South American Development Society Journal

Vol.: 06, | Nº.: 18 | **Ano:** 2020 | **ISSN:** 2446-5763 | **DOI:** 10.24325/issn.2446-5763.v6i18p301-316
Data de Submissão: 17/10/2020 | **Data de Publicação:** 11/12/2020

SEGURANÇA DA INFORMAÇÃO PARA APLICAÇÕES IOT – INTERNET OF THINGS

Estefânia A. Pianoski Arata

Mestre em Engenharia da informação – UFABC, Especialista em Segurança da Informação. Especialista em Formação Pedagógica, Licenciada em Matemática, Graduada em Tecnologia da Informação. Coordenadora de Projetos na CESU – CPS. Professora de Ensino Superior e Técnico.

Maikol Nascimento

Doutorando em Ciências Sociais - PUC-SP. Mestre em Administração pela PUC-SP. Especialista em Gestão Empreendedora pelo Centro Universitário Senac. Bacharel em Administração - PUC-SP. Professor de Pós-Graduação no Centro Universitário Senac São Paulo; Professor do Centro Paula Souza

Caroline Batista Fantini de Novais

Mestre em Língua Portuguesa - PUC/SP, Especialista em Língua Portuguesa - PUC/SP, Licenciada em Letras - Universidade São Marcos. Docente no CEETEPS.

Resumo

Internet das Coisas também conhecida como IoT, vem tomando frente a novos negócios e pesquisas, o termo representa a conexão de objetos, capazes de se comunicarem e compartilharem informações entre si. Essa tecnologia é relativamente nova, e com isso carrega algumas limitações precisam melhorar, principalmente a questão de segurança da informação. Afinal, com o surgimento da Internet das Coisas - IoT - Internet of Things, estima-se que em 2020 entre 20 e 50 bilhões de dispositivos estejam conectados à Internet, possibilitando que ao mundo dos negócios, novas oportunidades e aplicações. Mas para que esses cenários surjam, segurança da informação é fundamental. Atualmente a Internet usa criptografia, protocolos e normas, para tratar as questões de segurança. Sendo esse, um desafio para IoT.

Palavras-chave—Internet das Coisas, Segurança da Informação, aplicações.

Abstract

Internet of Things, also known as IoT, has been at the forefront of the minds of the latest new businesses and research. The expression represents the connection between different objects, capable of communicating and sharing information between them. As this is a relatively new technology, improvements still need to be made, especially when it comes to data protection. After all, it is estimated that with the rise of IoT, about 20 to 50 billion devices will be connected to the internet in 2020, which will result in new applications and opportunities for businesses. Data protection is therefore crucial to enable these opportunities. Currently, internet uses cryptography, policies and regulations to protect data and those things are another challenge for IoT.

Key words: Internet of things, Data protection, applications.

INTRODUÇÃO

Pesquisar Internet das Coisas, do inglês Internet of Things (IoT) é um termo utilizado para representar vários aspectos relacionados a interconexão entre o meio físico com a Internet. E em um futuro próximo, estima-se que em 2020 entre 20 e 50 bilhões de dispositivos estejam conectados à Internet [1].

Pesquisas realizadas pelo Census Bureaux em 2014 mostram que os brasileiros passam mais de seis horas conectados na Internet, para enviar e-mail, utilizar redes sociais, aplicativos para Smartphones, jogos e muitas outras tarefas, com isso observa-se que as pessoas estão cada vez mais conectadas. A internet é vista como um grande avanço tecnológico, uma oportunidade de negócio, com a criação e utilização de objetos inteligentes (IoT).

Inúmeras aplicações com equipamentos são desenvolvidas com tecnologia IoT, tais como: sensores e atuadores que monitoram e interagem como meio físico, viabiliza cenários urbanos, saúde, transporte, monitoramento de trafego e urbano, predial, industrial, agronegócios entre outros [2].

Dentre as tecnologias utilizadas para Internet das Coisas está o RFID (Radio Frequency Idenfitication), uma tecnologia utilizada para identificar, rastrear e gerenciar

documentos e produtos; outra tecnologia utilizada é a de Redes de Sensores sem Fio (RSSF), um pouco mais complexa, que exige maior consumo de energia [3].

É relativamente novo o assunto segurança da informação para IoT, o termo remete a confidencialidade, integridade e disponibilidade da informação, que remete também a autenticidade, confiabilidade e não repúdio, para garantir os pilares da segurança da informação muitos conceitos são envolvidos, entre eles padronização nos protocolos, criptografia, entre outros [4].

Alguns trabalhos relacionados a protocolos de redes para aplicações IoT já foram desenvolvidos, com propostas de adaptações, como é o caso do 6LowPAN com mecanismo de compreensão de cabeçalho para trabalhar como uma camada de adaptação entre a camada de rede e a IEEE802.15.4, sendo o IPv6 muito comprido para utilizar em dispositivos tão pequenos [2].

Quanto a camada de transporte para Internet tem os protocolos Transport Protocol Data Unit (TCP), protocolo orientado a conexão e User Datagram Protocol (UDP), protocolo não orientado a conexão. Onde o TCP é considerado um protocolo seguro, o qual estabelece uma conexão confiável, mas devido algumas restrições não consegue, ainda, ser utilizado para IoT. E para proporcionar segurança a camada de transporte aplicada aos padrões IoT estudos indicam o protocolo Datagram Transport Layer Security (DTLS), desenvolvido para imitar o protocolo TLS, o qual será visto com mais detalhes nas próximas secções [5] [6].

II. OBJETIVO

Com o crescente avanço tecnológico para Internet das Coisas com uso seguro, esse trabalho tem como objetivo estudar sobre aplicações IoT, assim como os conceitos de segurança da informação aplicada a mesma, expondo possíveis padrões de protocolos de redes para seu funcionamento, juntamente a uma conexão segura para o usuário final. Empresas, precisam de segurança da informação, para que possam utilizar as aplicações, que IoT pode proporcionar.

O objetivo específico da pesquisa é expor as características dos protocolos utilizados em aplicações IoT e seus aspectos de segurança, pois a mesma tem restrições, como tamanho do dispositivos, capacidade computacional e consumo de energia, quesitos que dificultam algumas implementações entre elas segurança.

III. METODOLOGIA

Este artigo representa um survey, com principais características sobre aplicações para Internet das Coisas, com desafios como segurança da informação, consumo de energia e tamanho dos dispositivos. Devido às dificuldades para essas aplicações o tema irá expor sobre o protocolo DTLS, para tratar problemas de segurança da informação e adaptação com as características que acompanham IoT.

IV. INTERNET DAS COISAS

O termo Internet das Coisas, muito discutido na atualidade, remete a interação entre diversos objetos que são capazes de comunicarem uns com os outros, através de tecnologias conectadas por uma rede. Alguns autores ainda ressaltam que é preciso tomar cuidado ao utilizar a nomenclatura, Internet of Things [7].

O uso da Internet das Coisas veio para alavancar o conceito de conexão, pois pesquisas desenvolvidas pelo NIC- Conselho Nacional de Inteligência dos EUA prevê que em 2025 todos os objetos do cotidiano, entre eles embalagens, documentos e outros, poderão estar conectados à internet, podendo ser esses objetos quaisquer dispositivos. A figura 1, abaixo pode mostrar o que se conecta a Internet das Coisas [8].

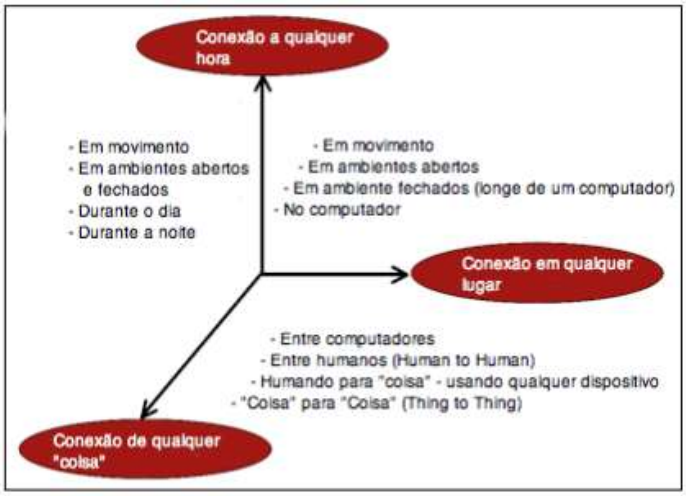

Fig. 1 Exemplo do uso da Internet das Coisas.[10]

Uma explicação bem simples para o desenvolvimento da IoT, do inglês Internet of Things, é quando objetos como geladeira, fogão, carros, até mesmo seres vivos, como

animais e pessoas, estão conectados diretamente a internet, para facilitar a comunicação e a tomada de decisão para atingir um mesmo objetivo a qualquer hora e em qualquer lugar [9].

Mesmo com tantas utilidades e avanços relacionados a essa tecnologia, encontra-se restrições para suas aplicações sendo a falta de padronização nos protocolos de redes, baixos recursos computacionais e de energia dos dispositivos da IoT- Internet of Things, entre outros desafios que precisam de atenção. Essa tecnologia é composta de um número muito grande de objetos conectados, transmitindo dessa maneira, também, um grande fluxo de dados em rede, interligando e traduzindo as informações do meio físico conectado e respondendo a essas informações, dessa maneira gerando a interação entre si [10] [1].

Há uma grande dificuldade para alguns, imaginar como seria o meio físico respondendo entre si a ações realizadas por uma geladeira, por exemplo, ou então a carros que encontram seus estacionamentos. Para possibilitar o entendimento das aplicações a Internet das Coisas os exemplos de aplicações são descritos na próxima seção mostram como essa tecnologia pode ajudar em tantos setores diferentes.

V. EXEMPLOS DE APLICAÇÕES

A IoT- Internet of Things proporciona uma grande aplicabilidade para empresas, meio ambiente, cotidiano de pessoas comuns, novos negócios, uma vez que utilizados adequadamente, com tecnologias seguras e que não proporciona problemas irreparáveis para o meio ambiente e a segurança pessoal [1].

Para possibilitar a interação entre diversas coisas, ou objetos, conectadas, como são chamadas, há necessidade de tecnologias como redes de sensores sem fio, as quais se impulsionaram com criações militares, formada por nós, os quais interagem entre si, a falha que pode ocorrer está relacionada a interligação sem fio entre eles. Esses nós devem ter baixo custo, baixo consumo e tamanho reduzido, essas restrições trazem algumas dificuldades para suas aplicações.

Também utilizado para IoT, o RFID (Radio-Frequency IDentification) uma tecnologia de transmissão por meio de ondas de rádio, que torna possível o rastreamento, identificação e troca de informação e troca de informação com outros dispositivos que também possuem a mesma interface. Tecnologia muito similar a um código de barras.

Atualmente utilizadas em aplicações de cobrança automática de carros em uma determinada distância, monitoramento do ciclo de vida de produtos, entre outros [11][7].

Existem outras tecnologias que possibilitam essa interação tais como M2M, que também possibilita diversas aplicações, entre elas utilização em robôs, transporte, tecnologia de casas inteligentes, entre outas. Existem outras tecnologias que proporcionam a Internet das Coisas entre elas atuadores e NFC. [11].

Ainda que exista problemas para implementação da Internet das Coisas, a mesma também proporciona avanços para muitos setores, como pode ser visto na figura 2 e algumas listadas abaixo.

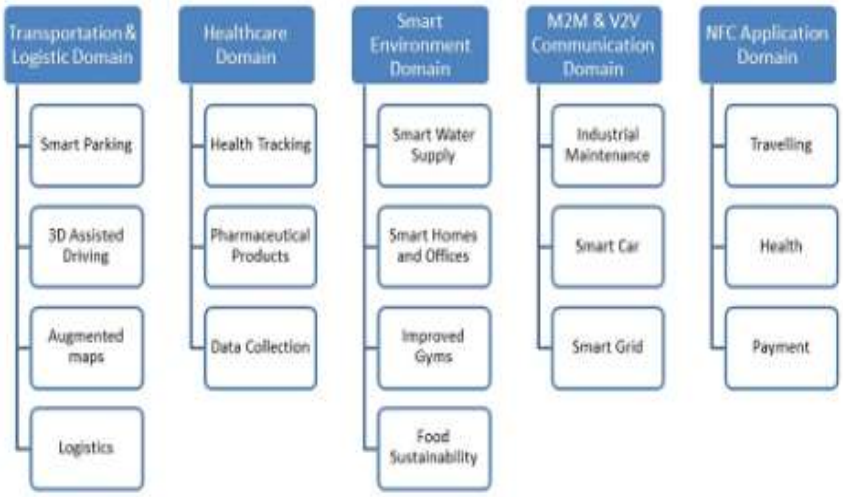

Fig. 2 Aplicações para IoT. [1]

- Medicina: A IoT pode melhorar consideravelmente a qualidade de vida do número cada vez maior de idosos. Por exemplo, imagine um dispositivo pequeno e utilizável que pode detectar os sinais vitais de uma pessoa e enviar um alerta para um profissional de saúde quando atingir determinado limite ou sentir quando uma pessoa cair e não conseguir se levantar [10].
- Ambientais: Há dispositivos que coletam informações do tempo, como temperatura, riscos de tsunamis entre outras e disponibiliza para agencias responsáveis por esses dados. Em caso de cidades, o monitoramento, do vazamento de água, por exemplo, com a utilização de sensores, pode evitar a

perda da água, detectando vazamentos indevidos, corrigindo o problema, no local exato [7].

- Domésticos: A geladeira inteligente, pode utilizar tags de RFID, para se comunicar e dizer se precisa comprar algum item ou não, tornando – se um frigorífico inteligente. São muitos os eletrodomésticos, que faz parte de uma residência ou uma empresa, com isso sensores e atuadores instalados, proporciona maior flexibilidade ao cotidiano das pessoas, quando os mesmos estão conectados, podem medir o consumo de energia da residência, desligando o que não está em uso, ou até mesmo resfriando ou aquecendo o ambiente quando necessário, proporcionando economia e conforto a vida das pessoas [1][7].
- Pecuária: Dispositivos RFID são utilizados para rastrear o gado, e assim detectar possíveis doenças e regiões, dessa maneira sabe a origem da carne, uma maneira mais simples de escolher entre consumir ou não aquele alimento. Atualmente tem empresas de fornecimento de carnes, os fazendeiros, que utilizam um rastreador na orelha do gado, monitorando seus movimentos, origem e saúde, dessa maneira agrega valor à carne vendida, pois garante conhecimento sobre o produto consumido [10].

VI. SEGURANÇA EM IOT

Internet das Coisas um terno novo, com inúmeras aplicações, mas ainda com restrições, entre elas, segurança da informação, afinal um meio interconectado, pode gerar inúmeros riscos relacionados a privacidade do cliente, integridade dos dados, controles de acesso, capacidade a resistência a ataques, entre outros. Alguns dos problemas relados acima estão ligados a falta de padronização quanto a arquitetura utilizada para IoT [12]

Segurança em IoT é algo crítico para essa tecnologia, afinal garantir a confidencialidade, integridade e disponibilidade em objetos interligados, trocando informações a todo momento, com dispositivos de tamanho reduzido e grande consumo de energia, soluções de segurança é um desafio para Internet das Coisas alavancar, como pode ser visto na figura abaixo [9].

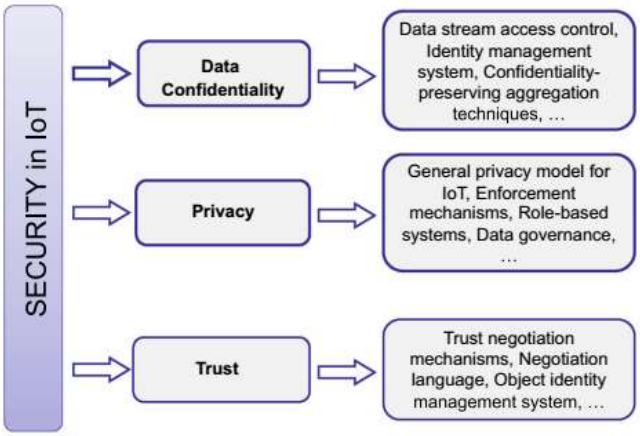

Fig. 3- Representação gráfica de desafios de segurança no Internet - de -Things. [1]

Resumidamente segurança da informação utiliza de princípios básicos que são descritos abaixo, segundo a ISO/IEC 27001:2006.

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. Sendo assim a informação precisa ser tratada adequadamente [4].
- Integridade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidade ou processo autorizado. A mesmo pode estar relacionada a erro humano, intencional ou não [4].
- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada. Aplica-se não somente a informação, mas também ao canal eletrônico onde a informação se encontra disponível [4].

Com isso é indispensável um controle de acesso as informações, garantido a confidencialidade e a integridade. Assim como a presença de um método de autenticação do objeto, para certificar que o autor da transmissão da mensagem é quem diz ser. Fatores esses citados também relacionados à segurança da informação [9].

Há grandes ameaças à segurança da informação, uma vez que os dispositivos estão ligados a meios físicos, por exemplo, um acesso indevido a um objeto responsável por monitoramento a um alerta de tsunami, esses dados devem estar acessíveis apenas aos órgãos responsáveis por tomar determinadas providencias [1][9].

A privacidade é uma questão de segurança a qual chama muita atenção, pois com informações trafegando em meio sem fio, aumento o risco de ataques e violação da mesma, imagine dados relacionados a saúde, que são sensíveis aquela determinada pessoa e empresa [1].

A criptografia é a principal ferramenta para segurança, com ela é possível proteger os pilares de segurança da informação, exceto a disponibilidade. Criptografia é a forma de transformar algo legível em algo ilegível para pessoas não autorizadas.

Tradicionalmente a criptografia é separada em simétrica e assimétrica, como pode ser visto nas definições abaixo as principais diferenças, segundo [13]:

- Simétrica: é caracterizada por um único segredo, onde a mesma chave que é utilizada para criptografar é utilizada para descriptografar os dados, principal vantagem é rápida e a desvantagem é que a mesma precisa ser transportada para o destinatário.
- Assimétrica: enquanto a criptografia simétrica utilizava uma única chave à assimétrica utiliza duas chaves uma pública, a qual é distribuída aos membros da rede e a privada é mantida em segredo pelo nó. A desvantagem desse método é o gasto computacional que é bem maior em relação a simétrica, mas o método é mais seguro pois não é preciso passar a chave ao destinatário.

VII. PROPOSTA DE PROTOCOLOS PARA IOT

Para utilização das aplicações IoT é necessário a padronização dos protocolos de redes, passando pelas diversas camadas do modelo híbrido, alguns protocolos foram adaptados para Internet das Coisas. Como pode ser visto na Tabela 1 as camadas de redes e alguns protocolos para aplicações na internet [5].

Tabela I. Pilha de protocolos

Aplicação – HTTP
Transporte TCP/UDP
Rede /IP – IPV4

Enlace
Física

A Tabela 2 propõe alguns protocolos adaptados para IoT, passando pelas camadas de redes, de modelo já existente no mercado. Os quais serão descritos nas próximas seções.

Tabela II. Pilhas protocolos para aplicações IoT

Camada	**Protocolos**
Aplicação	**CoAP**
Adaptação	**DTLS**
Transporte	UDP
Rede /IP-	IPv6/RPL
Adaptação	**6LowPAN**
Enlace	IEEE 802.15.4
Física	

A. IPV6 over Low power Wireless Personal Area Network (6LowPAN)

Com as características e limitações presentes nas aplicações IoT, como capacidade de energia reduzida e possibilidade de abundância de dispositivos conectados, fez-se necessária a adoção de um padrão que onerasse pouco a camada física em energia e processamento, além da adoção da tecnologia principal da internet de próxima geração [14].

Dentre as características do padrão 6LowPAN estão tamanhos de pacote pequenos, de 127 bytes, sendo 81 bytes disponíveis para dados; Taxas de transferência baixas com velocidades de 250kbps, 40kbps, e 20kbps para cada uma das camadas físicas definidas; Baixo consumo de energia, sendo facilmente adotável por dispositivos alimentados a bateria [15]

Uma grande vantagem da adoção do IPV6 na tecnologia 6LowPAN é a gigantesca disponibilidade de endereços. Com aproximadamente 3.4×10^33 endereços, teríamos mais de 6.67*10^27 endereços por metro quadrado em nosso planeta, o que supriria a demanda para aplicações de larga escala e alta densidade [14].

Devido a características das aplicações IoT, uma importante característica do 6LowPAN, é de autoconfiguração do IPV6, trabalha com roteamento na camada de redes e auxilia a camada de enlace. Sendo assim esse protocolo de adaptação entre camada de redes e enlace, comprime o cabeçalho para utilização desses protocolos [16].

O padrão 6LowPAN não define formas de compressão para cargas de UDP, ou das camadas acima. No entanto, foi proposto um plug-in para o padrão, chamado 6LowPAN-GHC, que seria usado para comprimir cargas UDP. Seria usado um bit de identificação no cabeçalho NHC (Next Header Compression) que indicaria se a carga está comprimida. As taxas de compressão com esta técnica podem chegar a 75% [16].

Uma preocupação que nasce com a adoção do 6LowPAN é a de segurança e privacidade. A maior parte dos protocolos de endereçamento IPV6 assume que o endereço dos nós não se altera por toda permanência do nó na rede. Mesmo que se utilize de formas de criptografia nos pacotes enviados, é possível que algum dispositivo que intercepte os pacotes leia os endereços e obtenha informações como quando um usuário está ativo, ou quando ele utiliza determinado produto. Como os endereços de IP são dados indispensáveis e não podem ser facilmente escondidos de um interceptador, uma abordagem possível para este problema é o uso de endereços de IP dinamicamente modificados. Propõe-se o reendereçamento aleatório dos nós periodicamente. Dois possíveis esquemas para o reendereçamento são propostos: Descentralizado, onde todos os nodes são responsáveis pelo reendereçamento, e mantém unicidade de endereço através de uma técnica chamada DAD (Duplicate Address Detection, ou Detecção de Endereço Duplicado), e centralizado, onde um servidor é responsável pela execução do algoritmo de reendereçamento remoto para todos os nodes. A abordagem descentralizada tende a ser menos performática [17].

Outro problema que emerge é o da mobilidade. Dispositivos devem conseguir manter seu endereçamento enquanto muda de PAN (Personal Area Network, ou Rede de Área Pessoal). O protocolo IPV6 possui vários modelos para tratamento deste problema, como HMIPv6, FMPIv6 e MIPv6, que são baseadas em tunelamento. No entanto, estas soluções não se adéquam às características de baixo consumo e processamento inerentes ao 6LowPAN por conta de exigirem numerosos envios e recebimentos de informações de controle. Uma possível abordagem para a solução deste problema é a

adoção de ‘nós de gateway’, que seriam responsáveis por coordenar a transição entre redes PAN [15].

B. CoAP

Atualmente diversos serviços web operam utilizando infraestrutura REST. Com o intuito de permitir que dispositivos com limitações de processamento, memória, armazenamento e energia possam se utilizar dessa infraestrutura surgiu o protocolo CoAP (Constrained Application Protocol) [18].

O CoAP herda muitas funcionalidades e características do protocolo HTTP. Assim como o HTTP ele implementa a estrutura de RESTful de cliente e servidor, juntamente com os métodos GET, PUT, POST e DELETE e as respostas 2.xx, 4.xx, 5.xx. Porém existem duas principais diferenças entre o HTTP e o CoAP: o HTTP é unidirecional, suportando apenas chamadas via cliente e o CoAP suporta comunicação bidirecional; o HTTP utiliza como protocolo de transporte o TCP, provendo maior confiabilidade, o CoAP utiliza como transporte o UDP de forma a reduzir o tamanho de pacotes e dados transmitidos [19] [20].

O protocolo CoAP é útil para a comunicação entre nós que o utilizem, mas alcança o seu potencial completo ao se comunicar entre nós que utilizem tanto o CoAP quanto HTTP, através de intermediários é possível fazer essa conversão, de acordo com a terminologia REST utilizando PROXY. Como ambos os protocolos têm estruturas e comportamentos semelhantes essa tradução pode ser feita, praticamente, de forma estática [20].

Para atender alguns requisitos de uma rede IoT e suas limitações foram implementadas algumas funcionalidades. O CoAP funciona bem para pequenas mensagens, porém em algumas situações, como atualizações de firmware, é necessário a transferência de grande volume de dados, para não depender apenas da fragmentação do IP o CoAP implementa uma opção “Block” habilitando o servidor de manipular múltiplas requisições separadamente sem a necessidade de configurar uma conexão ou configurações adicionais. Para economizar energia e recursos, diferente do HTTP o CoAP pode receber chamadas do servidor a partir de chamadas assíncronas com a opção “Observe”, evitando ficar recursivamente verificando o

estado do servidor. Um protocolo bem definido e funcional o CoAP se propõe a se tornar um protocolo de aplicação padrão para IoT [20].

VIII. PROTOCOLOS DE SEGURANÇA

A. TLS

O Transport Layer Security (TLS) oferece uma implementação de segurança para proteger a camada de transporte em aplicações HTTP que utilizem o protocolo TCP [21].

Fornecendo privacidade e integridade dos dados entre a comunicação entre aplicações. O protocolo é composto principalmente pelo: TLS Record Protocol e TLS Handshake Protocol, fornecendo suporte para o encapsulamento de vários protocolos de nível superior e permitindo que cliente e servidor negociem o algoritmo e as chaves de criptografia antes de estabelecer a conexão, respectivamente [22].

Dada essas propriedades a natureza de uma conexão TCP passa a ter confiabilidade entre os dados enviados e recebidos. Esta confiabilidade adiciona certa sobrecarga adicional na comunicação TLS, como identificação para cada mensagem enviada e mensagens adicionais assegurando a fidelidade dos dados [22].

B. DTLS

O Datagram Transport Layer Security (DTLS) tem origem no TLS herdando algumas de suas características e permitindo aproveitar funções de segurança para aplicações que implementem comunicação UDP. Como o principal protocolo para aplicações IoT, o CoAP, utiliza o UDP como camada de transporte o DTLS é o protocolo recomendado para aplicações IoT [21].

Esse protocolo é designado para prover segurança dos dados transmitidos entre comunicação de aplicações sobre o protocolo UDP em nível de aplicação de forma que não seja necessária nenhuma modificação de kernel. Fornecendo as mesmas funcionalidades do TLS sobre transporte de datagramas [23].

VII. CONCLUSÃO

Ao analisar a evolução da internet, passando por protocolos de redes, que nos dias atuais estão passando por adaptações para compor a um mundo com objetos interconectado, e possibilitar um avanço em diversas áreas, como foi visto na pesquisa.

A qual trata das dificuldades da implementação da Internet das Coisas, devido suas características, entre elas a implantação de segurança da informação em suas conexões e interligações. Sendo explicado a existência de protocolos de redes que podem proporcionar segurança aos dados, passando pelas camadas de redes. O protocolo DTLS, exposto como o principal objetivo da pesquisa tem características que agregam e ajudam a melhorar a segurança da informação das aplicações para IoT.

Ambiente inteligentes, proporcionados pelo avança da tecnologia, irão disponibilizar novas oportunidades de negócio, tratar problemas ambientais, possibilitar maior segurança, avanços na medicina, entre outros. Ou seja, seria promissor para diversas áreas. Mas, para que essas oportunidades sejam implantadas, é preciso tratar as questões de segurança da informação, assim como as Leis atuais voltadas para a tecnologia deverá atender a todo um cenário inteligente e programado.

REFERENCIAS

[1] D. Miorandi, et al. “Internet of things: Vision, applications and research challenges" in Ad Hoc Networks, vol. 10, p1497–1516, 2012.

[2] V.H.P. Cardoso, R.F. Fernandes, A.L. Dias, G.S. Sestito, D. Brandão. “Aplicação Da Tecnologia De Internet Das Coisas Na Medição De Consumo”, USP, São Paulo.

[3] P.L. Tavares. “Redes de Sensores Sem – fio”, Universidade Federal do Rio de janeiro, p. 9-12, 2002.

[4] ABNT, NBR ISO/IEC 27001. “Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos”. ABNT, 2006.

[5] A.S. Tanembaum. “Computer Network”, 4 ed, p.404-412, Agosto 2002

[6] R. Fisher, G. Hancke. "DTLS for Lightweight Secure Data Streaming in the Internet of Things" in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on , p.585-590, 8-10 Novembro 2014.

[7] S. Agrawal, D. Vieira. “A survey on Internet of Things”, Minas Gerais, 2013.

[8] T.C. França, et al. “Web das Coisas: Conectando Dispositivos Físicos ao Mundo Digital”, Rio de Janeiro, 2011.

[9] L. Atzori, A. Iera, G. Morabito. “The Internet of Things: A survey” in Computer Networks vol. 54, 2010.

[10] FRANÇA, Tiago C, et al. Web das Coisas: Conectando Dispositivos Físicos ao Mundo Digital. Rio de Janeiro, 2011.

[11] D. Evans. “A Internet das Coisas Como a próxima evolução da Internet está mudando tudo.” Cisco Internet Business Solutions Group (IBSG) – 2011.

[12] W.M. Paes. “Interoperabilidade Móvel: A Internet das Coisas”, p806, São Paulo, 2014.

[13] R. Weber, H. “Internet of Things – New security and privacy challenges” 26, 2010.

[14] N.C. Fernandes. “Ataques e Mecanismos de Segurança em Redes Ad Hoc”, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

[15] Xin Ma, Wei Luo, "The Analysis of 6LowPAN Technology," in Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on , vol.1, p.963-966, 19-20 Dezembro 2008.

[16] Xiaonan Wang, Shan Zhong, Rong Zhou, “A mobility support scheme for 6LoWPAN”, Computer Communications, vol 35, p. 392-404, 1 February 2012.

[17] S. Raza, et al. “6LoWPAN Compressed DTLS for CoAP”. IEEE International Conference, pag 287, 2012.

[18] Xiaonan Wang, Yi Mu, "Addressing and Privacy Support for 6LoWPAN," in Sensors Journal, IEEE , vol.15, no.9, p.5193-5201, Setembro 2015.

[19] Z. Shelby, et. al. “The Constrained Application Protocol (CoAP)”, RFC 7252, Junho 2014.

[20] Giang, N.K., Minkeun Ha, Daeyoung Kim, "SCoAP: An integration of CoAP protocol with web-based application," in Global Communications Conference (GLOBECOM), 2013 IEEE , pp.2648-2653, 9-13 Dezembro 2013.

[21] Bormann, C., Castellani, A.P., Shelby, Z. "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," in Internet Computing, IEEE , vol.16, no.2, pp.62-67, Março 2012.

[22] V. Lakkundi, K. Singh, K. "Lightweight DTLS implementation in CoAP-based Internet of Things" in Advanced Computing and Communications (ADCOM), 2014 20th Annual International Conference on , p.7-11, 19-22 Setembro 2014.

[23] T. Dierks, E. Rescorla, RTFM, Inc. “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, Agosto 2008.

[24] E. Rescorla, RTFM, Inc., N. Modadugu, Google, Inc. “Datagram Transport Layer Security Version 1.2”, RFC 6347, Janeiro 2012.