Evento: XXVII Seminário de Iniciação Científica

INTERNET DAS COISAS E OBJETOS INTELIGENTES: UMA BREVE ANALISE DA SUA HISTÓRIA, ESTRUTURA E SEGURANÇA[1]
INTERNET OF THINGS AND SMART OBJECTS: A BRIEF ANALYSIS INTO YOUR HISTORY, STRUCTURE AND SECURITY.

Gabriel Henrique Danielsson[2], Mauro Fonseca Rodrigues[3]

[1] Pesquisa realizada na disciplina de Telecomunicações e Redes de Computadores do curso de Engenharia Elétrica
[2] Aluno do curso de Engenharia Elétrica da Unijuí, gabriel.danielsson@gmail.com
[3] Professor Mestre do curso de Engenharia Elétrica da Unijuí, coordenador das Engenharias da Unijuí Campus Santa Rosa, orientador, mauro.rodrigues@unijui.edu.br

INTRODUÇÃO

Este artigo tem como objeto de estudo a Internet das Coisas, abordando sua definição, história, a estrutura básica dos objetos inteligentes, protocolos de comunicação utilizados e um panorama geral da segurança envolvendo essa tecnologia.

Após a World Wide Web (década de 1990) e da Internet móvel (década de 2000), estamos andando para a terceira e potencialmente mais "perturbadora" fase da revolução da Internet - a "Internet das Coisas". A Internet das Coisas conecta os objetos do mundo real com o mundo virtual, possibilitando a qualquer momento, em qualquer lugar, conectividade para qualquer coisa e não apenas para qualquer individuo (Sundmaeker, Guillemin, Friess, & Woelfflé, 2010).

METODOLOGIA

A metodologia deste trabalho foi organizada através de uma revisão bibliográfica na área de Internet das Coisas e objetos inteligentes, analisando o assunto de forma integral, abordando sua historia, estrutura básica de objetos inteligentes, protocolos de comunicação e um panorama geral da segurança que abrange essa tecnologia. Assim obtemos uma base para estudos posteriores nessa área.

RESULTADOS E DISCUSSÃO

Definição e história da IoT

A Internet das Coisas, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do cotidiano, mas com capacidade computacional e de comunicação, se conectarem à Internet (Santos, Silva, Celes, Neto, & Peres, 2016). A IoT é a modernização dos equipamentos eletrônicos que possuimos dentro de casa, por exemplo: *Smart*TVs, *Smart Fridges, Smart bulbs,* etc.

O termo IoT surgiu pela primeira vez em 2009, por Kevin Asthon, na época o termo era associado ao uso da tecnologia RFID (Ashton, 2009). Em 2012, foi previsto que a IoT levaria entre cinco e dez anos para ser adotada pelo mercado, e hoje em dia é experienciado o maior pico de expectativas sobre a tecnologia no âmbito acadêmico e industrial(Santos, Silva, Celes, Neto, & Peres, 2016). Assim, a IoT vem ganhando cada vez mais espaço dentro das universidades como objeto de pesquisa e dentro de indústrias, comprovando sua importância no presente e futuro das organizações e individuos.

Assim essa tecnologia se torna presente no nosso cotidiano de forma intrísica, criando ambientes onde há troca de informações em tempo real, auxiliando na monitoração de ambientes para diversos tipos de serviços, no caso da IoT em ambientes residenciais é melhorar a qualidade de vida dos moradores.

Estrutura básica dos objetos inteligentes

A arquitetura básica de objetos inteligentes é constituida por quatro unidades: processamento/memória, comunicação, energia e sensores/atuadores, conforme figura 1.

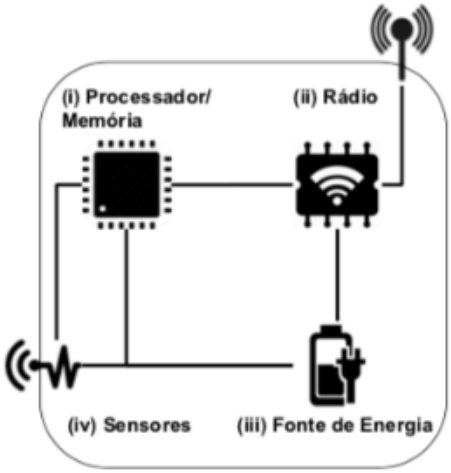

Figura 1: Arquitetura básica de objetos inteligentes (Santos, Silva, Celes, Neto, & Peres, 2016)

Conforme (Santos, Silva, Celes, Neto, & Peres, 2016):

Unidade de processamento/memória:composta de uma memória interna para armazenamento de dados e programas, um micro controlador e um conversor analógico-digital para receber sinais dos sensores. As CPUs utilizadas nesses dispositivos são geralmente as mesmas utilizadas em sistemas embarcados e não apresentam alto poder computacional. Normalmente existe uma memória externa do tipo flash, que serve como memória secundária, por exemplo, para mantém um “log” de dados. As características buscadas para estas unidades são: baixo consumo de energia e tamanho reduzido.

Unidade de comunicação:consiste de no mínimo um canal de comunicação com ou sem fio. No caso de comunicação sem fio, a maioria das plataformas usam rádio de baixo custo e baixa potência. Como consequência, a comunicação é de curto alcance e apresentam perdas frequentes.

Fonte de energia:responsável por fornecer energia aos componentes. A fonte de energia consiste de uma bateria e um conversor AC-DC e tem a função de alimentar os componentes.

Unidade de sensor/atuador: realizam o monitoramento do ambiente onde o objeto inteligente esta posicionado. Os sensores capturam valores de grandezas físicas (temperatura, umidade, pressão e presença). Atuadores, são dispositivos que produzem alguma ação, atendendo a comandos que podem ser manuais, elétricos ou mecânicos.

Tecnologias de Comunicação

Para entendermos melhor como funciona a troca de informações entre objetos inteligentes, necessitamos compreender como funcionam as Tecnologias de Comunicação, nesse caso iremos adentrar apenas as tecnologias Ethernet e Wi-Fi. Conforme (Santos, Silva, Celes, Neto, & Peres, 2016):

Ethernet- O padrão Ethernet (IEEE 802.3) foi oficializado em 1983 pelo IEEE e está presente em grande parte das redes locais com fio existentes atualmente. Sua popularidade se deve à simplicidade, facilidade de adaptação, manutenção e custo. Atualmente, existem dois tipos de cabos: par trançado e fibra óptica, que oferecem taxas de comunicação diferentes. Os cabos de par trançado podem atingir taxas de até 1 Gbps, limitados a 100 m. Os cabos de fibra ótica alcançam taxas de 10 Gbps,

Wi-Fi- A tecnologia Wi-Fi é uma solução de comunicação sem fio bastante popular, pois está presente nos mais diversos lugares, fazendo parte do cotidiano de casas, escritórios, indústrias, lojas comerciais e até espaços públicos das cidades. O padrão IEEE 802.11 (Wi-Fi1) define um conjunto de padrões de transmissão e codificação. Desde o seu lança- mento em 1997, já foram propostas novas versões do padrão IEEE 802.11 e, a versão IEEE 802.11ac prevê taxas de comunicação de 600 Mbps ou 1300 Mbps.

Para comparar melhor as características entre as tecnologias de comunicação, a tabela 1 a seguir:

Protocolo	Alcance	Frequência	Taxa	IPV6	Topologia
Ethernet	100-2000 metros	N/A	10 Gbps	Sim	Variada
Wi-Fi	50 metros	2.4/5 GHz	1300 Mbps	Sim	Estrela
3G/4G	35-200 km	1900/2100/2500 MHz	1-10 Mbps	Sim	Estrela

Tabela 1: Comparações entre as tecnologias de comunicação, adaptado de (Santos, Silva, Celes, Neto, & Peres, 2016)

Assim, dispomos das principais informações necessárias de cada tecnologia, possibilitando fazer a melhor escolha de comunicação de acordo com a necessidade de cada projeto a ser implementado.

Segurança na IoT

Com o avanço e popularização de objetos inteligentes, aparecem as preocupações com segurança e privacidade, uma vez que esses objetos inteligentes estão sendo utilizados em indústrias e residências. Afim de evitar essa resistência, precisamos explorar suas características para encontrar erros/falhas com o objetivo de tornar esses equipamentos mais seguros.

A Internet das Coisas precisa ser construída de forma a garantir um controle de usuário fácil e seguro. Os consumidores precisam de confiança para abraçar totalmente a tecnologia, a fim de aproveitar os seus benefícios e evitar riscos à sua segurança e privacidade (Sundmaeker, Guillemin, Friess, & Woelfflé, 2010).

Segurança para IoT engloba uma ampla gama de tarefas, incluindo incorporação de material de chaves durante o processo de fabricação do dispositivo, provisionamento de novo material de

chaves durante a operação, estabelecimento de políticas de controle de acesso para redes e serviços, processos para desenvolvimento de software de módulos de segurança de hardware para proteger chaves contra adulteração, gerenciamento de atualização de software e desenvolvimento e seleção de primitivas criptográficas eficientes. As soluções de segurança personalizadas oferecidas pela comunidade de pesquisa de IoT oferecem principalmente soluções pontuais, mas isso raramente ajuda a entender o panorama geral da proteção de dispositivos IoT**.**(Keoh, Kumar, & Tschofenig, 2014)

Tornando a IoT segura começa antes que as peças sejam colocadas no lugar. Começa durante o processo de seleção de equipamentos e softwares. Claramente, é importante selecionar equipamentos e software com segurança interna. (Narang, Nalwa, Choudhury, & Kashyap, 2018)

Na próxima seção será abordado dois métodos para segurança dos objetos inteligentes.

Modelo de encriptação hibrida

Conforme (Narang, Nalwa, Choudhury, & Kashyap, 2018)a técnica de criptografia híbrida é um modelo que pode ser usado para oferecer confiabilidade e confidencialidade das informações na troca de dados da IoT.

Passos para criptografia de *smart home* são:

1 – O usuário ou o residente da casa tem a chave publica que é gerada pela criptografia síncrona.

2 – As mensagens para serem criptografadas são enviadas para o algoritmo assíncrono pela chave pública.

3 – Então, a mensagem é criptografada pelo algoritmo de criptografia assíncrona e é enviada para o receptor na internet do ambiente.

4 – Os objetos inteligentes (*smart frigdes, smart bulbs*, etc) também possuem uma chave privada e o usuário não a conhece.

5 – Por causa da chave privada, os hackers não conseguem adivinhar as senhas dos objetos inteligentes. Consequentemente a segurança dos objetos é mudada.

Esse modelo prove segurança e aumenta a velocidade de criptografia e descriptografia ao gerar uma chave, assim utilizam também menos memoria dos objetos inteligentes.

Proteção contra *spoofing* de IP

O *spoofing*de IP (falsificação de IP), envolve a inundação de pacotes IP por usuários não autorizados, replicando o endereço de origem de usuários autorizados. Os roteadores examinam apenas o endereço IP de destino e o endereço de origem geralmente não é validado. Nesse caso, da falsificação de IP, o destino não tem conhecimento de quem é o usuário real e quando envia os pacotes de volta ao endereço IP de origem e o usuário real não receberá os dados esperados. (Rajashree, S, & Shah, 2018) No método proposto por (Rajashree, S, & Shah, 2018)o *gateway* mantém um pool de endereços IP que podem ser atribuídos ao objeto inteligente sob demanda, conforme figura 2.

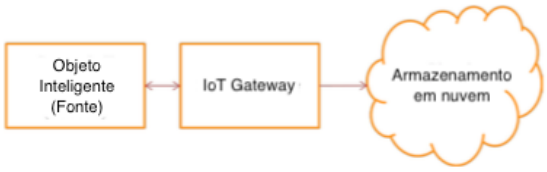

Figura 2: Comunicação do IP entre o objeto inteligente e o *Gateway,* adaptado de (Rajashree, S, & Shah, 2018)

Nesse método, assumimos que:
1 – Há uma comunicação IP entre o objeto inteligente e o*Gateway*em uma mídia física Ethernet.
2 – Tanto o dispositivo quanto o *gateway*recebem endereços MAC exclusivos.
3 – O objeto inteligente é capaz de lidar com pacotes IP *Multicast.*
Este método propõe modificações na pilha IP(IP stack) para suportar a troca de mensagens. O uso de protocolos como um DHCP para atribuição de endereços IP dinâmicos e configuração de filtros (listas de controle de acesso) para falsificação de IP é evitado. Este método evita o uso de esquemas criptográficos complexos para autenticação de pacotes. (Rajashree, S, & Shah, 2018)

CONSIDERAÇÕES FINAIS

A Internet das Coisas é um marco para o avanço tecnológico e possui uma enorme expectativa positiva para o futuro, assim é objeto de estudo de varias empresas e universidades ao redor do mundo.
O presente artigo forneceu uma gama de conteúdo sobre a Internet das Coisas, trazendo um panorama geral de como ela é composta em sua totalidade, além de abordar dois métodos para aumentarmos a segurança dos objetos inteligentes. Com isso, possuímos uma ótima revisão bibliográfica para continuar o estudo na área de Internet das Coisas e futuramente fazer uma correlação com as Cidades Inteligentes.

Palavras-chave: Telecomunicações; TPC/IP; IoT.
Key-words: Telecommunications; TPC/IP; IoT.

REFERÊNCIAS

Ashton, K. (2009). That 'internet of things' thing. *RFiD Journal*.
Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the Internet of Things: A Standardization Perspective. *IEEE INTERNET OF THINGS JOURNAL, 1*(3).
Narang, S., Nalwa, T., Choudhury, T., & Kashyap, N. (2018). An efficient method for security measurement in internet of things. *International Conference on Communication, Computing and Internet of Things (IC3IoT)*.
Rajashree, S., S, S. K., & Shah, P. G. (2018). Security with IP Address Assignment and Spoofing for Smart IOT Devices.
Santos, B. P., Silva, L. A., Celes, C. S., Neto, J. B., & Peres, B. S. (2016). Internet das Coisas: da Teoria à Prática.
Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). *Vision and Challenges for Realising the Internet of Things.*