Segurança em Internet das Coisas: Um Survey de Soluções *Lightweight*

Securing the Internet of Things: A Survey of Lightweight Solutions

Joelias S. Pinto Junior[1], Clerisson dos Santos e Silva[2], Danilo Domingos Xavier[3]

[1]Campus Canarana, [2]Campus Octayde Jorge
Instituto Federal de Mato Grosso, IFMT
[1]Canarana, Cuiabá - Brasil[2], Campus Alto Araguaia[3]
Universidade do Estado de Mato Grosso, UNEMAT
Alto Araguaia - Brasil

joelias.junior@bag.ifmt.edu.br, clerisson.silva@cba.ifmt.edu.br
daniloxavier@unemat.br

Resumo. *A conexão intermitente de dispositivos, máquinas e sensores em cenários com inteligência computacionais conectados à internet tem se tornado cada vez mais presente. A essa integração, dá-se o nome de Internet das Coisas (Internet of Things – IoT). Esse novo paradigma traz desafios de segurança, principalmente pela heterogeneidade e a quantidade de dispositivos com baixo poder computacional presentes nesse cenário. Propostas de segurança tradicionais não são viáveis nestes cenários e novas soluções são então necessárias. Surgem então as soluções lightweight. Entende-se por lightweight todas as técnicas, arquiteturas e esquemas de segurança consideradas "leves" em termos de consumo de recursos e adaptáveis a diferentes dispositivos. Neste trabalho é analisado o atual cenário de segurança lightweight em redes IoT, por meio de uma revisão e classificação da Literatura. São apresentadas propostas de algoritmos de criptografia baseadas em credenciais, uso da nuvem para autenticação, redução de latência, de consumo de energia e de perda de pacotes, entre outras vantagens. É pretendido assim, contribuir com o avanço das pesquisas em segurança em Internet das Coisas, apresentando as tecnologias de segurança "leves" em IoT, os desafios, os desenvolvimentos recentes, as questões em aberto e também os pontos futuros de pesquisa.*

Abstract. *The intermittent connection of devices, machines and sensor in computational intelligent scenarios connected to the internet have become usual. This integration we call Internet of Things, a new paradigm who brings security challenges, mainly for its heterogeneity and amount of low power devices connected. Traditional security solutions has become obsolete in this scenarios and new solutions are needed. 'Lightweight' solutions came up. As 'lightweight' we can regard every security technique, architecture and scheme who is light in resource consumption and adaptable to different devices. In this paper we analyze the current scenario for IoT lightweight security by literature review. Proposes of cryptography algorithms based on credentials, cloud*

authentication, latency reducing, energy saving and package loss decreasing are discussed. Thus, we seek to contribute with Internet of Things security research, by showing challenges, progress, open issues and future research of 'lightweight' security technology for IoT.

I. INTRODUÇÃO

Nas últimas décadas, os objetos eletrônicos têm cada vez mais se multiplicado e permeado por diversos contextos [15]. Dispositivos que antes se conectavam eventualmente com outros ou com a internet, como computadores, smartphones e *tablets*, agora permanecem comumente conectados intermitentemente, mesmo quando não interagimos com eles. Já outros objetos, como geladeiras, fogões, carros, relógios, etc., que antes pareciam improváveis que fossem se conectar, agora fazem parte de redes conectadas, inclusive pela internet [6]. Sensores com funções de identificação, controle e monitoramento também são agregados a essas redes e, por vezes, disparando gatilhos com ações autônomas ou permitindo comunicação remota [22].

Quando todos esses dispositivos se integram e formam uma rede em comum, com conexão à internet, eles são chamados de "coisas". Assim, temos a Internet das Coisas ou *IoT* (do Inglês, *Internet of Things*). *IoT* é uma rede de objetos fisicamente identificáveis globalmente, que se integram com a Internet e são representáveis no mundo virtual [26]. Essa rede também é, por vezes, caracterizada como *Web of Things* (*WoT*), um novo paradigma que visa a integração entre os objetos do mundo real com o virtual através da Web [9][8]. A quantidade de tecnologias envolvidas nessas redes é extremamente esparsa e envolve de máquinas a humanos, passando por dispositivos e sensores.

A maneira mais comum de se conectar essas redes, é através de redes sem fio. Vários são os problemas pertinentes a segurança nessas redes. Para a maioria deles, já existem algumas soluções satisfatórias, porém, limitadas. Em casos em que se utiliza criptografia assimétrica, por exemplo, a maioria das soluções são limitadas pelo poder computacional. Dispositivos de *IoT* como sensores, cartões inteligentes e outros de baixo poder computacional não conseguiriam processar os algoritmos de criptografia convencionais.

Duarte et al.[10] propõe um *middleware* para se operar a *IoT* em dispositivos com sistema operacional Android. Eles levantam a questão da necessidade de desenvolvimento dinâmico para dispositivos heterogêneos, inclusive com baixo poder de processamento, como *smartwatchs*. Este tipo de preocupação é compartilhado por Andrade et al.[8], um trabalho também aplicado a dispositivos com limitada capacidade de memória e poder de processamento. Li et al. [19] complementam essa discussão, quando pontuam que essas características de restrições, dinamicidade e heterogeneidade dificultam a implementação de segurança eficaz para *IoT*. Eles também classificam a *IoT* como um ecossistema aberto, onde a segurança se torna ortogonal a outras áreas de pesquisa. Eles destacam que a grande diversidade da *IoT* a faz vulnerável a ataques de disponibilidade, integridade de serviço, segurança e privacidade. Ainda, que a dificuldade de se implementar segurança aqui é dada principalmente pela limitada capacidade computacional e energética dos dispositivos sensoriais. Em outro trabalho, também recente, abrangendo a computação quântica, O'Neill [23] fala da dificuldade de se implementar bons algoritmos de segurança em *IoT*. Ele ressalta que essa dificuldade inclui, inclusive, algoritmos de segurança quântica, pois em alguns casos eles não são

práticos e em outros são ainda mais complexos que as técnicas de chave pública atuais. Também, o tamanho de suas chaves tende a ser muito grande, o que os torna impráticos para dispositivos de baixo poder computacional. Assim, o desenvolvimento de soluções de segurança para *IoT* apresenta-se como um problema em aberto, inclusive na computação quântica.

As redes *IoT* têm essa característica heterogênea intrínseca e para tratá-las em relação às questões de segurança, uma proposta que tem se trabalhado, são as soluções de segurança *lightweight*. Soluções *Lightweight*, são técnicas, arquiteturas, esquemas e tecnologias de segurança que, são leves em termos de processamento e consumo de recursos e têm capacidade de funcionamento em dispositivos heterogêneos [34].

É extremamente importante discutir propostas de segurança específicas para as necessidades da *IoT*. Vários trabalhos existentes como [30][10][8][9] e [22], propõem novas tecnologias para *IoT*, mas não trazem junto com suas propostas previsões de como assegurar e confidencializar as informações trafegadas através de suas redes e dispositivos. Assim, esse artigo contribui tanto reforçando a discussão sobre essa problemática, quanto em revisando os vários trabalhos visando discutir aqui os que parecem ser mais relevantes diante dos contextos de heterogeneidade e baixo poder computacional proporcionado pela *IoT* e *WoT* atualmente.

Quando se discute sobre segurança em qualquer âmbito, uma preocupação sempre concernente são os ataques maliciosos. No caso da *IoT*, entre diversos tipos de ataques, os realizados pelo *Mirai* [32] em 2016 traz inquietação e justifica essa necessidade por segurança discutida no presente trabalho. *Mirai* é um malware que se instala em computadores Linux para permitir controle remoto. Cada dispositivo passa a ser enxergado como um *bot* (robô) e pode se integrar, formando uma *botnet* (rede de robôs) [32]. Em setembro de 2016, o *Mirai* se instalou em uma série de dispositivos de *IoT*, como câmeras de vigilância e *DVRs* e controlou esses dispositivos remotamente coordenando um ataque *DDoS* (*Distributed Denial of Service*) de 620 *Gbps,* ao blog do colunista sobre segurança Brian Krebs. Em Outubro desse mesmo ano, esse mesmo malware comandou outro ataque semelhante que tirou do ar a Dyn e por consequência seus clientes –, empresa que provê infraestrutura a sites como *Twitter*, *GitHub*, *Reddit*, *Netflix*, *Airbnb* e muitos outros [18].

A motivação deste trabalho partiu de observar que ataques como esses ocorrem por falhas de segurança, e que as implementações de segurança em *IoT* ainda são poucas, quando não inexistentes, ineficazes ou inviáveis. Devido a eficácia das soluções *lighweight* para *IoT* e a pouca discussão no mercado comercial e acadêmico, esse trabalho discute arquiteturas e esquemas de segurança *lightweight* por visualizar contribuição científica e incontestável necessidade de amadurecimento desse tópico. Assim, serão explorados quatro trabalhos, dois que se autodenominam arquiteturas, uma baseada em *HIMMO* [12] e a outra denominada *OSCAR* [31], que se destacam principalmente por fazerem uma junção de tecnologias para proverem uma solução de criptografia com encriptação remota; e outros dois que se classificam como esquemas: *Lithe* [27] e *CoAPs-Lite* [29], sendo que ambos focam principalmente em implementar soluções de segurança para autenticação e confidencialidade, com latência reduzida.

Além desta introdução com a contextualização e proposta do trabalho, o restante deste artigo está organizado em outras três seções. Na Seção II estão os Trabalhos Relacionados. A Seção III estabelece a problemática de segurança em *IoT*. Na sequência,

na Seção IV, são discutidos dois esquemas e duas arquiteturas de solução *lightweight* para *IoT*. A Seção V faz um comparativo entre as arquiteturas e os esquemas. Ao final, na Seção VI estão as conclusões e expectativas de trabalhos futuros.

II. TRABALHOS RELACIONADOS

Não foram encontrados outros trabalhos de revisão que tratassem sobre segurança *lightweight* para *IoT*, apenas poucos trabalhos pontuais, com propostas de soluções e/ou contextos específicos. Por exemplo, alguns trazem revisões específicas sobre segurança em Redes de Sensores Sem Fio (RSSF), que é um dos contextos possíveis numa rede *IoT*. Outros tratam apenas de uma tecnologia de segurança, como algoritmos simétricos para dispositivos com recursos limitados. Também houve revisões mais amplas, no contexto geral de *IoT*, mas que traziam soluções de segurança sem necessidade de que fossem *lightweight* .

A Tabela I explicita um resumo comparativo entre os trabalhos relacionados que foram aqui analisados. A seguir, é possível conferir os comentários pertinentes a cada um deles.

Kong et al.[17] elaboraram um *survey* sobre soluções modernas de criptografia simétrica para dispositivos com recursos limitados, mas não especificamente só para dispositivos de *IoT*, nem com garantia de serem algoritmos *lightweight*. A discussão se baseia no emprego de algoritmos simétricos principalmente para Ambientes com Recursos Limitados, RSSF, Identificação por Radiofrequência (*RFID - Radio Frequency Identification*) e Plataformas *WISP* (*Wireless Identification and Sensing Plataform*).

No trabalho de Granjal et al.[14] é feita uma revisão sobre a segurança na integração de Redes de Sensores Sem Fio (RSSF) de baixa potência, com a Internet. Afirmam que essa discussão pode também ser estendida para *IoT*, pois as RSSF estão inclusas no mundo da Internet das Coisas. Assim, sua contribuição se torna bem específica e concisa se analisarmos o contexto de RSSF, mas limitada se for analisada a partir do contexto de *IoT*.

A robustez, segurança e privacidade em serviços baseados em localização para a Internet das Coisas foi verificada por Chen et al.[7]. Compreendem que a informação de localização é uma das informações cruciais para que se obtenha a inteligência e adaptabilidade ao contexto esperadas para sistemas de Internet das Coisas. Por isso, esse survey foca apenas em soluções de segurança para serviços de localização em *IoT*: discutem as ameaças e soluções relacionadas a posicionamento e localização; descrevem soluções de criptografia para esse tipo de serviço; e tratam das questões legais que compreendem este contexto.

Os *surveys* publicados por Borgohain et al.[5] e Granjal et al.[13] focam em apresentar problemas em detrimento a soluções de segurança e privacidade identificados em Internet das Coisas. Em [5] são abordados todos os problemas de segurança identificados para a *IoT* em conjunto com uma análise dos problemas de privacidade que um usuário final pode encontrar como consequência da expansão da *IoT*. Já em [13] o survey demonstra problemas existentes concernentes a protocolos e pontos de pesquisa em aberto na *IoT*.

Alaba et al.[1] e Mendez et al. [21] escreveram *surveys* focados em segurança e privacidade na visão geral do contexto de *IoT*. Ambos, como neste artigo, destacam a

importância e necessidade de tecnologias *lightweight* para que se possa implementar segurança com eficácia em *IoT*. No entanto, nenhum deles foca o trabalho nessa temática, apenas a discorrem subsidiariamente. Em [1] o foco é o estado-da-arte das ameaças de segurança e vulnerabilidades da *IoT*, expondo a taxonomia das atuais ameças de segurança no contexto de aplicação, arquitetura e comunicação. Já em [21] o objetivo é prover um *survey* sobre os desafios de segurança e privacidade da *IoT*, a partir de uma perspectiva das tecnologias e arquiteturas utilizadas.

Tabela 1. Comparativo entre Trabalhos Relacionados

Autores	Tipo	Considera Lighweight?	Foco
Kong et al.[17]	Survey	SIM	Criptografia simétrica para dispositivos com recursos limitados.
Granjal et al.[14]	Survey	NÃO	Segurança na integração de RSSF de baixa potência com a Internet.
Chen et al.[7]	Survey	SIM	Segurança e privacidade em serviços baseados em localização para *IoT*.
Borgohain et al.[5]	Survey	NÃO	Apresentar problemas de segurança e privacidade para usuário final da *IoT*.
Granjal et al.[13]	Survey	NÃO	Problemas concernentes a protocolos e pontos de pesquisa em aberto na *IoT*.
Alaba et al.[1]	Survey	SIM	Estado-da-arte das ameaças de segurança no contexto de aplicação, arquitetura e comunicação.
Mendez et al. [21]	Survey	SIM	Desafios de segurança e privacidade em *IoT*, com vistas a tecnologias e arquiteturas.
Tiburski et al.[28]	Artigo	SIM	Abordagens lighweight para a padronização de uma arquitetura segura para sistemas de middleware para *IoT*.

Assim, não foram encontrados outros *surveys* ou artigos de revisão especificamente sobre a temática de segurança *lighweight* para *IoT*. Entretanto, foi vislumbrado o artigo de Tiburski et al.[28], que não se trata de um *survey* ou revisão, mas optou-se por citá-lo nesta seção, visto que também traz a preocupação que é levantada no presente artigo, com a difusão de tecnologias *lighweight* factíveis e eficazes. Eles abordam a importância das abordagens *lightweight* para a padronização de uma arquitetura segura para sistemas de *middleware* para *IoT*. Destacam que a grande quantidade de dados que flui por um sistema de *middleware* demanda uma arquitetura segura, que garanta a proteção de todas as camadas do sistema, incluindo o canal de comunicação e as *APIs* (*Application Programming Interface*) de borda usadas para integrar as aplicações aos dispositivos de *IoT*.

Logo, esse trabalho propõe ser inédito ao fazer uma revisão sobre segurança *lightweight* para *IoT* e espera servir para, além de amadurecer essa discussão de modo geral, servir para os pesquisadores que buscam conhecimento introdutório e embasamento na área. Ainda, se postula como pertinente e de contribuição acadêmica e

mercadológica em discutir esta temática, porque ao pesquisar por "Segurança *Lighweight*" e "*Lighweight Security*" no Portal de Periódicos da Capes e diretamente em renomadas plataformas como *ACM Digital Library*, *IEEE Xplore Digital Library*, SciELO, Scopus e Google Acadêmico , foram encontrados publicados poucos trabalhos em inglês e nenhum em português. Foram também realizadas busca nestas bases bibliográficas por surveys e tra- balhos de revisão de tecnologias que tratassem pontualmente de segurança *lightweight* para a *IoT*. Nenhum foi encontrado.

Poucos trabalhos específicos sobre tecnologias de segurança *lightweight* para *IoT* foram encontrados. Assim, dentre aqueles disponíveis, resolveu-se optar por quatro trabalhos que, até o momento, foram aqueles que pareceram ter bom nível de amadurecimento e potencial para se tornarem propostas reais. São eles duas arquiteturas: Baseada em *HIMMO* [12] e *OSCAR* [31]; e dois Esquemas: *Lithe*[27] e *CoAPs-Lite*[29].

III. O PROBLEMA DE SEGURANÇA EM *IOT*

Como em qualquer outra tecnologia, em *IoT* há sérias preocupações com segurança. Algumas dessas preocupações são características específicas de *IoT*, outras são já conhecidas desde outras tecnologias. Borgohain et al. [5] falam sobre as tecnologias de conectividade que são utilizadas para Internet das Coisas e cita as Redes de Sensores Sem Fio (RSSF) e o *RFID* (*Radio Frequency Identification*) como as principais. Para esses tipos de rede, vários tipos de ataques e problemas já conhecidos foram reinventados e adaptados para explorar vulnerabilidades nessas redes. Alguns exemplos são: problemas de privacidade e autenticação em RSSF, ataques DoS, ataques de autenticidade, integridade, confidencialidade e disponibilidade em tags *RFID* e outros.

Para Zang et al. [33] o maior problema é que grande parte dos dispositivos produzidos para serem utilizados na internet das coisas não têm sido fabricados com as devidas precauções de segurança, embora já existam soluções embarcadas que fornecem este quesito por padrão, como a *suíte* de segurança do DASH7[2].

Há também problemas que nasceram com *IoT* e são típicos desse cenário. Como já há atualmente uma enorme oferta de dispositivos capazes de se conectar e fazer parte de uma rede de dispositivos de *IoT* e devido, principalmente, a heterogeneidade e escalabilidade desses dispositivos inteligentes, problemas de segurança envolvendo estes cenários são também mais complexos do que em cenários de conectividade tradicionais [33]. Além de dispositivos heterogêneos, em *IoT* encontramos também redes heterogêneas se comunicando. Logo, estruturas e protocolos heterogêneos se conectando tornam a proteção aos conteúdos dessa rede ainda mais complexa.

Em cenários de *IoT* é comum haver muitos dispositivos pequenos e com poder de processamento limitado, a ponto de não haver poder de processamento suficiente para implementar soluções de segurança convencionais, como os algoritmos de criptografia.

Imagine um cenário de *IoT* que existam dispositivos como: lâmpadas, roteadores, câmeras de vigilância, geladeira, ar-condicionado, etc. Por mais simples e desprovidos de inteligência computacional esses dispositivos possam parecer, eles estão em interação direta com o humano, fornecendo comodidades e capturando informações. Por isso, eles também precisam estar seguros. Aqui discutimos esses desafios: o quão leve uma solução de segurança precisa ser para conseguir se adaptar a todos esses dispositivos?

Assim, é preciso buscar soluções, como novos esquemas de criptografia, que utilizem baixo poder de processamento. Essas soluções "leves", são conhecidas em inglês por *lightweight*. Optamos aqui por utilizar o termo em inglês, por achar que não há uma tradução precisa para o mesmo.

IV. SEGURANÇA *LIGHTWEIGHT* PARA *IOT*

Em [16], criptografia *lightweight* é definida como um algoritmo ou protocolo criptográfico que é adaptado para implementação em ambientes heterogêneos, com diversidades de dispositivos com baixo poder computacional. Entre os dispositivos que compõem esse ambiente, estão as tags *RFID*, sensores, cartões inteligentes, dispositivos de atenção à saúde, entre outros.

Soluções *lightweight* têm sido exploradas tanto em nível de hardware, quanto em nível de software. Quanto ao hardware, são consideradas métricas as implementações quanto ao tamanho do chip e/ou consumo de energia. Já em questão de *software*, são desejáveis os menores códigos possíveis, ocupando o mínimo de memória RAM [16].

É importante esclarecer, que a intenção das tecnologias *lightweight* é entregar implementações mais leves e portáteis, mas que sejam, pelo menos, eficientes quanto as técnicas convencionais.

Logo, soluções de segurança *lightweight* tem se mostrado formas eficazes de resolver o problema de segurança em *IoT* em diversos aspectos. Os principais benefícios incluem:

- Portabilidade: o fato de poderem ser implementadas em qualquer tipo de dispositivo, com menor capacidade de processamento que seja.
- Integridade: podem ser implementados mecanismos de checagem de integridade da informação.
- Confidencialidade: Algoritmos com criptografia de ponta a ponta garantem que pessoas não autorizadas não conseguirão entender as mensagens.
- Autenticidade: as identidades dos usuários ou dispositivos poderão ser garantidas por, por exemplo, identificadores únicos presentes em cada dispositivo.
- Disponibilidade: informação sempre ao alcance dos dispositivos inteligentes quando necessária.
- Custo: soluções *lightweight* são viáveis mesmo em dispositivos pequenos e baratos, com baixo poder computacional, tornando-as viáveis em diversos tipos de cenários, sem altos investimentos.

Veremos a seguir, como as arquiteturas [12] e [31] e os esquemas [27] e [29] propõem soluções *lightweight* para a Internet das Coisas.

A. Arquiteturas lightweigth para IOT

A Internet das Coisas possibilita muitas aplicações para os objetos inteligentes, como controle de iluminação externa, energia inteligente e gerenciamento de água, ou sensores ambientais, em um ambiente de cidade inteligente [12].

A segurança em tais cenários permanece um desafio em aberto devido a natureza de recursos limitados dos dispositivos e redes ou os múltiplos caminhos em que oponentes podem atacar o sistema durante o ciclo de vida de um dispositivo inteligente.

Assim, [12] e [31] desenvolvem trabalhos com objetivos de segurança e operacionais em um cenário *IoT*. Em ambos trabalhos o cenário é inspirado em um ambiente de cidade inteligente. [12] e [31] apresentam uma arquitetura de segurança *lightweight* para assegurar a *IoT*. Em [12], essa arquitetura é focada no ciclo de vida de um dispositivo inteligente e a solução é baseada em um esquema *lightweight* denominado *HIMMO* [20]. Em [31] é apresentada uma arquitetura de segurança baseada em objeto, denominada *OSCAR* . O trabalho aproveita os conceitos de segurança tanto centrada em conteúdo, como abordagens orientadas a conexões tradicionais. É feita uma proposta de economia de energia em servidores restritos e sua aplicabilidade em Cidades Inteligentes.

Por arquitetura, nesse contexto, entende-se como uma composição de tecnologias. No caso de [12], a arquitetura é composta pelo esquema *HIMMO* para pré-distribuição de chaves, o *TTP* (Trusted Third Parties) para manipular as chaves dos objetos e o *DTLS* (Datagram Transport Layer Security) para prover a segurança da comunicação.

Já no caso de [31], é usado o *DTLS* para estabelecer canais seguros por meio de troca de chaves entre entidades comunicantes. Com o *CoAP* (*Constrained Application Protocol*), é feita a proteção contra ataques de repetição (*Replay*).

Mesmo com algumas diferenças de implementação, essas duas arquiteturas se inspiram em um cenário *IoT* em comum, e uma Cidade Inteligente. Ambas também trabalham em preocupações de segurança baseadas no ciclo de vida de um Objeto Inteligente. Para [12] o foco de sua implementação *lightweight* é atingir uma série de objetivos específicos de segurança e operabilidade da rede, enquanto [31] prima pela confidencialidade e autenticidade.

O Ciclo de Vida de um Dispositivo Inteligente é visto como o tempo de duração da comunicação deste dispositivo em uma rede inteligente de Internet das Coisas. Ele pode ser entendido como acessos a serviços intermitentes e trocas entre diferentes instâncias de serviços, por exemplo, a saída de uma rede sem fio para entrar em outra rede sem fio [25].

Tendo pontuado as semelhanças entre as arquiteturas [12] e [31], e estabelecidos os conceitos necessários para que se entenda como funcionam, a seguir é detalhado sobre cada uma delas.

1) Arquitetura lightweight baseada em HIMMO.

HIMMO [20], é um esquema de pré distribuição de chaves (*Key Pre-Distribution Scheme – KPS*), que automaticamente provê autenticação implícita dos nós e consequentemente, protege contra ataques do tipo *man-in-the-middle*. Ele é o primeiro esquema de pré distribuição de chaves inteligente tolerante a ataques em conluio.

O trabalho de [12] é baseado em *HIMMO*[11] e propõe uma arquitetura de segurança compreensiva que visa atender a objetivos de segurança e operacionais no contexto de ciclo de vida de um dispositivo inteligente, implantado em uma cidade

inteligente. Ele também pode ser facilmente integrado em protocolos de comunicação existentes, como o IEEE 802.15.4, padrão que especifica a camada física e o controle de acesso ao meio para Redes Pessoais Sem Fio de baixa taxa de transmissão [4]; ou *OMA LWM2M*, um protocolo *lightweight* criado pela *Open Mobile Alliance* para comunicação máquina a máquina (*M2M*) ou gerenciamento de dispositivos de Internet das Coisas [3].

Os autores dessa solução baseada em *HIMMO* afirmam que ela provê um número de vantagens de performance e inteligência de operação que soluções existentes não conseguem prover. Então, destacam todos os objetivos operacionais e de seguranças desejáveis para um cenário de cidade inteligente e que são atendidos por eles:

- Objetivos Operacionais:
  - Performance;
  - Adicionar dispositivo facilmente a um sistema em funcionamento;
  - Fácil gerenciamento de credenciais;
  - Fácil integração com protocolos existentes;
  - Adaptável ao ciclo de vida do dispositivo;
  - Segurança a longo prazo.
- Objetivos de Segurança:
  - Resiliente ao compromisso da raiz de confiança (*Root of Trust - RoT);*
  - RoT único não pode monitorar;
  - Garantia de chaves; – Facilitar a fabricação segura; – Autenticação e autorização de dispositivo;
  - Autenticação e autorização de backend;
  - Prevenção de ataques DoS;
  - Totalmente resistente a colisões;
  - Identificação e bloqueio de dispositivos;
  - Combinação de chaves;
  - Resiliência pós-quântica;
  - Segurança de encaminhamento perfeita;
  - Não repudiação.

Criptografia simétrica é *lightweight* , mas não é escalável. Criptografia assimétrica é escalável, mas não é *lightweight*. Assim, a necessidade da *IoT* é um esquema criptográfico escalável e *lightweight*. Por isso, o *HIMMO* possibilita que qualquer par de dispositivos em um sistema acordem diretamente uma chave simétrica baseada em seus identificadores e em um polinômio gerador de chave secreta. Como qualquer *KPS*, o *HIMMO* precisa de um *TTP* e isso é implementado através da Equação 1 [11]:

$$K\varepsilon,\eta = (G\varepsilon\ (\eta)N\square\square \qquad\qquad \square\square\square$$

Onde, *K* é a chave gerada; *G* é o polinômio gerador de chave; ε é o nó que quer comunicar com *η*; *N* é um módulo público, um número par de tamanho *(α + 1)B + b*, sendo *B* o tamanho de bits do identificador que será usado no sistema, b o tamanho de bits da chave que será gerada e α o grau máximo do polinômio. Então, *Kε,η e Kη,ε* têm que ser igual.

O processo de criptografia do *HIMMO* usa os identificadores de cada um dos dispositivos envolvidos na comunicação para gerar uma chave criptográfica assimétrica. Como os dispositivos de *IoT* podem não dispor de poder computacional suficiente para realizar o processo de criptografia assimétrica, uma forma de deixá-lo *lightweight* é fazer a criptografia simétrica, mas com garantia de autenticidade dos dispositivos através da consulta a um servidor *TTP* externo e retornando para os dispositivos a confirmação de autenticidade, para que possa prosseguir com a comunicação.

É considerado a utilização de múltiplo *TTP*, o que pode gerar e gerenciar de maneira segura as chaves de certificado raiz. Desta forma, credenciais de autenticação são fornecidas a objetos quando eles são fabricados e posteriormente verificadas quando ele tenta se conectar a uma rede.

Analisando a Figura 1, podemos enxergar o funcionamento desta arquitetura em quatro passos:

(i). Uma estrutura de raiz de confiança (*TTP*), que fornece e confirma credenciais. Quando um objeto é fabricado ele recebe uma credencial de confiança vinculado ao *TTP* que lhe fabricou. Mais tarde, quando esse objeto é instalado em uma rede *IoT*, ele deverá conectar-se a esse *TTP* para validar suas credenciais.

(ii). Fábricas que produzem objetos inteligentes. Todos os dispositivos de *IoT* produzidos por essas fábricas serão configurados com chaves secretas e credenciais providas pelas *TTP*s do passo (i).

(iii). Um processo de autenticação. Aqui o dispositivo fabricado no passo (ii) com as credenciais providas no passo (i) já está em uso em uma rede *IoT*. O procedimento então, é que esse objeto inteligente se registre com um sistema de *backend*, que irá verificar sua credenciais com as *TTP*s do passo (i), para garantir sua autenticidade e então, se confirmado lhe fornecer acesso a rede.

(iv). Uma fase de operação segura. Nesse passo os objetos inteligentes já foram autenticados através de suas credenciais checadas no passo (iii), realizaram com sucesso a conexão à sua rede de *IoT* e podem seguramente se comunicar uns com outros, usando as credenciais obtidas no passo anterior.

Essa implementação do *HIMMO* é dividida em dois módulos: um que provê as funcionalidades de *TTP* e deve ser implementado no servidor, e outro que provê as funcionalidades de nó e deve ser implementado no dispositivo. O módulo de *TTP* é feito em Java e pode facilmente ser integrado em um servidor. Já o módulo do nó sacrifica a portabilidade para oferecer melhor performance, com várias implementações possíveis, por causa da natureza heterogênea dos dispositivos.

Assim, ainda ficam dois principais questionamentos sobre esse trabalho:

(1) A autenticação na rede é dada principalmente pelas credenciais dos dispositivos. Dispositivos conhecidamente maliciosos podem ter suas credenciais inseridas em uma blacklist e o seu acesso revogado. Mas, e se um dispositivo autêntico tiver suas credenciais clonadas?

(2) Outra crítica, é a respeito da falta de portabilidade. Em uma rede *IoT*, é muito grande a variedade e heterogeneidade de dispositivos. Será que usando essa proposta, seria funcional se fazer tantas implementações específicas e customizadas quanto necessárias?

Essas são questões levantadas pelos autores deste survey, mas que não são tratadas no trabalho [12] e ficam em aberto.

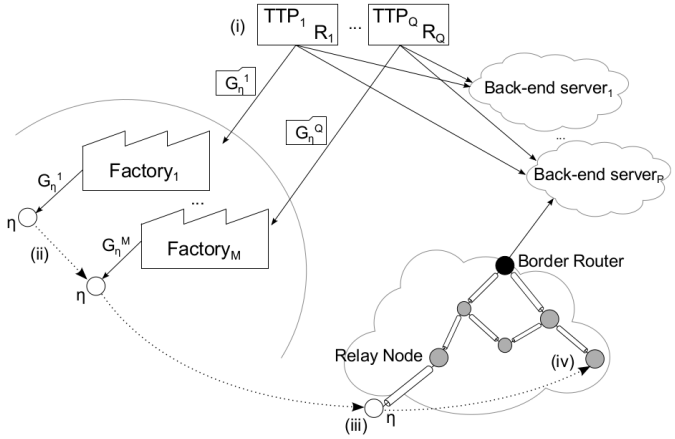

Figura 1. Visão Geral da Arquitetura [12]

2) OSCAR

OSCAR (Object Security Architecture) [31] é uma proposta que tem como objetivo aplicar seus conceitos de segurança tanto em redes centradas em conteúdo quanto àquelas abordagens tradicionais orientadas a conexões.

Essa arquitetura fornece segurança de ponta a ponta na Internet das Coisas, baseia-se no conceito de segurança do objeto, e foca a segurança em sua carga útil. Como objeto, são tratadas todas as "coisas" da Internet das Coisas. Por carga útil, se entende como a parte autenticada do objeto encriptado. Esse conceito de segurança de objeto visa proteger o conteúdo da informação em si. Assim, a segurança é introduzida dentro da carga útil do aplicativo, considerando confidencialidade e autenticidade como domínios separados.

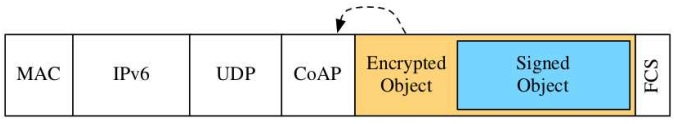

Figura 2. Segurança do Objeto[31]

A Figura 2 ilustra como é implementada por [31] a segurança do objeto. Os objetos nesse contexto estão protegidos dentro da pilha de rede da *IoT*. A seta representa a ligação da chave de criptografia do objeto com o cabeçalho *CoAP* subjacente. Ou seja, o objeto autenticado (*Signed Object*, na figura) é encriptado, usando como chave

criptográfica o cabeçalho *CoAP*. Assim, esse objeto autenticado é o que é considerado pelo autor como a carga útil do objeto criptografado e seu foco de segurança.

Já para realizar o processo de autenticidade, a *OSCAR* depende de canais seguros, que são providos pelo *DTLS*, uma solução de segurança implementada pelo *CoAP* (*Constrained Application Protocol*). Esses canais conectam os hosts até a central de distribuição de chaves.

A autenticidade está ligada a um host e o conteúdo é encapsulado dentro de objetos assinados digitalmente, o que garante confiança nas informações.

A confidencialidade é usada como um meio de fornecer controle de acesso e proteção contra a espionagem durante a comunicação. Para proporcionar confidencialidade de forma *lightweight*, em [31] a confidencialidade do conteúdo é assegurada por criptografia simétrica executada a partir de um servidor por demanda. Assim, os principais objetivos de segurança atingidos são: Proteção contra negação de serviço, Confidencialidade, Proteção ao Ataque de Repetição, Segurança de objeto com autenticação.

A proteção contra ataques de repetição é feita acoplando a chave de criptografia do conteúdo com o mecanismo de detecção de duplicação do *CoAP*. Além de atingir esses objetivos de segurança ponta a ponta e mecanismos de autorização e controle de acesso, *OSCAR* também propicia reduzido consumo de energia e baixa latência, pois diminui a quantidade de handshake, preservando características de *lightweight*. Ainda, oferece suporte a multicast, troca de mensagens assíncronas, implementa proxy e recursos de cache, apresenta baixa sobrecarga de comunicação e faz mapeamento de cabeçalhos para H*TTP*. Assim, se mostra muito útil em implantações de Smart Cities, pois possui fácil integração com Redes de Baixo Consumo e Baixa Potência (*LLN-Low-Power* e *Lossy Networks* – Padrão 802.15.4) e redes de comunicação Máquina a Máquina (Machine-to-Machine – M2M). Testes realizados nesses tipos de rede, demonstraram resultados em que *OSCAR* supera um esquema de segurança baseado em *DTLS* quando o número de nós aumenta. E ainda através dos testes e experimentos, os autores de [31] mostram economias de energia em servidores restritos e otimização de atrasos.

B. Esquemas lightweigth para IOT

Os padrões 6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks*), IEEE 802.15.4, juntamente com o protocolo *CoAP* têm sido apresentados como um dos principais protocolos da Internet das Coisas com suporte a entidades de padronização, como o ITU/T, ISO/IEC, IEEE, IETF, entre outras, principalmente no que se refere a alternativas para comunicação de dados em dispositivos limitados. Preocupadas em prover segurança neste cenário, estas entidades têm também trabalhado na definição de padrões e regulamentações relativas a segurança específicas para *IoT* [20]. Pesquisas desenvolvidas por [27] e [29] vão ao encontro destas proposições, onde os esquemas *Lithe* e *CoAP*s-*Lite* são apresentados, respectivamente.

1) *Lithe*: Segundo [27], o *DTLS* é o principal protocolo de segurança para garantia de autenticação e confidencialidade nas comunicações, ocorrendo sobre o UDP. É configurado por padrão para ser utilizado em redes com alta capacidade de banda e links confiáveis, mas, como discutido anteriormente, os cenários de comunicações da *IoT*

estão sujeitos a várias restrições que tornam o uso do *DTLS* "original" não aplicável. A principal limitação decorre do fato de que o *DTLS* realiza inúmeras trocas de mensagens para estabelecer uma sessão segura, o que acaba por ocasionar uma latência considerável e consequentemente demandar uma alta requisição de recursos energéticos nos dispositivos de *IoT*. Recursos estes, geralmente escassos.

O *Lithe* é então apresentado por [27] como uma integração de *DTLS* e *CoAP* para *IoT*. Essa solução acontece num cenário onde a utilização do padrão 6LoWPAN é também a principal opção para permitir o uso de IP em redes sem fio de baixa potência, sujeitas a perdas, como as redes de sensores sem fio (*WSNs*). Embora o 6LoWPAN já defina a compressão de cabeçalhos IPV6, ele somente utiliza como opção de segurança o *DTLS*. O *Lithe*, então, aproveita esta disponibilidade para realizar uma compressão de cabeçalhos *DTLS* de forma que seja garantida a autenticação, confidencialidade e integridade sobre o *CoAP*.

A compressão de cabeçalhos do *Lithe* funciona basicamente considerando que o *DTLS* consiste em duas camadas: a camada inferior contém o protocolo Record e a camada superior contém um dos três protocolos: Handshake, Alert e ChangeCipherSpec. O protocolo Record adiciona campos de cabeçalho longos de 13 bytes para cada pacote e é enviado durante toda a vida útil de um dispositivo que usa *DTLS*. O protocolo handshake, por outro lado, adiciona 12 bytes de cabeçalho para mensagens de handshake. O *Lithe* comprime os cabeçalhos Record e Handshake a medida que reduz o comprimento dos cabeçalhos para 5 e 3 bytes, respectivamente. Como os pacotes são menores, também diminui-se a fragmentação das mensagens, reduzindo o overhead e consequentemente as vulnerabilidades relativas a ataques de fragmentação.

A implementação do *Lithe* foi realizada utilizando o sistema operacional *Contiki*[24] e em um hardware real, o *WiSMote*.

Ao comprimir cabeçalhos *DTLS* sobre o *CoAP*, os autores comprovam uma melhora no consumo energético, no tempo de processamento e resposta, além de proporcionar uma compatibilidade nas comunicações fim a fim sem prejudicar ou interferir nos padrões de segurança já estabelecidos na internet, garantindo a interoperabilidade entre dispositivos. Uma clara desvantagem do *Lithe* deve-se ao fato de que quando o protocolo RDC (Radio Duty Cycling) está ativado os ganhos com a redução de latência são minimizados.

2) *CoAPs-Lite:* O *CoAP*s-*Lite* é um esquema proposto por [29], baseado na modificação em cabeçalhos do *CoAP*, que adiciona um componente de autenticação chamado Auth-*Lite*. Ele oferece uma solução de segurança lightweigh para utilização em um cenário customizado de *IoT*.

O cenário apresentado por [29] consiste de um veículo de transporte comercial dispondo de um dispositivo de *IoT*. Considerando que estes veículos estão sujeitos a ataques de interceptação de mensagem, de reprodução, man-in-the-middle, entre outros, alternativas existentes de segurança como o uso do *DTLS*, oferecem segurança requerendo um threshold com requisitos de baixa latência. Isso se deve principalmente ao fato de que neste cenário, veículos trafegam com alta mobilidade e alta velocidade. Logo, a perda de pacotes é uma constante.

Portanto, como solução às limitações do *DTLS* neste ambiente, os autores propuseram excluí-lo, substituindo-o pelo componente Auth-*Lite* [29]. Desta forma,

fornecem um meio de autenticação e gerenciamento de chaves, garantindo a autenticidade, com um esquema que realiza menos trocas de mensagem que o *DTLS*. Reduz também a troca de mensagens nas requisições do *CoAP*, garantido ainda assim a confidencialidade através de uma troca de chaves simétricas, que utiliza o AES com Cadeia de Cifra de Bloco de 128 bits (Cipher Block Chaining – CBC). A integridade é otimizada também a medida que uma baixa taxa de perda de pacotes acontece, visto que as etapas de autenticação e requisições passam a requerer um menor número de mensagens trafegando na rede. Em [29] é realizada ainda uma análise de segurança que comprova a eficácia do *CoAP*s-*Lite* em relação a ataques como o ataque de reprodução.

Algumas restrições a implantação do *CoAP*s-*Lite* são o fato de que é necessário um ID único e uma chave privada a serem instaladas nos dispositivos no momento da fabricação ou da implantação. Esse ID é utilizado para autenticar o veículo em sua comunicação com o servidor de backend da empresa, que possui uma tabela com os IDs autorizados a comunicar. Feita a autenticação, o dispositivo está pronto para enviar os dados. Isso será feito através do protocolo de comunicação *CoAP* já otimizado (*CoAP*s-*Lite*) e criptografado com o algoritmo AES. Quando o dado chega no servidor, ele está disponível para ser acessado pela rede de internet convencional. Estas restrições limitam o uso do *CoAP*s-*Lite* de forma ampla, à medida que requerem que seja aplicado em um cenário customizado. Verifica-se, portanto, três contribuições principais deste trabalho para um cenário de *IoT*:

- Garantia de segurança: os princípios de confidencialidade, autenticidade e integridade são mantidos mesmo realizando alterações no *DTLS*, com comprovada proteção a ataques como o ataque de interceptação de mensagem, de reprodução, man-in-the-middle, entre outros.
- Redução na Perda de Pacotes: um dos problemas mais comuns em redes sem fio. A redução da latência teve resultados significativamente positivos, acarretando redução de perdas de pacotes.
- Redução da Latência: Como resultado direto da diminuição significativa na perda

de pacotes, a latência na troca de mensagens não excede 5% quando a perda de pacotes é de 20%.

Tabela II . Comparativo entre arquitetura baseada em HIMMO E OSCAR

	Arquitetura Baseada em HIMMO	***OSCAR***
Autenticação	Na nuvem, por *TTP*	Na nuvem, através do esquema de carga útil.
Tecnologias Utilizadas	*HIMMO*, *TTP* e *DTLS*	*DTLS* e *CoAP*
Padrões	IEEE 802.15.4 e OMA LWM2M	IEEE 802.15.4 e LLN
Segurança	É um esquema de pré distribuição de chaves, que automaticamente, provê autenticação implícita dos nós através de uma arquitetura segmentada e modular	Usa conceito de segurança do objeto, e foca a segurança em sua carga útil.
Modular	Sim, possui módulo de backend e dispositivo.	Não se aplica
Latência	Varia de acordo com cenário e aumenta conforme a necessidade de troca de informação de autenticação entre os objetos.	Linear, em teste no WiSMote.
Consumo Energético	Não é avaliado.	29.7% menos.

V. COMPARATIVO

As arquiteturas [12] e [31] mostraram em comum o fato de usarem a nuvem para auxiliar o processo de autenticação. Esse procedimento é extremamente eficaz para complementar a segurança de algoritmos simétricos e evitar conexão de dispositivos não autênticos, que poderiam gerar ataques, como um DoS. No entanto, é válido lembrar que essa comunicação adicional gera um aumento nas taxas de transferências, e é preciso analisar em cada cenário se esse aumento gerará desvantagem ou será imperceptível.

Também, consideremos que as questões de possível clonagem de credenciais e necessidade de customização de implementação de um módulo de nó para cada dispositivo em [12] são questões em aberto. A proposta de arquitetura de [12] compreende a junção das tecnologias *HIMMO*, *TTP* e *DTLS* funcionando sobre os padrões IEEE 802.15.4 ou OMA LWM2M, além de implementar um esquema de funcionamento distribuído em 4 fases e com dois módulos diferentes. Em [31], a arquitetura é composta por tecnologias como *DTLS* e *CoAP*, mas também permite integração ao padrão IEEE 802.15.4 e Low-Power and Lossy Network (LLN). Já as propostas de Esquemas, [27] e [29], trazem como principal ponto em comum uma modificação no *DTLS*.

Entretanto, essas modificações não incorrem na perda dos princípios confidencialidade, autenticidade e integridade com comprovada proteção a vários famosos ataques. A Tabela II mostra a comparação entre as arquiteturas baseadas em *HIMMO*[12] e a *OSCAR* [31]. As duas arquiteturas trazem semelhança na forma de autenticar, na nuvem, embora de formas diferente: *HIMMO* usando *TTP*s e *OSCAR* implementando seu conceito de segurança de carga útil do objeto. Demonstram

semelhança também em utilizar a mesma tecnologia para assegurar o canal de comunicação, o *DTLS*, mas diferem quando [12] realiza a autentica- ção por *TTP*s e *OSCAR* [31] através do *CoAP*. Ambas funcionam sob o padrão IEEE para *IoT*, o 802.15.4, mas também se espandem para padrões mais específicos, como o OMA LWM2M para *HIMMO* e LLN para *OSCAR*.

O *HIMMO* possui uma interessante característica modular, que designa módulos diferentes para backend do sistema e dispositivo, enquanto *OSCAR* não possui essa possibilidade.

Tabela III. comparativo entre CoAPs LITE e LITHE

	CoAPs-Lite	***Lithe***
Autenticação	Através da adição do componente Auth-*Lite*	*Lithe* (*CoAP* + *DTLS*).
Tecnologias Utilizadas	*CoAP*	*CoAP* e *DTLS*
Padrões	Aplicável a comunicação veicular	6LoWPAN
Segurança	Propõe um esquema de segurança no *CoAP*, usando algoritmo AES de chave simétrica de 128. Preserva os princípios confidencialidade, autenticidade e integridade, com comprovada proteção a ataques como o ataque de interceptação de mensagem, de reprodução, man-in-themiddle.	Preserva os princípios confidencialidade, autenticidade e integridade com comprovada proteção a ataques de fragmentação.
Latência	Não excede 5% quando a perda de pacotes é de 20%.	Não é avaliado.
Consumo Energético	Não é avaliado.	Apresenta economia de até 15% na troca de mensagens.

O consumo de energia infelizmente não é avaliado na arquitetura *HIMMO*, mas atinge consideráveis 29.7% a menos na *OSCAR*. Dois dos itens comparados que mais chamaram atenção aqui foram segurança e latência. Segurança, porque enquanto *OSCAR* aposta sua leveza necessária no minimalismo de assegurar apenas a carga útil do objeto, *HIMMO* já prefere usar técnicas de baixo poder computacional, mas distribuídas pela estrutura da arquitetura e com níveis de segurança diferentes.

No entanto, são justamente essas características de segurança que também ditam a diferença na Latência, o outro fator de atenção. Como a técnica de segurança de *OSCAR* é mais simplista, com um teste no WiSMote foi comprovada latência linear. Em *HIMMO*, todavia, a estrutura de segurança modular e em níveis, evita demanda de processamento, mas traz grande necessidade de troca de mensagens entre os objetos inteligentes e seus controladores. Dessa forma, a latência será escalar: quanto maior a quantidade de dispositivos que devem comunicar entre si e com os dispositivos de controle, maior será a troca de mensagens. Já a Tabela III, apresenta uma comparação entre os esquemas *Lithe* [27] e *CoAP*s Auth-*Lite* [29]. Cada um deles desenvolveu seu método específico de autenticação, por isso não se assemelham nesse quesito. As tecnologias utilizadas são parecidas, pois enquanto o *CoAPsLite* utiliza apenas o *CoAP*, o *Lithe* usa o *CoAP* integrado ao *DTLS*. Os padrões empregados,assim como os objetivos, são diferentes. *CoAP*s-*Lite* se aplica a comunicação veicular, enquanto *Lithe* foca em redes com baixa capacidade energética.

No quesito segurança os dois esquemas se beneficiam dos princípios de confidencialidade, autenticidade e integridade oferecidos pelo *CoAP*. A latência, assim como a perda de pacotes não são tópicos avaliados no *Lithe*, mas o *CoAP*s-*Lite* avalia e

atinge oferece latência de no máximo 5% para quando a perda de pacotes não é maior do que 20%. Já quanto ao consumo de energia, somente o *Lithe* fez os testes e apresentou uma economia de até 15% quando na troca de mensagens.

VI. Conclusões e trabalhos futuros

Diversas são as questões em aberto diante o novo paradigma da *IoT*. Requisitos de segurança são uma das principais questões a serem resolvidas para que esta se desenvolva e alcance o nível de aceitação visto atualmente na internet tradicional.

Soluções como as apresentadas em [12], [31], [27] e [29], são proposições que podem ser consideradas em trabalhos futuros. Já se tem várias propostas de soluções de conexão e comunicação em *IoT* atualmente, mas ainda são poucas as propostas de segurança.

Destas, muitas ainda apresentam apenas adaptações de modelos de segurança já conhecidos, que por vezes se tornam inviáveis e/ou não funcionais devido à dificuldade em lidar com contextos heterogêneos ou exigir alta capacidade de processamento. A maior contribuição de todos os trabalhos revisados aqui são suas propostas *lightweight*, que têm soluções de processamento leve e capacidade de funcionamento em dispositivos e redes heterogêneas. No entanto, atualmente essa ainda é uma área que se tem pouco discutido e os trabalhos publicados a respeito ainda são escassos. Por isso, foram escolhidos para serem discutidos aqui os trabalhos que pareciam mais promissores e relevantes diante esse desafio e suas especificidades. As propostas trazem grande contribuição para questões de autenticidade, confidencialidade e integridade, mas ainda há muito o que se discutir sobre estes tópicos. As expectativas levantadas para trabalhos futuros se dão nos bons pontos de pesquisa ainda em aberto em *IoT* que essa pesquisa possibilitou enxergar. Se fosse possível agora, pegar o melhor de cada uma dessas propostas, o resultado seria uma tecnologia de segurança para a Internet das Coisas realmente leve, em nuvem, modular, amplamente compatível, com segurança incremental, de baixa latência, com reduzido consumo energético e pouca perda de pacotes. Assim, como trabalho futuro, é visada a proposta de uma tecnologia *lightweight* para *IoT* que possa reunir no mínimo mais qualidades do que uma dessas arquiteturas ou esquemas analisadas e idealmente todas essas vantagens aqui apontadas.

REFERÊNCIAS

[1] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. Internet of Things Security: A survey. Journal of Network and Computer Applications 88, April (2017), 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

[2] DASH7 Alliance. 2016. DASH7 Alliance Protocol. (2016). http://www.dash7-alliance.org/dash7-alliance-protocol

[3] Open Mobile Alliance. 2016. OMA Lightweight M2M v1.0. (2016). http://technical.openmobilealliance.org/Technical/technical-information/ release-program/current-releases/oma-lightweight m2m-v1-0

[4] IEEE Standards Association. 2016. IEEE 82.15: Wireless Personal Area Networks (PANs). (2016). https://standards.ieee.org/about/get/802/802.15.html

[5] Tuhin Borgohain, Uday Kumar, and Sugata Sanyal. 2015. Survey of Security and Privacy Issues of Internet of Things. arXiv preprint arXiv:1501.02211 (2015), 7. arXiv:1501.02211 http://arxiv.org/abs/1501.02211

[6] Edson (Revista Galileu/Globo) Caldas. 2014. Internet das coisas: aparelhos conectados à rede são destaque na CES. (2014)..globo.com/Tecnologia http://revistagalileu/noticia/2014/01/internet-das-coisas-aparelhos-conectados-rede-sao-destaque-na-ces.html

[7] Liang Chen, Sarang Thombre, Kimmo Jarvinen, Elena Simona Lohan, Anette K Alen-Savikko, Helena Leppakoski, Mohammad Zahidul Hasan Bhuiyan, Shakila Bu-Pasha, Giorgia N. Ferrara, Salomon Honkala, Jenna Lindqvist, Laura Ruotsa- lainen, Paivi Korpisaari, and Heidi Kuusniemi. 2017. Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. IEEE Access V, c (2017), 1–1. https://doi.org/10.1109/ACCESS.2017.2695525

[8] Nailton Vieira de Andrade Jr, Jeferson Lima de Almeida, Ramon Dias Costa, Leandro José Silva Andrade, Geroge Pacheco Pinto, and Cassio Vinicius Serafim Prazeres. 2015. Web of Things Gateway: A Performance Evaluation. In Proce- edings of the 21st Brazilian Symposium on Multimedia and the Web (WebMedia '15). ACM, New York, NY, USA, 25–32. https://doi.org/10.1145/2820426.2820440

[9] Tito Gardel do Prado Filho and Cassio Vinicius Sera m Prazeres. 2015. MultiAuth-WoT: A Multimodal Service for Web of Things Athentication and Identi cation. In Proceedings of the 21st Brazilian Symposium on Multimedia and the Web (Web- Media '15). ACM, New York, NY, USA, 17–24. http://doi.org/10.1145/2820426. 2820438

[10] Paulo Artur Duarte, Luís Fernando Maia Silva, Francisco Anderson Gomes, Windson Viana, and Fernando Mota Trinta. 2015. Dynamic Deployment for Context-Aware Multimedia Environments. In Proceedings of the 21st Brazilian Symposium on Multimedia and the Web (WebMedia '15). ACM, New York, NY, USA, 197–204. http://doi.org/10.1145/2820426.2820443

[11] OSCAR García-Morchón, Domingo Gómez-Pérez, Jaime Gutiérrez, Ronald Riet-man, Berry Schoenmakers, and Ludo Tolhuizen. 2015. HIMMO: A Lightweight Collusion-Resistant Key Predistribution Scheme. (2015).

[12] OSCAR Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, and Jose Luis Torre-Arce. 2016. A Comprehensive and Lightweight Security Ar- chitecture to Secure the IoT Throughout the Lifecycle of a Device Based on HIMMO. International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (2016).

[13] Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva. 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials 17, 3 (2015), 1294–1312. http://doi.org/10.1109/COMST.2015.2388550

[14] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. 2015. Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey. Ad Hoc Networks 24, PA (2015), 264–287. http://doi.org/10.1016/j.adhoc.2014.08. 001

[15] Gilson Cruz Junior and Erineusa Maria da Silva. 2010. A (ciber)cultura corporal no contexto da rede:. Rev. Bras. Ciênc. Esporte 32 (2010), 89–104.

[16] Masanobu Katagi and Shiho Moriai. 2008. Lightweight cryptography for the Internet of Things. Sony Corporation (2008), 7–10.

[17] Jia Hao Kong, Li Minn Ang, and Kah Phooi Seng. 2015. A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. Journal of Network and Computer Applications 49 (2015), 15–50. http://doi.org/10.1016/j.jnca.2014.09.006

[18] B. Krebs. 2016. Did the Mirai Botnet Really Take Liberia Offline? (2016). http://krebsonSecurity.com/2016/11/did-the-Mirai-botnet-really-take-liberia-offline

[19] Shancang Li, Theo Tryfonas, and Honglei Li. 2016. The Internet of Things: a Security point of view. Internet Research 26, 2 (2016), 337–359. http://doi.org/10.1108/IntR-07-2014-0173 arXiv:/dx.doi.org/10.1108/BIJ-10-2012-0068

[20] Aref Mebbed. 2016. Internet of Things Standards: Who stands out from the crowd? (2016), 40–47.

[21] Diego Mendez, Ioannis PapapanagIoTou, and Baijian Yang. Internet of Things: Survey on Security and Privacy. 1–16. arXiv:1707.01879 http://arxiv.org/pdf/1707.01879.pdf

[22] Cintia Carvalho Oliveira, Daniele Carvalho Oliveira, João Carlos Gonçalves, and Julio Toshio Kuniwake. 2016. Pratical Introduction to Internet of Things: Practice Using Arduino and Node.Js. In Proceedings of the 22Nd Brazilian Symposium on Multimedia and the Web (Webmedia '16). ACM, New York, NY, USA, 17–18. http://doi.org/10.1145/2976796.2988224

[23] Maire O'Neill. 2016. InSecurity by Design: Today's IoT Device Security Problem. Engineering 2, 1 (2016), 48–49. http://doi.org/10.1016/J.ENG.2016.01.014

[24] Contiki Organization. 2016. Contiki: The Open Source OS for the Internet of Things. (2016). http://www.contiki-os.org

[25] Stefan Poslad. 2009. Ubiquitous Computing: Smart Devices, Environments and Interactions. Wiley.

[26] Shahid Raza. 2013. Lightweight Security Solutions for The Internet of Things. Vol. 2013. 1–69 pages.

[27] Shahid Raza, Hossein Shafagh, Kasun Hewage, Rene Hummen, and Thiemo Voigt. 2013. Lithe: Lightweight secure CoAP for the Internet of Things. IEEE Sensors Journal 10 (2013), 3711–3720.

[28] Ramao Tiago Tiburski, Leonardo Albernaz Amaral, Everton De Matos, Dario F.G. De Azevedo, and Fabiano Hessel. 2016. The Role of Lightweight Approaches Towards the Standardization of a Security Architecture for IoT Middleware Systems. IEEE Communications Magazine 54, 11 (2016), 56–62. http://doi.org/10.1109/MCOM.2016.1600462CM

[29] Arijit Ukil, Soma Bandyopadhyay, Abhijan Bhattacharyya, Arpan Pal, and Tulika Bose. 2014. Lightweight Security scheme for IoT applications using CoAP. International Journal of Pervasive Computing and Communications 4 (2014), 372–392.

[30] Marcos Alves Vieira and Sergio T. Carvalho. 2016. Addressing the Concurrent Access to Smart Objects in Ubiquitous Computing Scenarios. In Proceedings of the 22Nd Brazilian Symposium on Multimedia and the Web (Webmedia '16). ACM, New York, NY, USA, 79–82. http://doi.org/10.1145/2976796.2988166

[31] Malisa Vucinic, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, and Roberto Guizzetti. 2014. OSCAR : Object Security Architecture for the Internet of Things. (2014).

[32] Wikipedia. 2016. Mirai (malware). (2016). http://en.wikipedia.org/wiki/Mirai

[33] Zhi Kai Zhang, Michael Cheng Yi Cho, Chia Wei Wang, Chia Wei Hsu, Chong Kuan Chen, and Shiuhpyng Shieh. 2014. IoT Security: Ongoing challenges and research opportunities. Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014 (2014), 230–234.

[34] S Zhou and Z Xie. 2012. On Cryptographic Approaches to Internet-Of-Things Security. (2012). http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/papers/ZhouSujing.pdf