FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO (NPGE/FANESE)

JOÃO PAULO ANDRADE LIMA

ESTUDO DE SEGURANÇA EM OBJETOS INTELIGENTES COM ENFOQUE EM IOT

Aracaju
2016

JOÃO PAULO ANDRADE LIMA

ESTUDO DE SEGURANÇA EM OBJETOS INTELIGENTES COM ENFOQUE EM IOT

Trabalho de conclusão de curso apresentado ao Núcleo de Pós-Graduação e Extensão da Faculdade De Administração e Negócios de Sergipe como requisito parcial para obtenção do título de especialista em redes de computadores e segurança da informação.

Orientadora: Prof.ª Maria José de Azevedo Araujo

Coorientador: Prof. Dr. Edward David Moreno Ordonez

Aracaju
2016

RESUMO

A Internet das Coisas (IoT) é uma abordagem que está em alta na literatura. Ela é definida pela inserção de objetos do cotidiano na Internet, objetivando comodidade e praticidade tanto para o ambiente familiar quanto para o ambiente de trabalho. Os dispositivos inteligentes são coisas ou objetos com processamento e comunicação que interagem entre si, porém possuem limitações. Essas restrições obrigam a academia a realizar adaptações na infraestrutura da rede mundial para o uso desse novo paradigma.

Porém, a segurança nessa "nova ideia" ainda possui muitas brechas, e na medida em que objetos do cotidiano tornam-se riscos de segurança da informação, a IoT pode distribuir esses riscos mais amplamente do que a Internet já fez. Como isto é o principal empecilho para o uso desse novo paradigma, o objetivo desse capítulo é apresentar um levantamento crítico de alguns *frameworks* de segurança atuais, analisando artigos no estado da arte que apresentam mecanismos e/ou arquiteturas para servir como base de estudo, ou até mesmo um ponto de partida para trabalhos futuros.

Palavras-chave—IoT; segurança; dispositivos inteligentes; levantamento crítico;

SUMÁRIO

1 INTRODUÇÃO

A nova tendência da atualidade é a Internet das Coisas (IoT), cujo ideia básica é a inserção e a presença de uma variedade de coisas ou objetos do dia a dia na Internet, através de esquemas de endereçamento único e que interagem uns com os outros, com o objetivo de facilitar a vida dos usuários ou de alguma maneira, tirar proveito disso. Essa interação acaba construindo uma rede bem maior do que a rede mundial de computadores, o que acaba trazendo benefícios tanto em ambientes familiar quanto em ambientes de trabalho.

Contudo, devido à diversidade na infraestrutura da Internet e dos objetos que serão inseridos, é necessária uma adaptação nas tecnologias existentes. Na verdade, essa adaptação também é necessária por causa das restrições existentes nos dispositivos, que em sua maior parte são limitações de armazenamento, processamento e energia. Em relação a esses aspectos, a academia dedicou e ainda dedica muitos esforços em relação à interoperabilidade desses dispositivos inteligentes e em soluções ou alternativas para as suas restrições.

No entanto, esse tema é mais complicado do que parece, pois em uma era em que um dos bens mais valiosos é a informação, e a Internet como está consolidada apresenta tantos riscos de segurança, uma abordagem que preza a absorção ubíqua de informações irá ampliar esse problema. De fato, destaca-se que na medida em que objetos do cotidiano tornam-se riscos de segurança da informação, a IoT pode distribuir esses riscos mais amplamente do que a Internet já fez (ATZORI *et al.*, 2010), pois um dos principais conceitos é deixar os dispositivos de forma autônoma no ambiente, o que permite a invasão de pessoas mal-intencionadas tanto logicamente como fisicamente. Então, uma questão relevante é como controlar a privacidade, segurança e confiança de informações na IoT.

A literatura começou a destinar esforços nessa área há pouco tempo, pois recentemente a necessidade de implantação de mecanismos de segurança que abordam as implicações de controle de acesso e segurança significantes, tornou-se a principal preocupação para a implantação do cenário da IoT (HERNANDEZ-RAMOS *et al.*, 2015). Muitos esforços foram aplicados no uso de mecanismos existentes para a Internet, porém por causa da configuração dos objetos, essas ferramentas ainda não puderam ser utilizadas. Devido a isso, a pesquisa nessa área está seguindo para a adaptação dos principais mecanismos para o uso em objetos inteligentes com restrições.

Como a segurança é o principal empecilho para o uso desse novo paradigma, o objetivo deste trabalho é apresentar um levantamento crítico de alguns *frameworks* de segurança para IoT atuais, analisando artigos no estado da arte que apresentam mecanismos e/ou arquiteturas que inserem privacidade,

segurança, confiança, autorização, autenticação e controle de acesso a usuários e dispositivos inteligentes. Vale ressaltar que esse trabalho serviu como base para o desenvolvimento do capítulo sete do livro "Segurança em Sistemas Embarcados Modernos – Desafios e Tendências" (MORENO, 2015) com o ISBN 978-85-69567-06-6, do mesmo autor e orientador deste trabalho.

Nas próximas seções o trabalho foi dividido em: 2. Fundamentação Teórica, 3. Análise de trabalhos correlatos, 4. Desafios e tendências e 5. Conclusões.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção é apresentada uma breve definição de temas necessários para o entendimento do trabalho. Esses assuntos estão catalogados em: abordagem geral, tipos de comunicação, protocolos, tipos de ataque e *frameworks*.

2.1 Abordagem Geral:

Nesta subseção, são abordados conceitos de várias categorias:

- Segurança em IoT:

Segurança é o conjunto de ações ou de recursos utilizados para proteger algo ou alguém, deixando estes, no estado livre de perigos, incertezas e riscos. Esse estado é desejável em tudo que nos cerca, principalmente em um mundo tão inseguro como o nosso e em dispositivos que podem ser invadidos tanto fisicamente como logicamente.

Como a arquitetura da Internet não foi projetada para os requisitos da IoT, muitos mecanismos e protocolos foram adaptados para essa nova abordagem. Porém, devido a restrições de memória, processamento e bateria, muitos dessas ferramentas não conseguem fornecer a segurança desejada. Segurança que nesse nova paradigma significa autenticação e políticas de autorização para acesso de usuários, canal seguro para trocas de mensagens, integridade de informação, disponibilidade dos recursos, entre outros.

- Objetos inteligentes:

Em IoT, objetos inteligentes são qualquer dispositivo do cotidiano que possui a capacidade de se comunicar uns com outros para realizar alguma tarefa específica. Eles se caracterizam pela presença de sensores e atuadores pelo qual eles “sentem” e atuam no ambiente, um pequeno microprocessador pelo qual eles processam os dados recebidos, um módulo de comunicação pelo qual eles trocam informação com outros dispositivos e se comunicam com a Internet e um módulo de alimentação que fornece energia para o funcionamento do dispositivo.

Mesmo com muitas características semelhantes, os objetos inteligentes podem ser muito diferentes, pois o seu comportamento depende de onde ele está e de como ele é usado.

- Cidades inteligentes:

Cidades inteligentes são definidos como cidades que utilizam a Internet das Coisas para facilitar o convívio social e o gerenciamento das atividades presentes na cidade. Alguns exemplos de atividades são: Controle de tráfego, levantamento estatístico de dados, monitoramento de segurança, prevenção de riscos, entre outros.

- Abordagem sistêmica

É uma abordagem baseada na teoria geral de sistemas e que busca contextualizar conceitos de várias áreas em torno de um objeto de pesquisa, caracterizada com a necessidade de integração de áreas para explicar o objeto como um todo.

- Abordagem cognitiva:

É uma abordagem que estuda cientificamente a aprendizagem como sendo um ponto importante no desenvolvimento do objeto, o que se assemelha a dizer que é interacionista com o ambiente ao redor. No caso de IoT, é uma abordagem em que o dispositivo inteligente aprende com o ambiente e se adapta ao mesmo.

- Abordagem holística

É uma abordagem que considera o todo levando em consideração as partes e suas inter-relações. Em IoT, foca-se na análise do objeto com os seus módulos, o qual só funciona bem com a total integração de suas partes.

- ARM (*Architectural Reference Model* - Modelo de Referência Arquitetural):

Segundo (BASSI *et al.*, 2013), o modelo ARM apresenta orientações e estruturas comuns para lidar com aspectos essenciais de desenvolvimento, uso e análise de sistemas de IoT que serve como base comum para a Internet das Coisas. Em outras palavras, além de definir as entidades, suas interações básicas e relacionamentos, o modelo ARM define as melhores práticas e orientações para transformar o modelo em arquitetura para sistemas específicos.

- REST (*Representational State Transfer*-Transferência de Estado Representacional):

A arquitetura REST é o resultado da junção de vários modelos arquitetônicos baseados em rede que fornece uma interface para conexão uniforme, que restringe a forma de compartilhar a informação, porém permite uma maior liberdade para implementação. Esse modelo arquitetônico é uma abstração do *world wide web*, realizando a conexão entre objeto e conector sem se preocupar com os detalhes da implementação nem dos protocolos utilizados.

Na verdade, essa abstração só funciona devido a elementos de informação chamados de recursos, e através de identificadores, pode-se manipular esses recursos em uma conexão cliente-servidor sem estado.

- Rádio cognitivo:

O rádio cognitivo é uma forma de comunicação *wireless*, onde o transceptor de forma inteligente e cognitiva, observa o espectro de frequência e modifica seus parâmetros para enviar ou receber a comunicação pelos canais que estiverem vazios ou com menos utilização. Isso é muito interessante, porém em IoT deve-se observar se o custo do módulo de comunicação buscar pelo melhor canal, não é alto.

- Simulador Cooja:

O simulador Cooja é um simulador flexível de rede, que foi projetado para simular redes de sensores sem fio que executam o Contiki OS (OSTERLIND, 2006). Ele é um simulador baseado em Java que permite a simulação de plataformas reais (nós), o que torna o uso dos dispositivos muito mais práticos, uma vez que após realizar os testes, o usuário só necessita descarregar o mesmo código simulado no objeto para utilizá-lo.

Um ponto interessante desse simulador é que pode simular redes com diferentes tipos de plataformas, como por exemplo, redes com nós Z1 e WiSMote, que se encaixa perfeitamente na diversidade presente no paradigma de Internet das coisas.

- Plataformas zolertia z1, WiSMote, ST GreenNet e JN5148:

É importante definir que essas plataformas representam dispositivos inteligentes e cada uma tem configuração e usos específicos.

- Criptografia de curva elíptica (ECDSA):

Em 1985 (MILLER, 1986) e (KOBLITZ, 1987) propuseram uma variação do algoritmo de assinatura digital, eles trocaram o uso das exponenciações por sistemas de criptografias baseados em curvas elípticas (cálculos realizados em cima de curvas). Essa troca foi proposta devido às operações com curvas elípticas gerarem chaves bem menores do que as com função exponencial, e proporcionar o mesmo nível de segurança. Isso garante segurança com baixo custo.

2.2 Tipos De Comunicação:

Nesta subseção, serão definidas algumas comunicações utilizadas.

- Comunicação E2E (*End-to-End* – Fim a Fim):

Comunicação fim a fim é uma comunicação em que um dispositivo/protocolo/camada só se comunica com dispositivos semelhantes da mesma categoria. Os protocolos responsáveis pelo transporte desconsideram os elementos intermediários, entregando a informação ao dispositivo semelhante. Na verdade, somente o dispositivo certo pode interpretar a informação, pois geralmente é o único que pode retirar o "cabeçalho" do pacote (no caso da comunicação de pacotes).

- Comunicação M2M (*Machine-to-Machine* – Máquina a Máquina):

Antes de falar de comunicação máquina a máquina, deve-se definir o que é telemetria. Telemetria é o ato de um sensor (ou qualquer dispositivo) registrar fatos de um ambiente, e transmiti-lo através de ondas de rádio ao objeto que vai processar essa informação.

A comunicação M2M é uma variação da telemetria. A diferença para esta é que na comunicação M2M, o dispositivo utiliza-se de uma infraestrutura de rede presente (cabeada ou sem fio) para transmitir a informação para o consumidor do que foi obtido. Essa comunicação se encaixa perfeitamente no cenário da Internet das Coisas, pois fornece interoperabilidade para os vários objetos se comunicarem.

2.3 Protocolos:

Nesta subseção, serão definidos alguns dos protocolos presentes nos mecanismos.

- CoAP (*Constrained Application Protocol* – Protocolos para Aplicações Limitadas):

Segundo o RFC 7252 (Constrained application protocol, 2014), CoAP é um protocolo de transferência web especializado para uso em dispositivos e redes restritos, que foi projetado para ser utilizado em máquinas com comunicação M2M. Em outras palavras, ele traduz o protocolo HTTP para ser utilizado em dispositivos limitados, além de fornecer *multicast*, pouca sobrecarga de cabeçalho e simplicidade.

- DTLS (*Datagram Transport Layer Security* – Segurança para Camada de Transporte de Datagramas):

O TLS (*Transport Layer Security*) é um protocolo de segurança para a camada de transporte, que fornece privacidade e integridade da informação, através da autenticação dos usuários e da aplicação de criptografia nos dados transportados em uma comunicação cliente-servidor. Esse protocolo geralmente é usado nas aplicações de e-mail, navegação web e transferência segura de arquivos.

Segundo o RFC 4347 (Datagram Transport Layer Security, 2006) o protocolo DTLS é baseado no protocolo TLS e fornece comunicação segura para protocolos de datagramas (em contrapartida ao TLS que utiliza segmentos TCP confiáveis), permitindo que aplicações cliente-servidor se comuniquem tendo proteção contra espionagem e alteração de informações.

- EAP (*Extensible Authentication Protocol* – Protocolo de autenticação extensível):

O protocolo EAP baseou-se no protocolo PPP (ponto a ponto) e fornece autenticação de usuários através de utilização de métodos arbitrários que carregam credenciais e trocas de mensagens também aleatórias, em redes sem fio e conexões ponto a ponto. O protocolo que usa o EAP é responsável por encapsular os pacotes de autenticação.

- EAPOL (*Extensible Authentication Protocol over Lan* – Protocolo de autenticação extensível sobre *Lan*):

O protocolo EAPOL é responsável por fornecer autenticação ou até mesmo controle de acesso à porta *Lan* de uma rede. Enquanto a autenticação não ocorre (aguardando confirmação de credenciais), o único tráfego que passa pela porta é requisições EAPOL para autenticação.

2.4 Tipos de Ataques:

Nesta subseção, serão apresentados os principais ataques que os mecanismos são mais sensíveis;

- Ataques de Repetição:

É um ataque que se caracteriza pela captura de pacotes, e seu posterior reenvio, com o objetivo de causar algum mal à aplicação.

- Negação de Serviço (*Denial of Service* - DoS):

É um ataque que tem como característica realizar várias requisições (alguns milhares ou centenas de milhares, dependendo da infraestrutura) a um serviço, com o intuito de retirá-lo de funcionamento ou impedir a comunicação entre o consumidor e o serviço, devido à infraestrutura não suportar essa demanda. Com o serviço “fora do ar”, o atacante pode tirar algum benefício desse fato.

Além disso, no cenário da IoT, por causa das configurações limitadas, esse é um ataque bem propício a ocorrer.

- Homem no Meio (*Man in the Middle*):

É um ataque em que uma pessoa/objeto passa-se por outra pessoa, solicita e obtém chaves de criptografias. Na verdade, existe a comunicação entre a dupla verdadeira, porém o invasor literalmente fica

no “meio da conversa” e captura os pacotes que eram destinados a um lado, retira a informação desejada e depois repassa a informação. O atacante faz o mesmo no sentido inverso, e no final tem o par de chaves necessário para realizar a decodificação. Feito isso, ele fica capturando os pacotes e sem esforço, os decodifica.

- Ataque físico

Esse ataque ocorre principalmente em cenários da IoT, pois como alguns dos objetos inteligentes têm que ficar em ambientes expostos e sem segurança, invasores possuem uma maior chance de conseguir obter o nó fisicamente e retirar as informações desejadas.

2.5 *Frameworks:*

Nesta subseção aborda-se alguns frameworks utilizados ou que serviram como base para cada proposta apresentada.

- DCapBAC:

Segundo (HERNANDEZ-RAMOS et al., 2014) o DCapBac é um mecanismo de controle de acesso baseado em capacidades e segurança que utiliza um conjunto de otimizações criptográficas de curvas elípticas. Ele tem como fatores positivos as vantagens de uma abordagem de segurança distribuída, que fornece escalabilidade, interoperabilidade e segurança fim a fim.

- OAuth:

O OAuth (The OAuth 2.0 Authorization Framework, 2012) um protocolo livre que permite que aplicações de terceiros obtenham autorização segura, em um método padrão e simples para aplicações web, móvel e desktops.

3 ANÁLISE DE TRABALHOS CORRELATOS

O artigo (POHLS et al., 2014) intitulado: "*RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects*," apresenta os objetivos e as contribuições pretendidas pelo RERUM. O qual pretende aumentar a confiança das tecnologias de IoT, preservando a privacidade dos cidadãos e dos usuários finais, objetivando o sensoriamento do meio ambiente de forma eficaz, eficiente, em tempo real e mais confiável. Ao mesmo tempo, em que protege a privacidade de informações inseridas por humanos ou por objetos, incluindo segurança durante a troca de dados. Esse feito é alcançado pelo framework de acompanhamento de protótipos de hardware de objetos inteligentes, o qual foi desenvolvido pelo RERUM.

O autor se baseou nos trabalhos de (TRAGOS et al., 2013), (ARAUJO et al., 2013) e (FRAGKIADAKIS et al., 2013) para superar as questões de interferência de radio e congestionamento de redes, utilizando as vantagens da tecnologia de rádio cognitivo e acesso ao espectro dinâmico em cooperação com sensoriamento de espectro e mecanismos de atribuição de espectro. Além de criptografia na camada de acesso ao meio (MAC) que foram observadas nos trabalhos de (BECHKIT et al., 2013), (ROMAN et al., 2011) e (ILIA et al., 2013), o padrão 802.15.4 (802.15.4-2006 , 2011) especifica um *framework* para trocas criptografadas de frames da camada 2. E métodos para a troca segura de pacotes para as camadas de rede e de transporte como o trabalho de (RAZA et al., 2011) que tenta implementar o IPv6 IPsec para dispositivos embutidos, o de (WANG et al., 2011) para estabelecer sistemas criptográficos baseados em chave pública e o (MZID et al., 2010) para implementar segurança na camada de transporte em sensores sem fio.

Já em relação à reputação e confiança (exceto em IoT), o trabalho de (JØSANGet al., 2007) apresentou métodos propostos de pesquisas e algoritmos baseados em avaliação de usuários, enquanto (GLIGOR et al., 2011) mostrou um estudo e a teoria sobre elementos de confiança comportamental e computacional que serve como modelo de comunicação entre entidades como humanos, *hosts* e aplicações. Em (PERRIG et al., 2002), o autor percebeu a importância de códigos de autenticação de mensagens para proteção de integridade e autenticação de origem, para assim poder aplicar e ampliar a técnica criptográfica chamada assinaturas maleáveis. Percebe-se que os trabalhos relacionados trouxeram um embasamento teórico necessário para o RERUM manter um nível de integridade e privacidade em IoT.

Como o artigo apresenta os problemas de segurança e confiança presentes nos dispositivos inteligentes atualmente, a metodologia apresentada pelo autor foi somente mostrar que o RERUM desenvolveria novos protocolos e algoritmos para melhorar a segurança, privacidade e confiança. O autor mencionou que num primeiro momento, utilizariam simulação através do simulador Cooja presente no

Contiki (OSTERLIND, 2006) para realizar uma avaliação entre compensação e a segurança obtida. Depois de realizados os testes, foram construídos protótipos utilizando a plataforma zolertia Z1 (Starter Platform, ___) para realizar testes em ambientes caracterizados como "cidades inteligentes".

O ponto forte deste artigo foi apresentar um novo *framework* focado na segurança e privacidade, que pode aumentar a confiança nos dispositivos inteligentes tendo como consequência uma popularização no uso do mesmo. Porém, o que faltou no mesmo foi o resultado dos testes, pois mesmo cumprindo com a ideia do artigo, cujo objetivo foi apresentar e fundamentar a ideia do que ia ser feito, a confiança seria maior se já fosse apresentado os resultados.

Segundo o trabalho de (RIAHI *et al*., 2014), intitulado "*A systemic and cognitive approach for IoT security*", a inserção dos objetos inteligentes no dia a dia, irá trazer muitos benefícios para os usuários, pois através da informação e da inteligência fornecida aos mesmos, tais objetos irão tomar decisões e reagir a situações do ambiente. Porém, esses objetos precisam se relacionar com outros objetos e com humanos para tomar decisões, e consequentemente é necessário resolver problemas de segurança envolvendo essa relação.

Esse trabalho buscou resolver os problemas de ameaças e de acesso não autorizado, além de aumentar os esforços em relação à segurança de redes e protocolos, dados e privacidade, gerenciamento de identidade, confiança e governança, tolerância a falhas, confiança dinâmica, segurança e gerenciamento de privacidade. Os autores usaram uma abordagem sistêmica e cognitiva para a segurança da Internet das coisas, incluindo o que foi citado anteriormente, em uma metodologia holística que pode ser transformada em um *framework.*

Este é um trabalho que apresentou uma boa ideia, pois ele muda o foco da segurança em IoT, pois ele concentrou a pesquisa nas interações entre os diferentes elementos do sistema, abordando uma área pouco estudada. Porém, por se tratar de uma área pouca abordada, o autor se baseou em trabalhos de (KIELY et al., 2008) e em um próprio trabalho como trabalhos relacionados. E somente para definir e discutir os problemas das relações entre os personagens deste modelo, é que o mesmo utilizou de trabalhos específicos como base.

O trabalho não apresenta um resultado prático deste framework, nem apresenta a ideia de realizar testes do mesmo no futuro, somente explicitou que a abordagem permanece aplicável mesmo na presença das limitações do paradigma IoT, e os desafios futuros da pesquisa.

Com o aumento na utilização do paradigma de IoT, as instituições regulamentadoras viram a necessidade de adaptar a pilha de protocolos IP para o uso em dispositivos inteligentes. Porém, em relação à

segurança, o núcleo desse protocolo foi projetado para modelos de confiança orientados a conexão, o qual não se encaixa com as restrições do IoT. Pensou-se então, em utilizar o protocolo DTLS, mas ele não foi utilizado, pois não suporta *multicast*, *cache* e por causa de problemas de escalabilidade devido às restrições dos dispositivos.

Para resolver esse impasse, o trabalho de (VUCINIC *et al*., 2014), intitulado "*OSCAR: Object Security Architecture for the Internet of Things*", apresentou uma nova arquitetura de segurança para IoT, que fornece segurança fim a fim e controle de acesso, separando os domínios de confidencialidade e autenticidade, além de suportar *multicast*, *cache* e tráfego assíncrono. Isso se deu, utilizando os princípios de segurança de objeto, onde o objeto protege a informação contida nele mesmo, e o controle de acesso baseado em capacidade para fornecer confidencialidade na comunicação e evitar ataques de repetição respectivamente. Além de resolver o problema de escalabilidade, baseando-se em uma arquitetura REST, que não guarda estado em uma relação servidor e cliente, e nos princípios do protocolo DTLS para realizar uma distribuição de chaves autenticadas em canais seguros.

A arquitetura do OSCAR (como é chamado, a arquitetura) é apresentada durante o trabalho, e é avaliada utilizando duas plataformas de hardware (WiSMote baseado em 16-bit MSP430 e o ST GreenNet baseado em um ARM de 32-bit) e camadas MAC, em uma plataforma de teste real e em um simulador de nível de instrução, o Cooja, em um cenário máquina para máquina (M2M) com limitações. Nesse trabalho, os principais pontos observados foram o cálculo da sobrecarga em dispositivos limitados utilizando o algoritmo de assinatura digital de curva elíptica (ECDSA) e a escalabilidade em cenários de comunicação M2M. Além do consumo estimado de cada componente utilizando a ferramenta Energest do Cooja.

Em relação ao tempo de computação, os testes na plataforma de 32 bits foi 4 vezes mais rápido do que a plataforma de 16 bits, o que teve como consequência uma redução de 3.084 vezes no consumo de energia. Esses dados reforçaram a ideia de controle de acesso baseado em capacidade (nesse caso de processamento), porém em relação a sobrecarga nos dispositivos devido ao uso da criptografia, teve um aumento de 0.3 para 0.9 segundos para a plataforma de 32 bits e 1.18 para 3.63 segundos para a plataforma de 16 bits. Mesmo assim, para os autores esse aumento é aceitável, pois o OSCAR compensa esse aumento com a redução no uso de energia pelo transmissor durante a fase de *handshake*.

Já em termos de escalabilidade relacionada com o consumo de energia total do servidor e em relação à energia consumida por requisição e resposta, o OSCAR superou rápido o protocolo DTLS LITE (adaptação do DTLS para IoT) na primeira relação enquanto que na segunda, somente a partir de uma determinada quantidade de requisições e respostas. Em termos de latência, a curva que representa o DTLS aumenta exponencialmente com o número de clientes, e espera-se uma saturação em redes densas.

O autor observou o modelo de consumidor e produtor para o controle de acesso em computação de nuvem no trabalho de (JUNG *et al*., 2013) e percebeu que ele podia ser mapeado para o problema de segurança em IoT; E utilizou-se do trabalho de (KEOH *et al*., 2014) para resolver o problema de ataques de repetição. Em partes mais específicas, porém relacionadas, o trabalho de (LUK *et al*., 2007) buscou apresentar uma solução para segurança fim a fim (*end-2-end*), (KOTHMAYR *et al*., 2012) discutiu a necessidade de autenticação entre clientes e servidor durante uma ação de *handshake* do DTLS. (SEITZ *et al*., 2013) utilizou dos benefícios do conceito de segurança de objetos para fornecer controle de acesso para um framework de autorização baseado em afirmação, o qual segundo o autor, é um trabalho complementar ao abordado e como sugestão do mesmo, pode ser utilizado junto ao do autor para cobrir uma maior quantidade de casos de usos.

O autor conseguiu provar que o artigo em questão fornece uma arquitetura que supera os protocolos/mecanismos comparados. E, além disso, supera o protocolo DTLS LITE, fornece segurança fim a fim, controle de acesso e confidencialidade, respeitando as limitações de IoT. Apesar disso, é escalável e possui consumo reduzido;

O trabalho de (HERNANDEZ-RAMOS *et al*., 2015), intitulado "*Toward a Lightweight Authentication and Authorization Framework for Smart Objects*" apresentou um *framework* de mecanismos de autenticação e de autorização leve, que é estendido para funcionar com outras tecnologias de segurança padrão, funcionando como uma abordagem de segurança holística, a qual objetiva funcionar na fase de inicialização e no nível operacional. Em outras palavras, o *framework* é baseado no modelo ARM (para fornecer interoperabilidade), porém amplia o mesmo, inserindo grupos funcionais com segurança (compartilhamento em grupo) e componentes adicionais que são necessários para o ambiente de IoT atual.

Em relação aos trabalhos relacionados, (PORAMBAGE *et al*., 2014) apresentou um esquema de distribuição de chave e autenticação para rede de sensores sem fio no estágio de inicialização dos dispositivos, enquanto que o trabalho de (SARIKAYA *et al*., 2012) fornece as principais abordagens e protocolos para serem considerados no âmbito de IoT. Além deles, (HUMMEN *et al*., 2013), (FORSBERG *et al*., 2008) e EEE/ISO/IEC (EEE/ISO/IEC, 2013) apresentam os protocolos HIP-DEX, PANA e 802.1X respectivamente, que foram analisados como alternativas no trabalho.

Para o estabelecimento de chaves, o autor analisou o trabalho de (LIU *et al*., 2012) que apresentou uma abordagem em criptografia de curva elíptica e o de (FERRAIOLO *et al*., 1995) que mostrou um modelo de controle de acesso baseado em regras para a definição de políticas de controle de acesso. Em contrapartida, (HUMMEN *et al*., 2013) apresentou um esquema de controle de acesso e autenticação que é baseado no estabelecimento de chaves eficientes utilizando criptografia de curvas elípticas. Contudo,

(HERNANDEZ-RAMOS *et al*., 2014) introduziu o DCapBAC como uma abordagem distribuída de controle de acesso viável a ser implantado em ambientes com restrições, utilizando lógica de autorização, além de adaptar as tecnologias de comunicação e o formato de intercâmbio de dados.

Em relação à metodologia utilizada, o autor explica a necessidade de utilizar a arquitetura baseada em ARM e a inclusão de mecanismos de segurança leves. Logo após ele apresenta esses mecanismos dividindo-os em nível de inicialização e em nível operacional, fundamenta a necessidade dos mesmos, e depois explicita o cenário proposto pelo trabalho. No nível de inicialização, o autor utilizou o protocolo EAP (ABOBA *et al*., 2004) para fornecer autenticação flexível juntamente com o protocolo SEAPOL (uma alteração do próprio autor do EAPOL) para transportar as mensagens EAP. E no nível operacional, baseia-se no DCapBAC [9] focando na comunicação objeto com objeto, além de proporcionar uma abordagem descentralizada, com segurança fim a fim, escalável, flexível e com interoperabilidade.

Para realizar os testes na fase de inicialização com o EAPOL e o SEAPOL, utilizaram-se nós Tmote Sky (um funcionando como ponto de acesso e os outros como clientes na rede) e alteraram três aplicações no Contiki OS (*native boarder router*, *slip-radio* e *sky-websense*) para avaliar o consumo de memória. Os resultados mostraram uma diminuição no consumo de memória flash de 270 bytes para o protocolo SEAPOL (aplicação *slip-radio*), como também 336 bytes no aplicativo *sky-websense*. Além disso, também foi analisado o impacto do uso de diferentes métodos EAP com o SEAPOL e com o EAPOL. No consumo de memória, EAP-MD5 é o método EAP mais leve comparando com o EAP-PSK. Nos métodos que utilizam o ECDSA (os quais utilizam mais memória), como por exemplo, o EAP-TLS, o SEAPOL também consumiu menos memória do que o seu concorrente, destacando-se o TLS-1.0. Já nos EAP-TLS com RSA, percebeu-se que utilizam menos memória ROM do que os com ECDSA, porém consomem muito mais memória RAM, inviabilizando o seu uso em IoT.

Outra métrica abordada foi o consumo de rede nas variações de métodos EAP comparando o SEAPOL com o EAPOL. Os resultaram mostraram que o EAP-MD5 com o SEAPOL é o que consome menos, porém mostrou um dilema. Os métodos EAP-TLS baseados em ECDSA são os que mais compensam a questão da segurança com as restrições de IoT.

Na fase operacional, avaliou-se o tempo para trocas de mensagens e para produção dos *token* em nós JN5148 com Contiki OS. Foram realizados 100 testes e percebeu-se que o atraso necessário para o funcionamento seguro de todo processo é 2168,16 ms, o que segundo o autor, é um tempo razoável e permite incorporar esses mecanismos de segurança em dispositivos inteligentes que fazem parte da IoT.

Em resumo, todos os mecanismos apresentados, assim como o *framework* com esses inclusos, produz uma melhoria significativa para a segurança, mais especificamente autenticação e autorização, para dispositivos inteligentes. O autor realizou avaliações para comprovar que o seu *framework* era melhor do que outros atuais, porém ele executou comparações com mecanismos e não com uma solução completa.

Atualmente houve um aumento na disseminação de dados e informações pessoais que é divulgada a terceiros através de aplicativos utilizados. Com o advento da IoT, isso irá aumentar mais ainda, o que trouxe à discussão a segurança/privacidade dos dados pessoais. O trabalho de (CIRANI *et al*., 2015), denominado "*IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios*", oferece uma nova arquitetura que disponibiliza um serviço de autorização externa baseada no protocolo OAuth, indicado como IOT-OAS, que trás como benefícios: Facilidade de implementação para desenvolvedores, pois não há a necessidade de se preocupar com segurança e autorização; Simplicidade no objeto inteligente, pois o mesmo só necessita invocar o serviço de autorização externo de forma segura; E a facilidade em configurar as políticas de acesso, sem a necessidade de ir até o objeto.

No início da pesquisa, o autor de IoT-OAS (CIRANI *et al*., 2015) buscou artigos correlatos para fundamentar o seu trabalho. Ele utilizou artigos no estado da arte como o de (CIRANI *et al*., 2013) que apresenta uma revisão dos mecanismos de segurança de IoT que fornecem confidencialidade, integridade e autenticação. Já o de (NING *et al*., 2013) apresentou a arquitetura "U2IoT" que fornece segurança para interações heterogêneas e domínios em expansão como, por exemplo, a internet com a IoT. Mas o autor também pesquisou trabalhos mais específicos, (YAO *et al*., 2013) mostrou um esquema de autenticação *multicast* leve para aplicações IoT em pequena escala, (LAI *et al*., 2014) definiu o CPAL como um mecanismo de autenticação que permite as partes autorizadas a vincular as informações de acesso do usuário, preservando o anonimato do mesmo e a privacidade. (SCHIFFMAN *et al*., 2010) apresentou um mecanismo de sub-delegação refinado que é responsável pelas permissões de acesso para os consumidores de aplicações web, denotado como "Dauth." O IETF WG ACE propôs o DCAF (GERDES *et al*, 2014), uma arquitetura de servidores para autenticação e autorização, a qual objetiva aliviar o armazenamento de informações em objetos inteligentes, delegando essa tarefa para uma entidade externa. Dessa maneira, este é o trabalho mais relacionado com IOT-OAS, porém o DCAF focou em ambientes com restrições (IoT), enquanto o IOT-OAS foca em ser genérico e integrado de forma transparente com os cenários da IoT e da Internet.

Em relação à metodologia, o autor modelou a arquitetura do IOT-OAS, definindo e apresentando os personagens e o fluxo de operação e regras da arquitetura. Após descrever detalhadamente os fluxos, o mesmo apresentou e descreveu os detalhes da comunicação entre as partes, e por fim destacou a

facilidade na criação, atualização e exclusão de políticas de acesso através da estrutura chamada loja/armazém de permissões.

Logo em seguida, o autor apresentou a arquitetura aplicada em cenários com quatro tipos diferentes de comunicação: comunicação com agente de rede, comunicação baseada em gateway, comunicação CoAP fim a fim e comunicação baseada em gateway híbrido. Na primeira, a comunicação acontece com o agente da rede com o papel de fornecedor de serviços e é ele o responsável por interagir com o serviço OAuth; Já na segunda comunicação, o gateway é responsável por traduzir as requisições do cliente para o objeto inteligente presente na sua rede e para o serviço OAuth, pois nesse caso, o objeto não suporta o protocolo de comunicação (por exemplo http); No terceiro caso, a comunicação ocorre diretamente com o objeto, e é ele o responsável em encaminhar a requisição em CoAP para o serviço OAuth; Por fim, no gateway híbrido, a comunicação é semelhante, porém o gateway só faz a "tradução" e a responsabilidade para encaminhar a requisição para o serviço OAuth permanece com o objeto.

Para demonstrar o desempenho da arquitetura proposta, o autor fez testes para avaliar o consumo de energia das interfaces da CPU e de radio nos objetos inteligentes, comparando a arquitetura proposta com o OAuth da academia. Como a comunicação CoAP fim a fim e a comunicação baseada em gateway híbrido exigem que o nó interaja com o serviço de autorização, só são esses casos que necessitam de atenção e foram os abordados. Os testes foram implementados em casos de testes reais e em cenários simulados utilizando o simulador Cooja presente no Contiki, utilizando a plataforma experimental Zolertia Z1 de 16 bits. E o ambiente experimental foi constituído por um nó cliente Coap que envia uma requisição a um servidor Coap, o qual deve autorizar o pedido e decidir se irá ou não fornecer o serviço.

Os resultados mostraram que o consumo de energia no processamento do IOT-OAS foi menor do que a energia gasta no processamento dos objetos que implementavam OAuth, porém no consumo total o IOT-OAS acabou consumindo um pouco mais que o dobro do seu concorrente, devido ao maior uso do rádio. Porém, segundo o autor, mesmo com essas restrições de energia deve-se considerar esse método, pois: i) para inserir o OAuth na ROM do objeto inteligente foi necessário retirar vários módulos do dispositivo; ii) pouco espaço para o banco de dados com os usuários autorizados e seus *tokens* de acesso no objeto (inviável por causa da memória); iii) facilidade na atualização das políticas de acesso em um serviço de autenticação externo. Ele ainda afirma que o IOT-OAS é uma ótima opção em dispositivos com capacidades de recursos maiores ou objetos que executem comunicação com agente de rede ou comunicação baseada em gateway.

Assim, o trabalho apresentou uma ideia boa, leve e relativamente simples para a autorização e controle de acesso, porém o alto consumo dessa arquitetura repele o seu uso. Além do que, existem

frameworks (como os citados analisados anteriormente) na academia que implementam não só autorização mas também autenticação e confiança para objetos inteligentes sem um custo energético desse nível.

A tabela 7.1 realiza uma comparação dos principais pontos dos trabalhos analisados neste estudo.

Tabela 7.1. Comparação dos principais pontos dos trabalhos analisados neste estudo.

TEMA	MECANISMO	FOCO	MÉTRICAS	RESULTADOS	PONTOS POSITIVOS	PONTOS NEGATIVOS
RERUM: Building a reliable IoT upon privacy- and security-enabled smart objects (POHLS et al., 2014)	*Framework*	-Confiança; -Privacidade de informações; -Segurança entre troca de dados;	Nenhuma	Nenhum	-Um novo *framework* focado na segurança e privacidade; -Popularização do IoT;	-Não apresentou avaliação do *framework* proposto.
A systemic and cognitive approach for IoT security (RIAHI et al., 2014)	*Framework*	- Interações entre os elementos do sistema; -Confiança; -Privacidade de informações; -Segurança entre troca de dados;	Nenhuma	Nenhum	-Muda o foco da segurança em IoT; -Analisa as interações entre os elementos.	-Não apresentou avaliação do *framework* proposto.
OSCAR: Object Security Architecture for the Internet of Things (VUCINIC et al., 2014)	Arquitetura	- Segurança fim a fim; -Controle de acesso; -Confidencialidade na comunicação;	- Sobrecarga de tempo; - Escalabilidade em cenários M2M; -Consumo energético;	-Aumento de 0.3 para 0.9 s (32 bits); - Aumento 1.18 para 3.63 s (16 bits); -É mais escalável do que o DTLS LITE (servidor, e requisição e resposta); - Redução de 3.084 vezes no consumo de energia;	-Supera o protocolo DTLS LITE; -Fornece segurança fim a fim, controle de acesso e confidencialidade e respeitando as limitações de IoT. -É escalável; -Possui consumo reduzido;	-Não deixou ideias para o futuro do trabalho;

Toward a Lightweight Authentication and Authorization Framework for Smart Objects (HERNANDEZ-RAMOS et al., 2015)	*Framework*	-Autenticação; -Autorização leve; -Segurança em compartilhamento em grupo; -Controle de acesso;	- Consumo de memória; -Atraso para funcionamento seguro;	-Redução de 270 bytes; -2168,16 ms;	-Mecanismo de autenticação e autorização leve; -Redução no consumo de memória exigido;	-Comparações com mecanismos e não com *frameworks* ou arquiteturas; -Não deixou ideias para o futuro do trabalho;
IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios (CIRANI et al., 2015)	Arquitetura	-Autorização externa;	-Consumo de energia	-Consumo de energia no processamento foi menor, mas no total foi maior devido ao maior uso do rádio (comunicação); -	-Facilidade de implementação para desenvolvedores; -Simplicidade no objeto inteligente; -Facilidade na configuração das políticas de acesso; -Apresenta uma ideia boa, leve e relativamente simples para a autorização e controle de acesso;	-É uma ótima opção em dispositivos com capacidades de recursos maiores; -Alto consumo de energia repele o seu uso;

4 DESAFIOS E TENDÊNCIAS

É muito importante que um trabalho esteja sempre em evolução, por isso, esse capítulo apresenta as ideias para trabalhos futuros deixados por cada autor dos trabalhos analisados, seguido de sugestões dos autores desse estudo.

a) *RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects* (POHLS et al., 2014):

O autor disse que iria construir protótipos utilizando a plataforma zolertia Z1 (Starter Platform, ___) para realizar testes em "cidades inteligentes" para observar o comportamento do *framework* em ambiente real. Porém, seria interessante, antes disso, realizar a avaliação de métricas como consumo de memória, energia e processamento. Além de realizar testes de segurança, simulando ataques aos nós para avaliar se o *framework* realmente fornece privacidade de informações e segurança entre troca de dados;

b) *A systemic and cognitive approach for IoT security* (RIAHI *et al*., 2014):

O autor não deixou ideias para o futuro do trabalho, somente explicitou desafios para a pesquisa em IoT: Resolver a falta de padronização, desenvolver mecanismos leves e robustos de autenticação de objetos e pessoas que se encaixe no paradigma de IoT, gerenciamento de políticas de segurança, armazenamento seguro e proteção de privacidade de dados em massa e distribuídos.

Porém, em relação ao trabalho, seria interessante realizar a avaliação do modelo através de testes em dispositivos reais e observar o seu comportamento, tanto em relação a segurança quanto em relação à concordância com o paradigma de IoT.

c) *OSCAR: Object Security Architecture for the Internet of Things* (VUCINIC *et al*., 2014):

O autor não deixou ideias para o futuro do trabalho. Porém, uma ideia interessante seria ampliar a arquitetura do OSCAR para uma quantidade maior de casos de usos, além de realizar testes em um ambiente com muitos nós e com diferentes níveis de processamento, para avaliar o comportamento da arquitetura em relação à escalabilidade, tempo de processamento (devido à sobrecarga) e comunicação, em nível de uma "cidade inteligente".

d) *Toward a Lightweight Authentication and Authorization Framework for Smart Objects* (HERNANDEZ-RAMOS *et al*., 2015):

Novamente, o autor não deixou ideias para o futuro do trabalho e executou comparações com protocolos e não com soluções como abordagens, *frameworks* ou arquiteturas. Por isso, seria interessante

em trabalhos futuros, a comparação com *frameworks* existentes para mostrar se o trabalho em questão, realmente é superior em relação a consumo de memória e a tempo de execução.

e) *IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios* (CIRANI *et al*., 2015):

O autor não deixou ideias para o futuro do trabalho. Então, pelo que foi analisado, seria interessante melhorar o consumo energético desse mecanismo, pois o alto consumo repele o seu uso. Além de avaliar a inclusão dessa arquitetura (ou da ideia de realizar autenticação através de uma entidade externa) em frameworks existentes para quem sabe, produzir um produto mais viável e menos oneroso.

5 CONCLUSÕES

O novo paradigma da Internet das Coisas insere a necessidade de um nível de segurança mais forte, pois em uma era em que um dos bens mais valiosos é a informação, essa abordagem que preza a absorção ubíqua de informações, destaca-se como um possível distribuidor de riscos para a segurança da informação. A academia busca resolver esse problema investindo esforços para adaptar os mecanismos de segurança atuais para resolver esse dilema.

Como a segurança é o principal empecilho para o uso de cenários de IoT, este trabalho apresentou um estudo crítico de alguns *frameworks* de segurança atuais, mostrando como cada arquitetura trabalha e seus pontos positivos e negativos. A partir desse estudo, percebe-se que os mecanismos de seguranças existentes avançaram, porém ainda possuem limitações com objetos inteligentes.

Dos trabalhos analisados os que tiveram melhor comportamento foram o OSCAR (VUCINIC *et al.*, 2014) e o SEAPOL (HERNANDEZ-RAMOS *et al.*, 2015), pois ambos apresentaram uma arquitetura coesa que mesmo com limitações, fornecem alto nível de segurança com pouco ônus. E como trabalho futuro, seria interessante a ampliação deste trabalho com a análise de outros artigos, para realizar a comparação com outros mecanismos de segurança.

REFERÊNCIAS

"***Constrained application protocol***", Request for comments, 7252. Jun. 2014.

"***Datagram Transport Layer Security***", Request for comments, 4347. April. 2006.

"**The OAuth 2.0 Authorization Framework**", Request for comments, 6749. Oct. 2012.

"***802.15.4-2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)***, " IEEE Standard, 2011.

ABOBA, B.; et al., "***Extensible Authentication Protocol (EAP)***," IETF, Fremont, CA, USA, RFC 3748, Jun. 2004.

ARAUJO, A.; et al., "***Security in cognitive wireless sensor networks. Challenges and open problems***," Journal on Wireless Communications and Networking, vol. 48, 2012.

ATZORI, L.; IERA, A.; MORABITO, G. "***The Internet of Things: A survey***," Comput. Netw., vol 54, no. 15, pp. 2787-2805, Oct. 2010.

BASSI, A. *et al.*, "***Enabling Things to Talk***," 2013.

BECHKIT, W.; et al, "***A highly scalable key pre-distribution scheme for wireless sensor networks***," Wireless Communications, IEEE Transactions on, vol. 12, no. 2, pp. 948–959, 2013.

CIRANI, S.; FERRARI, G.; VELTRI, L. "***Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview***," Algorithms, vol. 6, no. 2, pp. 197–226, 2013. [Online]. Available: http://www.mdpi.com/1999-4893/6/2/197.

CIRANI, S.; PICONE, M.; GONIZZI, P.; VELTRI, L.; FERRARI, G."***IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios***," *Sensors Journal, IEEE* ,

vol.15, no.2, pp.1224,1234, Feb. 2015
doi: 10.1109/JSEN.2014.2361406.

EEE/ISO/IEC, "***Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks***"—Part 1X: Port-Based Network Access Control, IEEE Std. 8802- 1x-2013, Dec. 6, 2013. [Online]. Available: http://dx.doi.org/10.1109/ ieeestd.2013.6679204.

FERRAIOLO, D.; CUGINI, J.; KUHN, R. "***Role-Based Access Control (RBAC): Features and motivations***," in Proc. 11th Annu. Comput. Security Appl. Conf., 1995, pp. 241–248.

FORSBERG, D.; OHBA, Y.; PATIL, B.; TSCHOFENIG, H.; YEGIN, A. "***Protocol for carrying authentication for network access (PANA)***," IETF, Fremont, CA, USA, RFC 5191, 2008.

FRAGKIADAKIS, A.; TRAGOS, E.; ASKOXYLAKIS, I. "***A survey on security threats and detection techniques in cognitive radio networks***," IEEE Commun. Surveys Tuts., vol. 15, no. 3, pp. 428–445, 2013.

GERDES, S.; BERGMANN, O.; BORMANN, C. "***Delegated CoAP authentication and authorization framework (DCAF)***," IETF Internet Draft, Tech. Rep. draft-gerdes-ace-dcaf-authorize-00, Jul. 2014. [Online]. Available: http://tools.ietf.org/html/draft-gerdes-ace-dcaf-authorize-00.

GLIGOR, V.; WING, J.M. "***Towards a theory of trust in networks of humans and computers***," in 19th Int. Workshop on Security Protocols, ser. LNCS. Springer Verlag, 2011.

HERNANDEZ-RAMOS, J.L.; JARA, A.J.; MARÍN, L.; GÓMEZ, A.F.S. "***DCapBAC:embedding authorization logic into smart things through ECC optimizations***," Int. J Comput. Math, pp. 1-22,May 2014.

HERNANDEZ-RAMOS, J.L.; PAWLOWSKI, M.P.; JARA, A.J.; SKARMETA, A.F.; LADID, L. "***Toward a Lightweight Authentication and Authorization Framework for Smart Objects***," Selected Areas in Communications, IEEE Journal on , vol.33, no.4, pp.690,702, April 2015 doi: 10.1109/JSAC.2015.2393436.

HERNANDEZ-RAMOS, J.L.; PAWLOWSKI, M.P.; JARA, A.J.; SKARMETA, A.F.; LADID, L. "***Toward a Lightweight Authentication and Authorization Framework for Smart Objects***," *Selected Areas in Communications, IEEE Journal on* , vol.33, no.4, pp.690,702, April 2015 doi: 10.1109/JSAC.2015.2393436.

HUMMEN, R.; HILLER, J.; HENZE, M.; WEHRLE, K. "***Slimfit—A HIP DEX compression layer for the IP-based Internet of things***," in Proc. IEEE 9th Int. Conf. WiMob, 2013, pp. 259–266.

ILIA, P.; OIKONOMOU, G.; TRYFONAS, T. "***Cryptographic key exchange in ipv6-based low power, lossy networks***" in Proc. of WISTP '13 ser. Lecture Notes in Computer Science. Springer, May 2013, pp. 34–49.

JØSANG, A.; ISMAIL, R.; BOYD, C. "***A survey of trust and reputation systems for online service provision***," Decis. Support Syst., vol. 43, no. 2, pp. 618–644, 2007.

JUNG, T.; LI, X.Y.; WAN, Z. "***Privacy Preserving Cloud Data Access With Multi-Authorities***," in Infocom. IEEE, 2013.

KEOH, S.; KUMAR, S.; GARCIA-MORCHON, O.; DIJK, E.; RAHMAN, A. "***DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs) draft-keoh-dice-multicast-security-05***," IETF work in progress, 2014.

KIELY, L.; BENZEL, T. "***Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs***," Institute for Critical Information Infrastructure Protection (ICIIP), 2008.

KOBLITZ, M. "***Elliptic Curve Cryptosystems***," Math Comp., 48, 203-209, 1987.

KOTHMAYR, T.; SCHMITT, C.; HU, W.; BRUNIG, M.; CARLE, G. "***A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication***," in LCN. IEEE, 2012, pp. 956–963.

LAI, C.; LI, H.; LIANG, X.; LU, R.; ZHANG, K.; SHEN, X. "***CPAL: A conditional privacy-preserving authentication with access linkability for roaming service***," IEEE Internet Things J., vol. 1, no. 1, pp. 46–57, Feb. 2014.

LIU, J.; XIAO, Y.; CHEN, C.L.P. "***Authentication and access control in the internet of things***," in Proc. 32nd ICDCSW, Macau, China, Jun. 2012, pp. 588–592.

LUK, M.; MEZZOUR, G.; PERRIG, A.; GLIGOR, V. "***MiniSec: a secure sensor network communication architecture***," in IPSN. IEEE, 2007, p. 479.

MORENO, E.D. "**Segurança em sistemas embarcados modernos: desafios e tendências."** Aracaju. ArtNer Comunicação, 2015.

MILLER, V. "***Uses of Elliptic Curves in Cryptography***," Advances in Cryptography, Crypto 85, Springs Verlag LNCS 218, 417-426, 1986.

MZID, R.; et al, "***Adapting TLS handshake protocol for heterogenous IP-based WSN using identity based cryptography***," in Int. Conf. on ICWUS '10), 2010, pp. 1–8.

NING, H.; LIU, H.; YANG, L.T. "***Cyberentity security in the internet of things***," Computer, vol. 46, no. 4, pp. 46–53, Apr. 2013.

OSTERLIND, F. "***A Sensor Network Simulator for the Contiki OS***", Swedish Institute of Computer Science technical report, 2006.

PERRIG, A.; et al., "***SPINS: Security protocols for sensor networks***," Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

POHLS, H.C.; ANGELAKIS, V.; SUPPAN, S.; FISCHER, K.; OIKONOMOU, G.; TRAGOS, E.Z.; RODRIGUEZ, R.D.; MOUROUTIS, T. "***RERUM: Building a reliable IoT upon privacy- and security-enabled smart objects***,"*Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE* , vol., no., pp.122,127, 6-9 April 2014. doi: 10.1109/WCNCW.2014.6934872.

PORAMBAGE, P.; SCHMITT, C.; KUMAR, P.; GURTOV, A.; YLIANTTILA, M. "***PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications***," Int. J. Distrib. Sensor Netw., vol. 14, 2014, Art. ID. 357430.

RAZA, S.; et al., "***Securing Communication in 6LoWPAN with Compressed IPsec***", in Proc. 7th IEEE DCOSS '11), Jun. 2011.

RIAHI, A.; NATALIZIO, E.; CHALLAL, Y.; MITTON, N.; IERA, A."***A systemic and cognitive approach for IoT security***," *Computing, Networking and Communications (ICNC), 2014 International Conference on* , vol., no., pp.183,188, 3-6 Feb. 2014doi: 10.1109/ICCNC.2014.6785328.

ROMAN, R.; et al., "***Key management systems for sensor networks in the context of the Internet of Things***," Computers & Electrical Engineering, vol. 37, no. 2, pp. 147—159, Mar. 2011.

SARIKAYA, B.; OHBA, Y.; MOSKOWITZ, R.; CAO, Z.; CRAGIE, R. "***Security bootstrapping solution for resource-constrained devices***," IETF, Fremont, CA, USA, 2012, Draft-Sarikaya-Core-Sbootstrapping-05.

SCHIFFMAN, J.; ZHANG, X.; GIBBS, S. "***DAuth: Fine-grained authorization delegation for distributed web application consumers,***" in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw. (POLICY), Jul. 2010, pp. 95–102.
SEITZ, L.; SELANDER, G.; GEHRMANN, C. "***Authorization framework for the internet-of-things***," in WoWMoM. IEEE, 2013, pp. 1–6.

STARTER PLATFORM. Disponível em: <http://www.zolertia.com/products/Z1>. Acessado em 28 de janeiro de 2016.

TRAGOS, E.; et al., "***Spectrum assignment in cognitive radio networks: A comprehensive survey***," IEEE Commun. Surveys Tuts., vol. 15, no. 3, pp. 1108–1135, 2013.

VUCINIC, M.; TOURANCHEAU, B.; ROUSSEAU, F.; DUDA, A.; DAMON, L.; GUIZZETTI, R.; "***OSCAR: Object security architecture for the Internet of Things,***" *A World of Wireless, Mobile and*

Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on , vol., no., pp.1,10, 19-19 June 2014doi: 10.1109/WoWMoM.2014.6918975.

WANG, H.; et al., "***Public-key based access control in sensornet***," Wireless Networks, vol. 17, no. 5, pp. 1217–1234, 2011.

YAO, X.; HAN, X.; DU, X.; ZHOU, X. "***A lightweight multicast authentication mechanism for small scale IoT applications***," IEEE Sensors J., vol. 13, no. 10, pp. 3693–3701, Oct. 2013.

YE, N.; ZHU, Y.; WANG, R.C.; MALEKIAN, R.; QIAO-MIN, L. "***An efficient authentication and access control scheme for perception layer of Internet of things,***" Appl. Math. Inf. Sci., vol. 8, no. 4, pp. 1617–1624, Jul. 2014.