Estudo sobre a Segurança e Privacidade na Comunicação de Dispositivos IoT

Mariana Liberato de Abreu
Instituto Nacional de Telecomunicações - INATEL
marianaliberato@gea.inatel.br

Rafael Liberato Jóia
Instituto Nacional de Telecomunicações - INATEL
rafael.liberato@inatel.br

***Resumo* – Assim como nenhuma rede está totalmente segura, dispositivos que utilizam *IoT*, Internet das Coisas, sofrem ataques assim como qualquer outro tipo de rede. O objetivo deste artigo é mostrar os principais ataques frequentes conjuntamente com alguns tipos de protocolos e meios de comunicação que o *IoT* faz com qualquer dispositivo. No final, mostrando a importância da segurança dos dados e, como mantê-los seguros na rede.**

***Palavras-chave*: Ataques, IoT, Segurança, Protocolos.**

***Abstract*- Just as no network is fully secure, devices that use IoT, Internet of Things, suffer attacks just like any other type of network. The purpose of this article is to show the main frequent attacks together with some types of protocols and means of communication that IoT does with any device. In the end, showing the importance of data security and how to keep them safe in the network.**

Keyswords: Attacks, IoT, Security,Protocols

I. INTRODUÇÃO

A Internet das Coisas *(IoT)*, representa a hiperconexão entre qualquer objeto por meio de sensores e *softwares* transmitindo dados para a rede, possibilitando a comunicação entre pessoas e objetos físicos. Com o seu crescimento exponencial, algumas em empresas já aderiram soluções em diversos setores.

Em um ecossistema que se utiliza a Internet das Coisas, um ponto de alta relevância é a segurança da informação no processo [1], uma falha na segurança da comunicação entre os dispositivos *IoT* pode acarretar riscos no mundo real.

Essa pesquisa tem como objetivo mostrar os principais protocolos de rede, os tipos de comunicações e como eles fazem essa troca de informação conjuntamente apresentar algumas vulnerabilidades que estas redes sofrem.

II. PROTOCOLOS DE REDE

Ao implementar alguma tecnologia, o processo de camadas de segurança é imprescindível. A escolha de protocolos de utilização para as "coisas" se difere do HTTP utilizado para os PC'S, pois possuem poder computacional restrito limitando o uso desse protocolo. Para recuperar informações e resolver esse problema, foram desenvolvidos dois protocolos para dispositivos com baixo poder computacional: CoAP e MQTT.

A. MQTT

O MQTT *(Message Queue Telemetry Transport)* é um protocolo projetado para dispositivos extremamente limitados e utiliza a estratégia de *publish/subscribe* para transferir mensagens entre *devices*. Esse protocolo se baseia em três componentes: *subscriber*, *publisher* e *broker*. Inicialmente, dispositivos se registram (*subscribe*) a um *broker* para obter informações sobre dados específicos, para que o *broker* os avise sempre que publicadores (*publishers*) publicarem os dados de interesse. O intuito desse protocolo é minimizar o uso da banda larga da rede e recursos dos dispositivos. Além disso, esse protocolo provê mecanismos para a garantia de entrega de mensagens. Utilizando os protocolos das camadas de transporte e rede da arquitetura TCP/IP, o seu cabeçalho pode ter tamanho fixo (dois bytes) ou variável. Um exemplo de uma implementação *open source* do MQTT é o Mosquitto20.

B. CoAP

A CoAP (*Constrained Application Protocol)* define uma forma de transferir dados assim como é feito através do *Representational State Transfer* (REST) utilizando funcionalidades similares ao do HTTP tais como: GET, DELETE, PUT, POST.

O modelo de arquitetura REST permite que clientes e servidores acessem ou consumam serviços *Web* de maneira prática usando *Uniform Resource Identifiers* (URIs). O CoAP se diferencia do REST por utilizar o protocolo UDP, que o coloca como mais adequado para aplicações em IoT,

pois não ocorre a confirmação do recebimento do pacote de dados.

Dispositivos conectados à *Internet* precisam de um meio de comunicação, para isso, existem quatro tipos de modelos para a comunicação: *Device-to-device, Device-to-cloud, Device-to-Gateway, Back-End Data Sharing.*

A. Device-to-device

Esse padrão é a conexão de dois ou mais dispositivos que, conectam em si e se comunicam sem o uso da *Internet*, conforme representado pela figura[1], que mostra um celular conectado à cafeteira via *Bluetooth* podendo o usuário escolher o tipo de café e a quantidade de açúcar desejada.

Fig. 1. Modelo *Device-to-Device.*
Fonte:https://www.embarcados.com.br/modelos-de-comunicacao-para-iot/

B. Device-to-cloud

Essa comunicação é feita entre o dispositivo *IoT* com um provedor remoto na nuvem, em outras palavras, é todo dado gerado e enviado via *Internet*, sem precisar de um equipamento para o servidor, que será responsável por toda a parte de análise e processamento de dados, para em seguida disponibilizar o usuário. Para ter comunicação dos serviços que o servidor faz precisa de protocolos que é o *Message Queue Telemetry Transport.*

C. Device-to-Gateway

Essa comunicação possibilita a interação entre diferentes tipos de redes. Seu funcionamento é bastante simples os pacotes adaptados e originários de uma rede 1 enviam para uma rede 2 o formato correto dos seus respectivos dispositivos. Um exemplo para isso que vem se popularizando são as pulseiras que monitoram exercícios físicos. No caso da figura [2] as redes são *Bluetooth* e o LTE. Todas as informações e dados são enviados pela *Wi-fi*. Como a pulseira não possui um IP e assim não estando conectada na *Wi-fi* ela precisará de um *Gateway* para fazer toda a troca de dados.

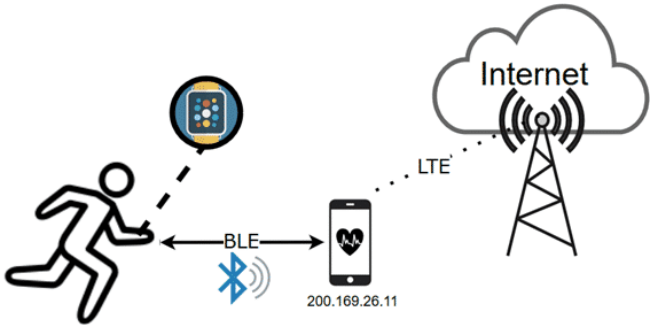

Fig. 2. Modelo *Device -to-Gateway*
Fonte:https://www.embarcados.com.br/modelos-de-comunicacao-para-iot

D. Back-End Data Sharing

O *Back-End Data Sharing* é a possível combinação e analise de diferentes bancos de dados e servidores. É a combinação sobre informações, como por exemplo, do clima, trânsito e agricultura.

Tudo será tão automático que o usuário não irá notar as tomadas de decisão executadas por máquinas a sua volta. A figura [3] mostra sensores medindo as características do solo e, todo dado coletado é enviado a um sensor "A" onde toda a aplicação inteligente é executada. No servidor, os dados são analisados, processados e enviados para o usuário final em forma de resposta. Para aumentar a precisão do resultado final ao usuário, o sensor "A" se comunica com os sensores "B" e "C", unindo informações relevantes ao clima do tempo para saber as características de cada tipo de plantio, dados sobre a melhor data para colheita ou o comando automatizado de máquinas para realizarem a colheita.

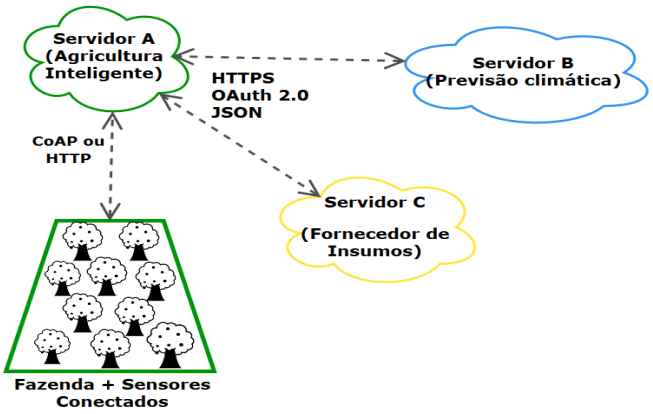

Fig. 3. Modelo *Back-End Sharing*.

Fonte: https://www.embarcados.com.br/modelos-de-comunicacao-para-iot/

III.SEGURANÇA NA REDE

Com o avanço das “coisas” a previsão de dispositivos conectados deve chegar até 20,4 bilhões em 2020[2]. Este progresso garante o conforto nas atividades do cotidiano como as *smart tv's*, sistemas eletrônicos de pagamentos, *smartwatches*, câmeras de segurança, como também no setor de lavoura em tempo real.

Com todo o conforto que o *IoT* traz para o dia a dia sua comunicação deve ser mantida de forma segura para não haver qualquer tipo de roubo as informações. Como a forma de comunicação é feita através do modo público e quanto mais dispositivos estiverem conectados à rede o risco de roubo de dados é grande para o usuário, por isso deve-se preocupar com as falhas de segurança que passam despercebidos pela a indústria.

Existem várias maneiras de burlar o sistema de segurança dos dispositivos, algumas são: o acesso ilegal, rede corporativa e a infraestrutura da nuvem.

Para se manter seguro na rede uma das medidas básicas a serem tomadas é a atualização regularmente, pois dispositivos desatualizados representam vulnerabilidades fáceis para *hackers.* Outras medidas preventivas, seria fazer *backups* e criar senhas difíceis para serem descobertas. Deve-se saber também o nível de acesso e ter o controle sobre quais dispositivos estão conectados à rede, realizar o monitoramento constante e reforçar a política de privacidade.

IV.ATAQUES NA REDE

Um dos ataques mais comuns na Internet das Coisas é DDoS (*Distributed Denial of Service)* que retira um computador ou uma rede da sua operação de serviço. Este ataque realiza várias acessos em diversos dispositivos em uma rede, com a sobrecarga no servidor, a consequência será a inoperabilidade do seu funcionamento. Uma das formas para se proteger desse ataque é usar um *firewall* para fazer o controle e gerenciar as solicitações de conexões de um site.

Alguns casos famosos de ataques a sites usando DDoS, já foram registrados, como por exemplo o GitHub que é a maior rede de hospedagem de código fonte do mundo, que foi derrubada durante seis minutos na onda de 1,3 tb/s. Para resolver este problema fez-se um redirecionamento de conexões e uma filtragem voltado para bloquear e detectar o tráfego de informações maliciosas. Contudo o site foi capaz de conter o ataque e rapidamente reduzir os riscos.

O objetivo do *hacker*, independente do negócio que o usuário tem, é roubar a informação. Alguns invasores tentam inserir vírus na máquina para coletar informações importantes, caso isso dê errado o ataque *man-in-the-middle* é um dos mais viáveis por ser difícil de detectar e especialmente por usuários inexperientes. Como o nome já diz, o *hacker* coloca suas armadilhas entre a vítima e um *site*, como por exemplo quando um cliente de um banco deseja acessar sua conta por meio da *Internet*, uma outra pessoa com intenções de roubar seus dados pode explorar a vulnerabilidade da rede, para receber todos os dados e enviar de volta a rede, e assim roubar informações do usuário.

Apesar de ser perigoso e causar danos o *man-in-the-middle* pode ser evitado. Cuidados básicos como a navegação na *Internet* evitando o HTTP pois o HTTPS é criptografado impedindo *hackers* a terem acesso à rede.

V.CONCLUSÃO

Com este trabalho, foi possível saber como um protocolo na *IoT* funciona na sua parte técnica. Aprender sobre os seus diferentes meios de comunicações e como eles podem ajudar e até mesmo fazer serviços que humanos realizam de uma forma ágil e prática com apenas alguns comandos. Assim, deve-se observar a implementação da camada de segurança na rede, para que os dispositivos não fiquem vulneráveis a ataques.

VI.REFERÊNCIAS

Sites:

[1] https://www.meupositivo.com.br/panoramapositivo/internet-das-coisas/

[2] https://canaltech.com.br/internet-das-coisas/o-desafio-da-seguranca-no-mundo-das-coisas-97404/

[3] https://www.frenet.com.br/blog/gateway-o-que-e-como-funciona/

[4]https://www.arcon.com.br/blog/iot-atencao-a-seguranca-da-informacao

[5]https://docs.microsoft.com/pt-br/azure/iot-fundamentals/iot-security-deployment

[6]https://www.welivesecurity.com/br/2017/03/17/ataques-a-iot/

[7]https://tecnoblog.net/235518/maior-ataque-ddos-github/