Web services*, computação compartilhada entre consumidores (*multi-tenancy*), terceirização (*outsoucing*) de dados e computação e a necessidade de padronização destas tecnologias com vistas a implementação de contramedidas de segurança.

Em contrapartida, o trabalho (ALMORSY et al., 2011) propõe uma plataforma de gerenciamento colaborativo de segurança baseado no padrão NIST-FISMA (*National Institute of Standards and Technology - The Federal Information Security Management Act*), um dos principais padrões de gerenciamento de segurança da informação. Entretanto, o modelo proposto depende da mútua colaboração e integração das partes interessadas, a saber: provedores de nuvem (*Cloud Provider*, CP), provedores de serviço (*Service Provider*, SP) e consumidores (*Cloud Consumer*, CC).

Para se alcançar a implementação do sistema de gerenciamento da segurança da informação no ambiente computacional em nuvem o *framework* Almorsy et al. (2011) usa o padrão NIST-FISMA (NIST, 2015) e executa os requisitos previstos nas seis fases da norma: serviço de categorização de segurança, seleção dos controles de segurança, implementação dos controles de segurança, avaliação dos controles de segurança, serviço de autorização e serviço de monitoramento.

A arquitetura do *framework* Almorsy et al. (2011) tem três camadas: gerenciamento, aplicação e retroalimentação. A primeira camada, gerenciamento, é responsável pela captura dos requisitos de segurança das partes interessadas. A camada de aplicação é a que se compromete com a gestão da segurança em termos da seleção de controles ajustados aos riscos identificados. E a camada de retroalimentação possui dois principais serviços: monitoramento e análise dos dados coletados. A combinação destes dois últimos serviços permite alcançar as metas de segurança pré-estabelecidas.

4. Discussão

Em cada perspectiva da arquitetura de infraestrutura para IoT analisada: rede de sensores, *middleware* e computação em nuvem, constatamos que todas encontram-se expostas a ameaças de segurança e violação de privacidade dos usuários. Para melhor compreensão, confronta-se cada trabalho levantado de infraestrutura para IoT sob os serviços de segurança do modelo CIA+ (SIMMONDS et al., 2004): confidencialidade, integridade, disponibilidade, autenticação, controle de acesso e não repúdio. No quadro 1, tem-se a avaliação de segurança sobre os trabalhos expostos.

		Serviço de segurança CIA+ (SIMMONDS et al., 2004)						
Perspectiva de infraestrutura	**Soluções**	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Autenticação**	**Controle de acesso**	**Não repúdio**	**Implantação**
Rede de sensores	Kumari et al. (2010)	√	√	√				
	Sharma et al. (2009)	√	√	√				√
Middleware	Mcanamara (2014)				√	√		√
	Castelli et al. (2007)				√	√		√
	Leitão et al. (2012)	√	√	√				√
	SCANDROID (2015)	√	√	√	√	√	√	√
Computação em nuvem	Fernandes et al. (2014)	√	√	√	√	√	√	
	Almorsy et al. (2011)	√	√	√	√	√	√	√

Quadro 1: Avaliação dos aspectos de segurança CIA+ sobre os trabalhos expostos.

Na perspectiva de rede de sensores, Kumari et al. (2010) realizam um levantamento dos vários esquemas de segurança aplicáveis em camada de comunicação de acordo com os possíveis ataques a que os sensores poderiam estar submetidos. Verificam que os estudos não são integrados, e por isso, propuseram uma abordagem holística de segurança em comunicação para rede de sensores sem fio. Entretanto, o trabalho não menciona qualquer tipo de implantação nem tampouco verifica o desempenho da solução proposta.

Sharma et al. (2009), por sua vez, propõe, ao contrário de Kumari et al. (2010), uma plataforma escalável, baseada em componentes de segurança, adaptativa ao contexto, sensível aos dados e com QoS. Para tal, introduz um componente ISA (*Intelligent Security Agent*) para sugerir e aplicar, de forma efetiva e adequada, as medidas de proteção, ao mesmo tempo, preserva intacto o protocolo de comunicação e, portanto, diminui-se *overheads*. Não ficou claro em nenhum dos estudos anteriores qualquer tratamento para os serviços de autenticação, controle de acesso e não repúdio.

Na perspectiva de *middleware*, apenas SCANDROID (2015) conseguiu atender todos os aspectos de segurança avaliados: confidencialidade, integridade, disponibilidade, autenticação, controle de acesso e não repúdio. Entretanto, esta solução encontra-se restrita ao sistema operacional Android e, portanto, limitada a dispositivos de considerável capacidade de processamento, energia e memória, realidade bastante diferente da maioria dos dispositivos IoT.

NaturalCloud (LEITÃO et al., 2012) utiliza a abordagem clássica de segurança em *Web Services*, todavia esta estratégia não é suficiente para a maioria das ameaças identificadas, como também é bastante custosa em termos de recursos computacionais. As outras duas soluções, *SicsthSense* (MCANAMARA, 2014) e *Browsing the World* (CASTELLI et al., 2007), são bastantes similares em termos de tratamento aos aspectos de segurança, cada qual provê apenas a autenticação e o controle de acesso ao repositório de dados coletados. Esta abordagem é bastante comum em *middleware* para IoT, todavia, faz-se também necessária a preocupação e o desenvolvimento de soluções para os demais aspectos de segurança (FREMANTLE e SCOTT, 2015).

Por fim, na perspectiva de computação em nuvem, as propostas Fernandes et al. (2014) e Almorsy et al. (2011) avaliavam os diversos aspectos de segurança aplicáveis a computação em nuvem. O mérito do primeiro estudo (FERNANDES et al., 2014) foi a elaboração de uma ampla taxonomia dos diversos aspectos de segurança aplicáveis a computação em nuvem, no entanto, não propôs nenhuma solução para tratamento das ameaças encontradas.

Em contrapartida, a segunda solução (ALMORSY et al., 2011) propõe e implementa um *framework* colaborativo para gerenciamento da segurança na plataforma de computação em nuvem. Adicionalmente, este trabalho cita a implantação de caso de uso do *framework* numa aplicação ERP sob o ambiente SaaS, todavia sem evidenciar questões de desempenho.

5. Desafios e Trabalhos Futuros

Como desafios tem-se a necessidade de enfrentamento contínuo das constantes ameaças de segurança, em especial a autenticação dos dados, o controle de acesso e a privacidade dos usuários (CHAQFEH et al., 2012), através da implantação de sugestões apresentadas nos estudos avaliados: otimização no consumo de energia em dispositivos inteligentes, tratamento da distribuição de chaves criptográficas em sensores, implementação do conceito de Projeto por Privacidade (*Privacy by Design*) (CAVOUKIAN, 2008) e de federação de identidades para usuários e dispositivos (FREMANTLE et al., 2014), além do contínuo aperfeiçoamento dos *frameworks* de segurança em infraestrutura IoT: Sharma et al. (2009), Ukil et al. (2011) e Almorsy et al. (2011).

Para *middleware* tem-se duas formas de implementação destas iniciativas (CHAQFEH et al., 2012): a primeira é tratar a segurança em uma única camada de forma a ser considerado como um serviço adicional por todo os sistema, este é o objetivo perseguido pelo *middleware* UBIWARE (KATASONOV et al., 2008); a segunda proposta sugere a distribuição do esquema de segurança entre todas as camadas, neste último, tem-se que ter em mente a constante necessidade de redução do *overhead* sobre o desempenho e a sobrevida da infraestrutura para IoT (SHARMA et al., 2009).

Para trabalhos futuros tem-se a necessidade de desenvolver uma solução na perspectiva de rede de sensores que efetue o devido tratamento aos aspectos de autenticação, controle de acesso e não repúdio, sem, no entanto, comprometer o desempenho e sobrevida da rede de sensores, ou seja, mantendo a configuração escalável e adaptativa ao contexto sem perder a acurácia na avaliação de segurança (SHARMA et al., 2009).

Ademais, deve-se, em termos da perspectiva *middleware*, desenvolver soluções, a exemplo do SCANDROID (2015) que implementem os aspectos de segurança sob plataformas de reduzido poder computacional e que ao mesmo tempo seja interoperável, de modo a poder interagir com qualquer tipo de dispositivo inteligente. Adicionalmente, torna-se desejável que *middleware* possua uma configuração de segurança adaptada ao contexto (FREMANTLE e SCOTT, 2015).

Quanto aos próximos passos na perspectiva de computação em nuvem, da mesma forma que discutido em

middleware, tem-se a necessidade de soluções interoperáveis (DI MARTINO, 2014), ou seja, soluções genéricas de gerenciamento colaborativo de segurança, a exemplo do *framework* Almorsy et al. (2011), de forma a eliminar a dependência do consumidor para com qualquer provedor de serviços em nuvem. Pois, do contrário, estaria parcialmente atendida o aspecto da disponibilidade. Há também a necessidade do desenvolvimento do conceito de serviço de nuvem personalizado, a exemplo do Webinos PZH (FREMANTLE e SCOTT, 2015).

6. Conclusão

Este estudo teve como objetivo levantar e avaliar os aspectos de segurança em infraestrutura para Internet das coisas abordados em alguns dos recentes trabalhos desenvolvidos na área. Constatou-se, ao final, que esta complexa infraestrutura computacional encontra-se exposta a uma pluralidade de ameaças, assim como possui importantes desafios tecnológicos a serem enfrentados, com destaque para otimização de recursos e interoperabilidade.

Ao mesmo tempo, este estudo trouxe para a literatura uma análise integrada e sistemática de algumas soluções de segurança que são importantes para o aperfeiçoamento da credibilidade na infraestrutura para IoT, tendo em vista a constante necessidade de se proteger os ativos de informação, especialmente a privacidade dos usuários.

Referências

ALMORSY, Mohamed; GRUNDY, John; IBRAHIM, Amani S. **Collaboration-based cloud computing security management framework**. In: Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011. p. 364-371.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. **The internet of things: A survey. Computer networks**, v. 54, n. 15, p. 2787-2805, 2010.

BANDYOPADHYAY, Soma; SENGUPTA, Munmun; MAITI, Souvik; DUTTA, SSubhajit. **A survey of middleware for internet of things**. In: Recent Trends in Wireless and Mobile Networks. Springer Berlin Heidelberg, 2011. p. 288-296.

CASADO, Lander; TSIGAS, Philippas. **Contikisec: A secure network layer for wireless sensor networks under the contiki operating system.** In: Identity and Privacy in the Internet Age. Springer Berlin Heidelberg, 2009. p. 133-147.

CASTELLI, Gabriella; ROSI, Alberto; MAMEI, Marco; ZAMBONELLI, Franco. **A simple model and infrastructure for context-aware browsing of the world.** In: Pervasive Computing and Communications, 2007. PerCom'07. Fifth Annual IEEE International Conference on. IEEE, 2007. p. 229-238.

CAVOUKIAN, Ann. **Privacy in the clouds.** Identity in the Information Society, v. 1, n. 1, p. 89-108, 2008.

CHAQFEH, Moumena; MOHAMED, Nader. **Challenges in middleware solutions for the internet of things.** In: Collaboration Technologies and Systems (CTS), 2012 International Conference on. IEEE, 2012. p. 21-26.

DI MARTINO, Beniamino. **Applications portability and services interoperability among multiple clouds.** IEEE Cloud Computing, n. 1, p. 74-77, 2014.

DUNKELS, Adam. **A big step for Contiki: built-in encryption.** 2014. Disponível em <http://contiki-os.blogspot.com.br/2014/10/a-big-step-for-contiki-built-in.html> Acesso em: 20 de jul. de 2015.

DUNKELS, Adam; GRÖNVALL, Björn; VOIGT, Thiemo. **Contiki-a lightweight and flexible operating system for tiny networked sensors.** In: Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, 2004. p. 455-462.

DWIVEDI, A. K.; VYAS, O. P. **Network layer protocols for wireless sensor networks: existing classifications and design challenges.** In: International Journal of Computer Applications (0975 8887), v. 8, n. 12, 2010.

DWIVEDI, A. K.; VYAS, O. P. **Wireless Sensor Network: At a Glance**. INTECH Open Access Publisher, 2011.

EMEAKAROHA, Vincent C.; HEALY, Philip D.; FATEMA, Kaniz; MORRISON, John P. **Cloud Interoperability via Message Bus and Monitoring Integration.** In: Euro-Par Workshops, 2013. p. 65-74.

FERNANDES, Diogo A. B.; SOARES, Liliana, F. B.; GOMES, João V. **Security issues in cloud environments: a survey.** International Journal of Information Security. Springer Berlin Heidelberg, v. 13,n.2,set. 2014.p.113-170.

FREMANTLE, P.; AZIZ, B.; KOPECKY, J.; SCOTT, P. **Federated Identity and Access Management for the Internet of Things.** In: Secure Internet of Things (SIoT), 2014 International Workshop on. IEEE, 2014. p. 10-

17.

FREMANTLE, Paul; SCOTT, Philip. **A security survey of middleware for the Internet of Things.** PeerJ PrePrints, v. 3, p. e1521, 2015.

KARLOF, Chris; WAGNER, David. **Secure routing in wireless sensor networks: Attacks and countermeasures.** Ad hoc networks, v. 1, n. 2, p. 293-315, 2003.

KATASONOV, A.; KAYKOVA, O., KHRIYENKO, O., NIKITIN, S.; TERZIYAN, V. Y. **Smart Semantic Middleware for the Internet of Things.** ICINCO-ICSO, v. 8, p. 169-178, 2008.

KHAN, R., KHAN, S. U., ZAHEER, R.; KHAN, S. **Future Internet: the Internet of Things architecture, possible applications and key challenges.** In: Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012. p. 257-260.

KO, J., DAWSON-HAGGERTY, S., GNAWALI, O.; CULLER, D.; TERZIS, A. **Evaluating the Performance of RPL and 6LoWPAN in TinyOS.** In: Workshop on Extending the Internet to Low Power and Lossy Networks (IP+ SN). 2011.

KUMARI, Pooja; KUMAR, Mukesh; RISHI, Rahul. **Study of Security in Wireless Sensor Networks**. Proceedings of International Journal of Computer Science and Technology, v. 1, n. 5, p. 347-354, 2010.

LEE, K.; MURRAY, D.; HUGHES, D.; JOOSEN, W. **Extending sensor networks into the cloud using amazon web services.** In: Networked Embedded Systems for Enterprise Applications (NESEA), 2010 IEEE International Conference on. IEEE, 2010. p. 1-7.

LEITÃO, L. ; SAMPAIO, A. ; HOLANDA FILHO, R. **NaturalCloud: Um framework para integração de Rede de Sensores sem Fio na Nuvem.** In: X Workshop em Clouds, Grids e Aplicações WCGA, 2012, Ouro Preto -MG. Anais do X Workshop em Clouds, Grids e Aplicações, 2012. p. 44-55.

LIU, Xuxun. **A survey on clustering routing protocols in wireless sensor networks.** Sensors, v. 12, n. 8, p. 11113-11153, 2012.

MCEWEN, Adrian; CASSIMALLY, Hakim. **Designing the internet of things.** John Wiley & Sons, 2013.

MCNAMARA, L.; AL NAHAS, B.; DUQUENNOY, S.; ERIKSSON, J.; VOIGT, T. **Demo Abstract: SicsthSense-Dispersing the Cloud**. 2014.

MELL, P.; GRANCE, T. **The NIST definition of cloud computing**. NIST - National Institute of Standards and Technology, 2009.

MULLIGAN, Geoff. **The 6LoWPAN architecture**. In: Proceedings of the 4th workshop on Embedded networked sensors. ACM, 2007. p. 78-82.

NIST. Standards for Security Categorization of Federal Information and Information Systems. FIPS-199. Disponível em: <http://www.itl.nist.gov/lab/bulletns/bltnmar04.htm> Acesso em: 20 de jul. 2015

PALLIS, George. **Cloud Computing The New Frontier of Internet Computing**. IEEE Internet Computing, vol. 14, n. 5, set./out. 2010. p. 70–73

PETAR, Kocovic. **Challenges in Cloud Computing**. IPSI Transactions of Internet Research, vol. 8 n. 2, jan. 2012. p. 24-29.

RUSCHEL, Henrique; ZANOTTO, Mariana Susan; MOTA, Welton Costa. **Computação em Nuvem.** Especialização em Redes e Segurança de Sistemas. Pontifícia Universidade Católica do Paraná, 2010.

SCANDROID. Security Certifier for anDroid. Disponível em: <http://spruce.cs.ucr.edu/SCanDroid/>. Acesso em: 22 de jul. 2015

SHARMA, Ankit; THAKUR, Jawahar. **An energy efficient network life time enhancement proposed clustering algorithm for Wireless Sensor Networks**. PDCS 2014, 2014.

SHARMA, K.; GHOSE, M. K. **Complete Security Framework for Wireless Sensor Networks.** arXiv preprint arXiv:0908.0122, 2009.

SIMMONDS, Andrew; SANDILANDS, Peter; VAN EKERT, Louis. **An ontology for network security attacks.** In: Applied Computing. Springer Berlin Heidelberg, 2004. p. 317-323.

TAN, Lu; WANG, Neng. **Future internet: The internet of things.** In: Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on. IEEE, 2010. p. V5-376-V5-380.

UKIL, Arijit; SEN, Jaydip; KOILAKONDA, Sripad. **Embedded security for Internet of Things.** In: Emerging Trends and Applications in Computer Science (NCETACS), 2011 2º National Conference on. IEEE, 2011. p. 1-6.

WALTERS, J. P.; LIANG, Z.; SHI, W.; CHAUDHARY, V. **Wireless sensor network security: A survey.** Security in distributed, grid, mobile, and pervasive computing, v. 1, p. 367, 2007.

WU, M.; LU, T. L.; LING, F. Y.; SUN, L.; DU, H. Y. **Research on the architecture of Internet of things.** In: Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on. IEEE, 2010. p. V5-484-V5-487.

ZHANG, Z.; WU, C.; CHEUNG, D.W. **A survey on cloud interoperability: taxonomies, standards, and practice.** SIGMETRICS Perform. Eval. Rev. 40(4), Abril, 2013. p. 13–22.

ZHOU, M.; ZHANG, R.; XIE, W.; QIAN, W.; ZHOU, A. **Security and privacy in cloud computing: A survey**. In: Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010. p. 105-112.