CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA

CURSO DE GRADUAÇÃO TECNOLÓGO EM
REDES DE COMPUTADORES

GIVALDO CORREIA DOS SANTOS
JULIANA SILVA CARVALHO

REDES DE SENSORES SEM FIO E OS PRINCIPAIS TIPOS DE ATAQUES.

RECIFE/2021

GIVALDO CORREIA DOS SANTOS
JULIANA SILVA CARVALHO

REDES DE SENSORES SEM FIO E OS PRINCIPAIS TIPOS DE ATAQUES.

S277r Santos, Givaldo Correia dos
Redes de Sensores Sem Fio e os Principais Tipos de Ataques / Givaldo Correia Dos Santos; Juliana Silva Carvalho. - Recife: O Autor, 2021.
28 p.

Orientador (A): Me. Ameliara Freire Santos de Miranda.
Coorientador: Me. Luiz Sérgio Lima

Trabalho de Conclusão de Curso (Graduação) Centro Universitário Brasileiro – UNIBRA Graduação Tecnologica em Redes de Computadores, 2021

1.Ataque de Negação 2.RFID 3.RSSF 4 Internet das Coisas 5.Ataque DDos. I. Centro Universitário Brasileiro. – Unibra.II. Título.

CDU: 004.7

GIVALDO CORREIA DOS SANTOS

JULIANA SILVA CARVALHO

REDES DE SENSORES SEM FIO E OS PRINCIPAIS TIPOS DE ATAQUE.

Trabalho de Conclusão de Curso apresentado ao Curso de Redes de Computadores, da Unibra, como requisito parcial para obtenção do certificado, sob orientação da Profª Msc Ameliara Freire Santos de Miranda.
Coorientador: Prof° Msc Luiz Sérgio Lima

GIVALDO CORREIA DOS SANTOS

JULIANA SILVA CARVALHO

REDES DE SENSORES SEM FIO E OS PRINCIPAIS TIPOS DE ATAQUES.

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores, pelo Centro Universitário Brasileiro – UNIBRA, por uma comissão examinadora formada pelos seguintes professores:

_____

Prof° Msc Ameliara Freire Santos de Miranda
Professor (a) orientador (a)

_____

Prof° Esp. Diego Ribeiro Gomes

_____

Prof° Esp. Osmar Carlos da Silva

Recife, ___/___/___

Nota:_____

Dedicamos esse trabalho a nossos pais, amigos e mestres.

AGRADECIMENTOS

Agradecemos aos nossos pais pelo amor e apoio incondicional. Aos nossos amigos, companheiros de trabalho que fizeram parte da nossa formação e que também estarão presentes no nosso futuro. À nossa orientadora Ameliara Freire e ao nosso coorientador Luiz Sérgio Lima, pelo suporte no pouco tempo que lhes couberam, pelas suas correções e incentivos, também aos mestres que nos proporcionaram conhecimento e dedicação durante esta jornada.

“ Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos alguma coisa. Por isso aprendemos sempre.”

(Paulo Freire)

SUMÁRIO

INTERNET DAS COISAS: ASPECTOS DE SEGURANÇA RELACIONADOS AOS DADOS DO USUÁRIO.

GIVALDO CORREIA DOS SANTOS
JULIANA SILVA CARVALHO
ORIENTADORA: AMELIARA FREIRE
COORIENTADOR: LUIZ SÉRGIO LIMA

Resumo: Abordaremos alguns problemas de segurança existentes na Internet das Coisas (IoT), com uma pequena análise dos problemas de privacidade que um usuário final pode enfrentar como consequência da disseminação da IoT.
Os resultados encontrados sugerem que para mitigar estes riscos é necessária a inserção de valores e princípios fundamentais, como privacidade e segurança, ainda no início da cadeia de desenvolvimento da IoT.
A conclusão desta pesquisa, apresentará uma proposta para as etapas necessárias a serem tomadas para abordar todas as questões de segurança da IoT.

Palavras-chave: Ataque de negação, RFID, RSSF, Internet das Coisas, Ataque DDoS.

Abstract

This research will address some security problems that exist in the Internet of Things (IoT), together with an analysis of the privacy problems that an end user may face as a consequence of the spread of IoT. The focus of this study is on the security breaches resulting from the information exchange technologies used in the Internet of Things.
The results found suggest that in order to mitigate these risks, it is necessary to insertion of fundamental values and principles, such as privacy and security, still at the beginning of the IoT development chain.
The conclusion of this research, will present a proposal for the necessary steps to be taken to address all IoT security issues.

Keywords: Denial attack, RFID, RSSF, Internet of Things, DDoS attack.

1 INTRODUÇÃO

A Internet das Coisas (IoT) é um conceito utilizado para definir a interconexão de objetos do nosso cotidiano na internet. A ideia começou com Bill Joy, co-fundador do Sun Microsystems em 1991, quando o protocolo TCP/IP começou a ficar em evidência e a rede começou a tomar forma, tornando o que conhecemos hoje (MAGRANI, 2018).

Segundo Tan e Wang, a Internet das Coisas é uma nova forma de tecnologia da informação e da comunicação que difere-se da habitual, onde pessoas se comunicam com outras pessoas. Agora as coisas também poderão se comunicar com as pessoas e com outros dispositivos. (TAN e WANG, 2010)

Dentro desse âmbito temos tecnologias como: casas inteligentes, aplicativos em geral, smartwatches (relógios inteligentes), computação em nuvem e muitos outros exemplos. Ainda que se obtenha bastante vantagens desse meio tecnológico, é de grande importância a preocupação com as vulnerabilidades de segurança e de privacidade que acompanham essa era revolucionária (ANSCOMBE, 2018).

De acordo com a pesquisa Fortify on Demand da HP, 90% dos dispositivos usados na IoT (Internet of Things) coleta dados pessoais do usuário, seja por meio da nuvem, aplicativo ou o próprio dispositivo e não oferece proteção adequada (SMITH; MIESSLER, 2014). Acarretando falhas de privacidade e confiança, tais problemas serão abordados durante essa pesquisa.

Apesar do imenso potencial da IoT em várias áreas, toda a infraestrutura de comunicação da IoT é falha do ponto de vista da segurança e é suscetível a perda de privacidade para os usuários finais. Alguns dos problemas de segurança proeminentes que assolam todo o desenvolvimento da IoT, surgem dos problemas de segurança presentes nas tecnologias usadas para retransmissão de informações de um dispositivo para outro.

Nesta pesquisa, abordaremos a tecnologia de comunicação RFID (IDENTIFICAÇÃO POR RADIOFREQUÊNCIA) que usa a infraestrutura da Internet para troca de informações. Mostraremos alguns os problemas de segurança que assolam a Internet das coisas, bem como as questões de privacidade, que mostraremos no texto, enfrentadas pelos usuários finais que utilizam a avançada arquitetura de compartilhamento de informações da IoT.

1.1 MOTIVAÇÃO

Em virtude da crescente aplicação da Internet das Coisas em vários setores do cotidiano, foi observado a necessidade de verificar as questões da falta de segurança e problemas de privacidade nas redes sem fio (RSSF) que as pessoas na sociedade enfrentam, e se realmente estão preparadas para IoT. Um ambiente de infraestrutura na internet no qual cada vez mais circulam dados que conectam indivíduos e empresas em todo o mundo. Essas tecnologias permitem que estudos, trabalho, negócios e lazer sejam conduzidos de forma simples, prática e facilitada, porém, não se pode afirmar que não existam riscos e vulnerabilidades.

Pensar em inovação tecnológica é olhar para o futuro, pois hoje a internet deixou de conectar apenas computadores, para conectar pessoas, a evolução das tecnologias permite essa conectividade em inúmeros tipos de dispositivos na rede IoT. Diante disso, é preciso analisar qual relevância da segurança da informação na proteção de dados que trafegam nessa nova tecnologia, tão atraente aos usuários pelo que pode proporcionar e ao mesmo tempo expor informações importantes e sigilosas que podem trazer transtornos irreparáveis.

1.2 METODOLOGIA DA PESQUISA

Análises bibliográficas, traduções de obras com auxílio de ferramentas específicas e compreensão sobre o tema.

2 IoT (Internet das Coisas)

Internet of Things (IoT) é um conceito emergente para as coisas habilitadas por sensores com endereço de protocolo de rede (IP). Ele pode se conectar com a Internet e coletar dados do sensor, analisar esses dados e tomar uma decisão automaticamente. IoT é uma rede de dispositivos (coisas) conectado para melhorar o desempenho do dia-a-dia e também incorpora diferentes tipos de dispositivos com recursos limitados, como implantáveis (etiquetas RFID) (Fan et al. 2009), wearables (relógios inteligentes) e dispositivos externos (smartphones, termostatos, geladeiras inteligentes).

Em 2000, um cientista da computação chamado Kevin Ashton expressou as primeiras definições para a Internet das Coisas (IoT) num laboratório do MIT(Instituto de Tecnologia de Massachusetts) enquanto fazia pesquisas para melhorar as atividades comerciais da empresa Procter e Gamble (P&G) conectando RFID (Identificação por

radiofrequência) e internet, para que o funcionamento da tecnologia não se limitasse à inserção de dados por humanos, e computadores pudessem fazer sua própria coleta de informações, mesmo que por pequenos comandos dados por nós(BALAGUER, 2014).

Nessa época a internet ainda enfrentava limitações e necessitava de melhorias consideráveis. Hoje temos o protocolo IPv6 que fornece uma grande quantidade de IPs para que cada vez mais dispositivos se conectem à rede de computadores (CANNO, 2013).

De um modo geral, a Internet das Coisas é uma rede de objetos com capacidade computacional e comunicação com a internet, que torna possível monitorar remotamente, além de possibilitar a coleta e a transmissão de dados (MAGRANI, 2018). O relatório "*IoT Healthcare Market of Components, application, end user - global forecast for 2020* "(Anonymous 2016a) diz que em todo o mundo o mercado de informações médicas de IoT valia $32,47 bilhões em 2015. Além disso, estima-se que esse valor de mercado aumentou em $163,24 bilhões em 2020. Outro estudo mais recente da "*IoT in Healthcare Market by Component (Medical Device, Systems & Software, Services, and Connectivity Technology), Application (Telemedicine, Connected Imaging, and Inpatient Monitoring), End User, and Region - Global Forecast to 2025*" afirma que nesse mercado irá crescer $ 72,5 bilhões em 2020 para $ 188,2 bilhões em 2025. O motivo dessa grande expectativa é o tratamento oportuno e a comunicação inteligente da IoT entre o médico e o paciente.

Ao usar dispositivos médicos IoT, um médico pode remotamente rastrear a saúde de um paciente, usando o funcionamento de dispositivos biomédicos na busca do melhor tratamento para o paciente (GRAHAM, 2014).

Este monitoramento em tempo real dos parâmetros fisiológicos do paciente é útil para prevenir problemas de saúde na fase inicial, por outro lado, estes dispositivos médicos são vulneráveis a ataques wireless quando associados à Internet por meio de IPv6(JVIANA,2017). Quando esses dispositivos, por exemplo, um marca-passo, é comprometido por invasores, dados médicos confidenciais serão expostos, ou o paciente pode ter seu dispositivo inutilizado, o que por sua vez ameaça a sua vida (RAYES; SALAM, 2016).

A troca automática de informações entre dois sistemas ou dois dispositivos sem qualquer entrada manual é o objetivo principal da Internet das Coisas. Esta troca automatizada de informações entre dois dispositivos ocorre por meio de algumas tecnologias de comunicação específicas, que são descritos abaixo:

2.1 Redes de Sensores Sem Fio (RSSF)

As redes sem fio surgiram como redes complementares às redes cabeadas, com o intuito de promover a mobilidade e a visualização rápida dos dados independentemente da localização do usuário, tendo os dados transmitidos pelo ar ou espaço livre, que se constituem como meio físico para propagação de sinais eletromagnéticos, provendo uma interconexão completa, e permitindo uma grande flexibilidade na localização das estações, sendo essa a principal diferença entre as redes sem fio e as redes convencionais. O processo continuou com o desenvolvimento de novas tecnologias e no aumento da velocidade de transmissão de dados que contribuiu com a diversificação das possibilidades até ao desenvolvimento de tecnologias para aplicações mais simples assim como o Bluetooth, com infraestrutura mais simples e baixo consumo energético o que lhe inclina a tal desinência (NÉRIO, 2003)

De acordo com (AKYILDIZ,2002), as RSSF são composições de nós independentes, cuja comunicação sem fio leva a colocar em frequência e largura de banda limitada. Os nós de comunicação de uma rede de sensores sem fio típica consistem nas seguintes partes:

i. Sensor
ii. Microcontrolador
iii. Memória
iv. Rádio Transceptor
v. bateria

Devido à faixa de comunicação limitada de cada nó de uma RSSF, ocorre a retransmissão de informações de vários saltos entre a fonte e a estação base. Os dados necessários são coletados pelos sensores sem fio por meio de colaboração entre os vários nós, que é então enviado para o coletor nó para roteamento direcionado para a estação base. A rede de comunicação formada dinamicamente pelo uso de transceptores de rádio sem fio facilita a transmissão de dados entre os nós. Uma transmissão multi-salto de dados requer diferentes nós para receber cargas de tráfego diversas (GUICHENG;BINGWU,2011).

2.2 *Radio Frequency Identification* (RFID)

RFID, ou Identificação por Radiofrequência, é uma tecnologia sem fio (wireless) destinada a coleta de dados. Tal qual o código de barras, o RFID faz parte do grupo de tecnologias de Identificação e Captura de Dados Automáticos. Seu surgimento remonta

há várias décadas, mas o crescimento massivo de seu uso vem se percebendo nos últimos anos, em especial pelam redução do custo de seus componentes.

Um sistema RFID é composto por um transceptor que transmite uma onda de radiofrequência, através de uma antena, para um transponder, ou mais conhecido por tag. O tag absorve a onda de RF e responde com algum dado. Ao transceptor é conectado um sistema computacional que gerencia as informações do sistema RFID.(fonte:https://www.teleco.com.br/rfid.asp)

Esta tecnologia é usada principalmente em etiquetas de informação interagindo com as outras automaticamente. Etiquetas RFID usam ondas de rádio de frequência para interação e troca de informações entre si, sem necessidade de alinhamento, de estar na mesma direção ou contato físico. Nela é usada a tecnologia *Automatic Identification and Data Capture* (AIDC) (Benjamin,2011).
Um RFID é composto do seguinte dois componentes:

2.3 Etiquetas RFID (Transponders)

Em uma etiqueta RFID, uma antena é embutida em um microchip.A etiqueta RFID também consiste em unidades de memória, que abrigam um identificador exclusivo conhecido como Electronic Product Code (EPC).A função do EPC em cada etiqueta é fornecer dados numéricos universais pelos quais uma determinada etiqueta é reconhecida. De acordo com (GUICHENG;BINGWU,2011),os tipos de etiquetas RFID são:

i. Etiqueta ativa: este tipo de etiqueta tem uma bateria interna, que facilita a interatividade do EPC exclusivamente com outros EPCs ao redor, remotamente de uma distância limitada.

ii. Etiqueta passiva: neste tipo de etiqueta, a informação é retransmitida do EPC apenas quando é ativada por um transceptor a partir de um intervalo predefinido da etiqueta. A falta de uma bateria interna nas etiquetas passivas é substituída pela utilização do sinal eletromagnético emitido por um leitor de etiquetas através acoplamento indutivo como fonte de energia.

Uma etiqueta RFID opera em conjunto com um leitor de etiquetas, o EPC do primeiro sendo a assinatura de identificação de um tag particular sob a varredura do último (BORGOHAIN; KUMAR; SANYAL, 2015) .

2.3.1 Leitores RFID (Transceivers)

O leitor RFID funciona como detector de identificação de cada etiqueta por sua interação com o EPC da tag sob sua varredura (CLAUBERG,2004).

Problemas de segurança na tecnologia RFID

No contexto da IoT, a tecnologia RFID é usada principalmente com etiquetas para troca automatizada de informações sem qualquer envolvimento manual. Mas as etiquetas RFID são propensas a vários ataques devido à falha de segurança da tecnologia RFID. Os quatro tipos mais comuns de ataques e problemas de segurança de etiquetas RFID(BURMESTER; MEDEIROS, 2007),(XIAO; GIBBONS; LEBRUN, 2009), são os seguintes:

I.*Unauthorized tag disabling* (Ataque à autenticidade):

Os ataques dos na tecnologia RFID levam a incapacitação das etiquetas RFID temporariamente ou permanentemente. Esses ataques controlam uma etiqueta RFID para apresentar mau funcionamento e/ou apresentar falha na leitura durante a varredura de um leitor de etiquetas, fazendo o EPC apresentar informações erradas de identidade na combinação numérica atribuída a ele. Estes ataques DOS podem ser feitos remotamente, permitindo que o invasor manipule o comportamento da etiqueta à distância (XIAO; GIBBONS; LEBRUN, 2009).

II. *Unauthorized tag cloning* (ataque à integridade):

A captura das informações de identificação (como o EPC) por meio da manipulação das etiquetas por leitores desonestos cai nesta categoria. Uma vez que a identificação da informação de uma etiqueta está comprometida, a sua replicação (clonagem) é possível, a qual pode ser usada para contornar medidas de segurança falsificadas, bem como introduzindo novas vulnerabilidades em qualquer indústria usando etapas de verificação automática de etiquetas RFID (XIAO; GIBBONS; LEBRUN, 2009).

III. *Unauthorized tag tracking* (Ataque à confidencialidade):

Uma etiqueta pode ser rastreada por meio de leitores infectados, o que pode resultar no acesso indevido à informações como o endereço de uma pessoa. Assim, do ponto de vista do consumidor, comprar um produto com RFID não lhes garante confidencialidade em relação à sua compra e põe em perigo sua privacidade. Esses são ataques de privacidade nos quais o invasor pode rastrear etiquetas por meio de leitores infectados. São chamados ataques de preocupações do "BigBrother" que entidades corporativas que gerenciam o servidor *back-end* podem aproveitar os recursos de RFID para invadir a privacidade dos consumidores (FLOERKEMEIER; SCHNEIDER; LANGHEINRICH, 2005).

IV. *Replay attacks* (Ataque à disponibilidade):

Neste tipo de ataques usando identificação falsa, o invasor usa a resposta da leitura de uma etiqueta por um leitor infectado para copiá-la(BURMESTER; MEDEIROS, 2007). Então o sinal de comunicação entre o leitor e a etiqueta é interceptado, gravado e reproduzido após o recebimento de qualquer consulta do leitor em um tempo, falsificando assim a informação da etiqueta.

Além destes, segue algumas vulnerabilidades na segurança de tecnologias RFID são (XIAO; GIBBONS; LEBRUN, 2009):

I. Engenharia Reversa:

A Engenharia Reversa é uma atividade que trabalha com um produto existente (um software, uma peça mecânica, uma placa de computador, etc.) tentando entender como este produto funciona, o que ele faz exatamente e como ele se comporta em todas as circunstâncias. Fazemos engenharia reversa quando queremos trocar, modificar uma peça (ou um software) por outro, com as mesmas características ou entender como esta funciona e não temos acesso a sua documentação(CANHOTA JUNIOR; et al 2005).

II. *Power Analysis* ou Ataque Lateral:

A análise de energia é um ramo dos ataques de canal lateral em que os dados de consumo de energia são usados como canal lateral para atacar o sistema (GAMAARACHCHI; GANEGODA, 2018) .

III. *Eavesdropping* (Interceptação):

Neste tipo de exploração, um terceiro elemento faz uso de uma antena receptora de ondas de rádio para interceptar o sinal enviado pelo emissor. Vale ressaltar que uma vez interceptado, o sinal deve ser decodificado para que informação útil seja extraída. Trata-se, dessa forma, de uma exploração passiva (DUARTE; COSTA, 2013) .

IV. *Man-in-the-middle attack* (Ataque Homem no Meio):

Trata-se de um ataque clássico, no qual dois elementos buscam se comunicar e são levados por um terceiro elemento a crer que de fato o fazem, quando na verdade estão participando de uma comunicação a três na qual esse terceiro elemento age como intermediário (DUARTE; COSTA, 2013).

V. *Denial of Service* (DoS) ou Ataque de Negação:

São, como o nome diz, um tipo de ataque cujo objetivo é interromper ou prejudicar o fornecimento de um serviço. Por exemplo, um ataque *DoS* pode ser realizado para

sobrecarregar uma rede de modo a torná-la lenta, para afetar a estabilidade de serviços de e-mail ou para impedir o acesso de uma página da Internet (GOMES; ARAUJO; CAMPOS, 2015) .

VI. *Spoofing*:

No contexto da segurança da informação, e especialmente da segurança da rede, um ataque de falsificação é uma situação em que uma pessoa ou programa se identifica com sucesso como outro falsificando dados, para obter uma vantagem ilegítima (JINDAL; DALAL; SHARMA, 2014).

VII. Vírus:

São softwares que são instalados em um computador sem o conhecimento do usuário, com a finalidade de fazer alterações prejudiciais, roubar dados e até mesmo estragar o hardware (KINAST, 2019).

VIII. *Tracking* ou Ataque de Rastreamento não autorizado:

É baseado no rastreamento das respostas de uma tag para uma tag falsa (BURMESTER; MEDEIROS, 2007).

IX. *Killing Tag Approach*:

Normalmente, esse ataque afeta a etiqueta RFID para evitar que ela se comunique, tornando-a impossível a sua leitura (XIAO; GIBBONS; LEBRUN, 2009).

2.4 SEGURANÇA DA INFORMAÇÃO

Tanto na Internet das Coisas, como em qualquer área de tecnologia, ocorrem sérias preocupações com a segurança. A Internet das Coisas, possui problemas em relação a segurança que são inerentes a ela, sem contar as falhas que advêm de outras tecnologias.

Embora exista um grande potencial da Internet das Coisas em vários campos de implementação, essa infraestrutura de interconexão é falha do ponto de vista de segurança e está sujeita a exposição da privacidade dos dados do usuário final.

De acordo com (BALAGUER, 2015):

> Com a rápida expansão da utilização da Internet das Coisas em todo o mundo, além da crescente disseminação de malwares para todo tipo de hardware e software (sejam sistemas operacionais ou aplicativos), a preocupação com a Segurança da Informação (dados pessoais e corporativos) também deve seguir entre as principais prioridades da indústria de Tecnologia da Informação.

Os problemas de segurança mais recorrentes no desenvolvimento da Internet das Coisas, advêm justamente das vulnerabilidades presentes nas tecnologias usadas em IoT para a retransmissão de informações de um dispositivo para outro.

A grande quantidade de dispositivos oferecendo comodidades, se tornou um grande atrativo para usuários comuns e é exatamente onde reside o risco à segurança. Observem essa análise (JUNIOR,2016):

> Como milhões de novos dispositivos passam a estar conectados, é inevitável que algumas pessoas levem seu gadgets para o ambiente de trabalho. Caso se conectem à rede da empresa, é natural que aquele objeto passe a ser mais um endpoint, ou seja, mais uma porta de entrada para vírus e malwares.

2.4.1 Problemas de segurança nas redes de sensores sem fio (RSSF):

As formas de ataque que podem ser realizadas em uma rede sem fio podem ser divididas em 3 categorias(SACHDEVA; SINGLA, 2013):

I. Ataque ao Sigilo e autenticação:

A confidencialidade dos dados é a questão mais importante na segurança da rede. Cada rede com qualquer enfoque de segurança, normalmente resolverá esse problema primeiro.

II. Ataques silenciosos à integridade dos serviços:

Com a implementação da confidencialidade, um adversário pode ser incapaz de roubar informação. No entanto, isso não significa que os dados estão seguros. O invasor pode alterar os dados, de modo a enganar a rede de sensores. O objetivo do invasor é fazer com que a rede aceite um valor de dados falso. Por exemplo, um invasor compromete um sensor nó e injeta um valor de dados falso por meio desse sensor.

III. Ataque na disponibilização de redes: O ataque de Negação de Serviços (DoS) cai nesta categoria.

As ações de acessibilidade buscando fazer invasores se passarem por usuários legítimos, podem ocorrer em diferentes camadas de uma rede de acordo com (JAYDIP,2013), (SAXENA,2007) e (SEN,2009):

Ataque DoS na camada física:

A camada física de uma rede de sensores sem fio realiza a função de seleção e geração de frequência portadora, modulação e demodulação, criptografia e descriptografia, transmissão e recepção de dados (BHAT, 2011). Esta camada da rede de sensores sem fio é atacada principalmente através de:

1. *Jamming*: neste tipo de ataque DoS o canal de comunicação entre os nós sofre uma interferência proposital, impedindo-os de se comunicarem uns com os outros.

2. *Node tampering*: A adulteração física do nó para extrair informações confidenciais.

Ataque DoS na camada de enlace:

A camada de enlace do RSSF multiplexa os vários fluxos de dados, fornece detecção de quadro de dados, MAC e controle de erros. Além disso, a camada de enlace garante ponto a ponto ou ponto de confiabilidade multiponto (ALKHATIB; BAICHER,2012).Os ataques DoS que ocorrem nessa camada são:

1. *Collision*: este tipo de ataque DoS pode ser iniciado quando dois nós transmitem simultaneamente pacotes de dados no mesmo canal de frequência. A colisão de pacotes de dados resulta em pequenas mudanças nos resultados do pacote em identificação do pacote como uma incompatibilidade no recebimento fim. Isso leva ao descarte do pacote de dados afetado para retransmissão (GHILDIYAL, 2014).

2. *Unfairness*: Conforme descrito em (GHILDIYAL, 2014), é um ataque baseado em colisão repetida. Também pode ser descrito como um ataque baseado em exaustão.

3. *Battery Exhaustion*: este tipo de ataque DoS causa tráfego excepcionalmente alto em um canal, tornando sua acessibilidade muito limitado para nós. Essa interrupção no canal é causada por um grande número de solicitações (*Request To Send*) e transmissões pelo canal.

Ataque DoS na camada de rede:

A principal função da camada de rede do RSSF é o roteamento. Os ataques DoS específicos que ocorrem nessa camada são:

1. *Spoofing*, reprodução e direcionamento incorreto do tráfego.

2. *Hello flood attack:* Este ataque causa congestionamento do canal com um alto número de mensagens HELLO falsas. Aqui um único nó malicioso envia uma mensagem falsa que é reproduzida por um invasor para criar um congestionamento.

3. *Homing*: em caso de ataque de *homing*, uma busca é feita no tráfego pelo *cluster heads* e/ou *key managers* que têm a capacidade de desligar toda a rede.

4. Encaminhamento seletivo: como o próprio nome sugere, em encaminhamento seletivo, um nó comprometido envia pacotes apenas para alguns nós em vez de todos os nós. Esta seleção de nós é feita com base no requisito do invasor para atingir seu objetivo malicioso e então, esses nós deixam de encaminhar pacotes de dados.

5. *Sybil*: em um ataque de *Sybil*, o invasor replica um único nó e o apresenta com múltiplas identidades para o outro nós.

6. *Wormhole*: este ataque DoS causa realocação de bits de dados de sua posição original na rede. Esta a realocação do pacote de dados é realizada por meio de tunelamento de bits de dados em um link de baixa latência.

Ataque DoS na camada de transporte:

Esta camada da arquitetura WSN fornece confiabilidade de transmissão de dados e evita congestionamento resultante de alto tráfego nos roteadores. Os ataques DoS nesta camada são:

1. *Flooding*: Refere-se ao congestionamento deliberado de canais de comunicação através da retransmissão de pacotes desnecessários e alto tráfego.

2. *De-synchronization*: Neste tipo de ataque, instruções falsificadas são enviadas em um ou ambos os endpoints solicitando retransmissões para correção de erro inexistente. Esta retransmissão resulta em perda de energia em um ou ambos os *endpoints* ao executar as instruções falsificadas.

Ataque DoS na camada de aplicação:

A camada de aplicação do RSSF assume a responsabilidade de gerenciamento de tráfego. Ele também atua como o provedor de software para diferentes aplicações que realiza a tradução de dados em uma forma compreensível ou ajuda na coleta de informações por meio do envio de consultas (ALKHATIB; BAICHER, 2012). Nessa camada, um ataque DoS baseado em caminho é iniciado estimulando os nós sensores para criar um enorme tráfego na rota em direção à estação base(Pathan,2010),(GHILDIYAL, 2014).

Na figura 3, são mostrados todos os ataques DoS mencionados acimanas diferentes camadas de uma rede de sensores sem fio.

Outros tipos Ataques de Negação (DoS) de acordo com (SAXENA,2007), (SEN,2009), (SACHDEVA; SINGLA, 2013) e (PADMAVATHI; SHANMUGAPRIYA,2009):

> I. *Neglect and Greed Attack* (Ataque de negligência e ganância); II. *Interrogation* (Interrogatório); III. *Black Holes* (Buracos Negros); IV. *Node Subversion* (Nó de Subversão); V. *Node malfunction* (Mau funcionamento do nó);VI. *Node Outage* (Falha do nó); VII. *Passive Information Gathering* (Coleta de informações passivas); VIII. *False Node* (Nó Falso); IX. *Message Corruption* (Corrupção de mensagens).

Outros problemas observados na segurança e privacidade em uma RSSF são(SACHDEVA; SINGLA, 2013),(BIANCHI,2010) e (ZIA,2008):

> I. Confidencialidade de dados; II. Integridade de dados; III. Autenticação de Dados; IV. Atualização de dados; V. Disponibilidade; VI. Auto-organização; VII. Sincronização de Horário; VIII. Localização Segura; IX. Flexibilidade; X. Robustez e capacidade de sobrevivência

De acordo com (Karlof;Wagner,2003) as ameaças que pairam sobre as RSSF podem ainda ser classificado da seguinte forma:

I. Ataques externos versos internos;
II. Ataques passivos versos ativos;
III. Ataques Mote-class verso laptop-class attacks

Conforme (Chen; et al 2009) os ataques às RSSF podem ser classificados como:
I. Interrupção
II. Interceptação
III. Modificação
IV. Fabricação

Os ataques a RSSF podem ainda ser classificados como:

I. *Host-based attacks*
II. *Network-based attacks*

São essas algumas das falhas de segurança existentes em uma infraestrutura de Internet das Coisas que podem revelar-se muito prejudiciais no seu desenvolvimento e implementação em diferentes áreas. Adotando práticas de medidas de segurança,

buscando se prevenir de falhas de segurança, implementando sistemas de detecção de intrusão, criptografias e medidas de segurança estenográfica no processo de troca de informações e usando métodos eficientes para comunicação, como resultado teremos uma infraestrutura de Internet das Coisas mais segura e eficiente.

3 CONCLUSÃO

Neste trabalho, examinamos algumas falhas de segurança que podem afetar a Internet das Coisas através de vulnerabilidades nas redes sem fio que podem ser bastante prejudiciais no desenvolvimento e implementação de IoT nos diferentes campos de atuação tecnológica.

Portanto, a adoção de medidas sólidas de segurança (GOYAL; et al 2006), (GOYAL; ABRAHAM; SANYAL; HAN, 2005), (GOYAL; et al 2005), (VASUDEVAN; ABRAHAM; SANYAL; AGRAWAL,2004) buscando se precaver ou combater as falhas de segurança detalhadas acima, bem como a implementação de vários sistemas de detecção de intrusão (BHATTASALI; CHAKI; SANYAL, 2012), (TRIVED, et al 2013). Acrescidos de medidas de segurança criptográficas e estenográficas (DEY; ABRAHAM; SANYAL,2007) nos processos de troca de informações e uso de métodos eficientes para comunicação (ROY; BANIK; et al 2012), isto resultará em um sistema mais seguro e robusto de Infraestrutura de IoT.

Ressaltamos que todas as ameaças de segurança mencionadas anteriormente, por exemplo, o *Hello flood attack*, ataque *wormhole*, o ataque *Sybil* serve a um propósito comum que é comprometer a integridade da rede que eles atacam. No passado, o foco não era na segurança de RSSFs. A segurança se tornou uma importante questão de confidencialidade de dados à medida que as várias ameaças foram surgindo. Nesta pesquisa, tentamos apresentar a algumas das ameaças de segurança em RSSF com estudo extensivo.

Desta forma, acreditamos que um esforço para o desenvolvimento de medidas de segurança e proteção à privacidade para a atual infraestrutura da Internet das Coisas seria mais produtivo, antes de continuar desenvolvendo novos dispositivos inteligentes no dia a dia.

REFERÊNCIAS

AKYILDIZ, I.F. ; Georgia Inst. of Technol., Atlanta, GA,USA ; Weilian Su ; Sankarasubramaniam, Y. ; Cayirci,E **"A survey on sensor networks."** Communications magazine, IEEE 40.8 (2002): 102 -114.

ALKHATIB, Ahmad Abed Alhameed; BAICHER, Gurvinder Singh. **"Wireless sensor network architecture."** International conference on computer networks and communication systems (CNCS 2012) IPCSIT. Vol. 35. 2012, pp. 11-15.

AL-Sakib Khan Pathan, **"Denial of Service in Wireless Sensor Networks: Issues and Challenges"**, Advances in Communications and Media Research, Vol. 6 (Edited by Anthony V. Stavros), ISBN: 978-1-60876-576-8, Nova Science Publishers, Inc., USA, 2010.

ANSCOMBE, Tony. **IoT AND PRIVACY BY DESIGN IN THE SMART HOME**. 2018. 19 f. Tese (Doutorado) - Curso de Redes de Computadores, Eset, Bratislava, 2018.
ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. **The Internet of Things: a survey. Computer Networks**, [S.L.], v. 54, n. 15, p. 2787-2805, out. 2010. Elsevier BV. http://dx.doi.org/10.1016/j.comnet.2010.05.010.

B. T. Wang and H. Schulzrinne, **"An IP traceback mechanism for reflective DoS attacks"**, Canadian Conference on Electrical and Computer Engineering, vol. 2, (2004) May 2-5, pp. 901-904.

BALAGUER, Adriano Lucas. **Internet das Coisas: das origens ao futuro**: hoje já se fala também em ioe (internet of everything ⁖ internet de todas as coisas) e wot (web of things - web das coisas). Hoje já se fala também em IoE (Internet of Everything – Internet de Todas as Coisas) e WoT (Web of Things - Web das Coisas). 2014. Disponível em: https://cio.com.br/tendencias/internet-das-coisas-das-origens-ao-futuro/. Acesso em: 30 maio 2021.

BHAT, Pavan. **Wireless sensor networks**: physical layer for wireless sensor networks. Physical Layer for Wireless Sensor Networks. 2011. Disponível em: http://sensors-and-networks.blogspot.in/2011/08 /physical-layer-for-wireless-sensor.html. Acesso em: 30 maio 2021.

BHATTASALI, Tapalina; CHAKI, Rituparna; SANYAL, Sugata. Sleep Deprivation Attack Detection in Wireless Sensor Network. International Journal Of Computer Applications, [S.L.], v. 40, n. 15, p. 19-25, 29 fev. 2012. Foundation of Computer Science. http://dx.doi.org/10.5120/5056-7374.

BORGOHAIN, Tuhin *et al*. **Survey of Security and Privacy Issues of Internet of Things**,Mumbai,India,p.1-7,2015.Diponível em: www.researchgate.net/publication/270763270_Survey_of_Security_and_Privacy_Issues_of_Internet_of_Things. Acesso em: 3 maio 2021.

BORGOHAIN, Tuhin; KUMAR, Uday; SANYAL, Sugata. **Survey of Security and Privacy Issues of Internet of Things.** 2015. Disponível em: https://www.researchgate.net/publication/270763270_Survey_of_Security_and_Privacy_Issues_of_Internet_of_Things. Acesso em: 23 jun. 2021.

BURMESTER, Mike; MEDEIROS, Breno de. **"RFID security: attacks, countermeasures and challenges."** The 5th RFID Academic Convocation,The RFID Journal Conference. 2007.

CANHOTA JUNIOR, Antonio Jorge Sapage da; SOUZA, Diego Alves de; MOUTINHO, Diogo dos Santos; LOHNEFINK, Felipe Paixão. **ENGENHARIA REVERSA**. 2005. 14 f. TCC (Graduação) - Curso de Ciência da Computação, Instituto de Computação, Universidade Federal Fluminense, Niterói, 2005. Disponível em: http://www.ic.uff.br/~otton/graduacao/informaticaI/apresentacoes/eng_reversa.pdf. Acesso em: 23 jun. 2021.

CANNO, Renato Montes. Redes IP I: Técnicas de Migração de Ambientes de Redes IPv4 para IPv6. 2013. Disponível em: https://www.teleco.com.br/tutoriais/tutorialredeip1/default.asp. Acesso em: 23 jun. 2021.

DEMO, P. **Pesquisa: Princípios científicos e educativos.** 7ª edição,São Paulo: Cortez, 2000.

DEY, Sandipan; ABRAHAM, Ajith; SANYAL, Sugata. An LSB Data Hiding Technique Using Prime Numbers. **Third International Symposium On Information Assurance And Security**, [S.L.], p. 3-7, ago. 2007. IEEE. http://dx.doi.org/10.1109/isias.2007.4299758.

DUARTE, Otto Carlos Muniz Bandeira; COSTA, Luís Henrique Maciel Kosmalski. **REDES DE COMPUTADORES II**: near field communication. Near Field Communication. 2013. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2013_2/nfc/seguranca.html. Acesso em: 22 jun. 2021.

FLOERKEMEIER, Christian; SCHNEIDER, Roland; LANGHEINRICH, Marc. Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. **Ubiquitous Computing Systems**, [S.L.], v. 3598, p. 214-231, mar. 2005. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11526858_17.
G. Bianchi, **“A comparative study of the various**

G. Padmavathi, and D. Shanmugapriya. **"A survey of attacks, security mechanisms and challenges in wireless sensor networks."** arXiv preprint arXiv: 0909.0576 (2009).
GAMAARACHCHI, Hasindu; GANEGODA, Harsha. **Power Analysis Based Side Channel Attack**. 2018. Disponível em: https://arxiv.org/abs/1801.00932. Acesso em: 23 jun. 2021.

GHIASABADI, Mansoureh; SHARIFI, Mohsen; OSATI, Nafiseh; BEHESHTI, Sareh; SHARIFNEJAD, Mona. **An Enhanced Routing Protocol for Wireless Sensor Networks. In: 2008 SECOND INTERNATIONAL CONFERENCE ON FUTURE GENERATION COMMUNICATION AND NETWORKING** (FGCN), 2., 2008, Tehran. 2008 Second International Conference on Future Generation Communication and Networking. Tehran, Iran: Ieee, 2008. p. 313-316.

GHILDIYAL, Sunil. ANALYSIS OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS SENSOR NETWORKS. **International Journal Of Research In Engineering And Technology**, [S.L.], v. 03, n. 22, p. 140-143, 25 jun. 2014. ESAT Publishing House. http://dx.doi.org/10.15623/ijret.2014.0322030.

GOMES, Lucas de Carvalho; ARAUJO, Marcos Seefelder de Assis; CAMPOS, Vinícius Silva. Negação de Serviço e Botnets: ataques de negação de serviço (denial of service - dos) e ataques distribuídos de negação de serviço (distributed denial of service - ddos). Ataques de Negação de Serviço (Denial of Service - DoS) e Ataques Distribuídos de Negação de Serviço (Distributed Denial of Service - DDoS). 2015. Disponível em: https://www.gta.ufrj.br/grad/15_1/dos/pages/dos.html#1. Acesso em: 22 jun. 2021.

GOYAL, V.; ABRAHAM, A.; SANYAL, S.; HAN, Sang Yong. The N/R one time password system. International Conference On Information Technology: Coding and Computing (ITCC'05) - Volume II, [S.L.], v. 1, n. 1, p. 2-7, maio 2005. IEEE. http://dx.doi.org/10.1109/itcc.2005.275.

GOYAL, V.; KUMAR, V.; SINGH, M.; ABRAHAM, A.; SANYAL, S..CompChall: addressing password guessing attacks. International Conference On Information Technology: Coding and Computing (ITCC'05) - Volume II, [S.L.], v. 1, n. 1, p. 2-6, maio 2005. IEEE. http://dx.doi.org/10.1109/itcc.2005.107.

GOYAL, Vipul; KUMAR, Virendra; SINGH, Mayank; ABRAHAM, Ajith; SANYAL, Sugata. A new protocol to counter online dictionary attacks. Computers & Security, [S.L.], v. 25, n. 2, p. 114-120, mar. 2006. Elsevier BV. http://dx.doi.org/10.1016/j.cose.2005.09.003.
GRAHAM, Camaeron. **Study: Wearable Technology & Preventative Healthcare**. 2014. Disponível em: https://technologyadvice.com/blog/healthcare/study-wearable-technology-preventative-healthcare/. Acesso em: 28 maio 2021.

J. SEN, **"A Survey on Wireless Sensor network Security"**, International Journal of Communications Network and Information Security, vol. 1, no. 2, (2009) August, pp. 59-82

JINDAL, Keshav; DALAL, Surjeet; SHARMA, Kamal Kumar. Analyzing Spoofing Attacks in Wireless Networks. **2014 Fourth International Conference On Advanced Computing & Communication Technologies**, Rohtak, v. 1, n. 1, p. 398-402, abr. 2014. IEEE. http://dx.doi.org/10.1109/acct.2014.46.

JVIANA. **IoT e a preocupação com a adoção da rede IPV6**. 2017. Disponível em: http://jviana.eti.br/portal/2017/12/12/iot-e-a-preocupacao-com-a-adocao-da-rede-ipv6/. Acesso em: 28 maio 2021.

KHOO, Benjamin. "**RFID as an enabler of the internet of things: issues of security and privacy."** Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011.
KINAST, Priscilla. O que é vírus de computador? 2019. Disponível em: https://www.oficinadanet.com.br/seguranca/27318-o-que-e-um-virus-de-computador. Acesso em: 23 jun. 2021

LU TAN E NENG WANG, **Future internet: The Internet of Things**, 2010 3ª Conferência Internacional sobre Teoria e Engenharia de Computação Avançada (ICACTE), 2010, pp. V5-376-V5-380, doi: 10.1109 / ICACTE.2010.5579543.
M. Saxena, **"Security in Wireless Sensor Networks-A Layer based classification"**, Technical Report, Center for Education and Research in Information Assurance & Security-CERIAS, Purdue University. pages.cs. wisc.edu/~msaxena/papers/2007-04-cerias.pdf, (2007).

M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, **"A Survey on Wireless Sensor Networks Security"**, SETIT, (2007).
magazine, IEEE 40.8 (2002): 102-114.

MAGRANI, Eduardo. **A Internet das Coisas**. Rio de Janeiro: Rio Editora, 2018.
MARCONI, M.A. & LAKATOS, E.M. **Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados**. 6ª edição, São Paulo: Atlas, 2007.

NÉRIO, A (2003):**Wireless** – Disponível em:
Networks", http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf, (2008).
RAYES, A.; SALAM, S. **Internet of things-from hype to reality: The road to digitization. Internet of Things From Hype to Reality: The Road to Digitization**, Springer International Publishing, Cham, v. 32, n. 8, p. 1–328, 2016. ISSN 0970034X.
Revista de Sistemas e Computação, Salvador, v. 7, n. 2, p. 365-384, jul./dez. 2017

ROLF CLAUBERG. **RFID and Sensor Networks: From Sensor/Actuator to Business Application**, RFID Figure 3 – Security Issues in RFID 6 Workshop, University of St. Gallen, Switzerland,September 27, 2004.

ROY, Bibhash; BANIK, Suman; DEY, Parthi; SANYAL, Sugata; CHAKI, Nabendu. Ant Colony based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services. **Cisjournal.** S.I, p. 10-14. jan. 2012. Disponível em: https://www.researchgate.net/publication/216713708_Ant_Colony_based_Routing_for_Mobile_Ad-Hoc_Networks_towards_Improved_Quality_of_Services. Acesso em: 26 jun. 2021.

SACHDEVA, Ratika; SINGLA, Aashima. **Survey on Privacy Issues and Security Attacks in Wireless Mesh Networks**. International Journal Of Advanced Research In Computer Science And Software Engineering. Punjab, India, p. 1-4. abr. 2013.

SANTOS, Carlos Cesar; SALES, Jefferson David de Araújo. O Desafio da Privacidade na Internet das Coisas. **Revista Gestão.Org**, Recife, v. 13, p. 282-290, 09 maio 2016.
security approaches used in wireless sensor networks,"International Journal of Advanced Science and Technology, vol. 17, (2010) April, pp. 31-44.

Sen, Jaydip. **"Security and privacy challenges in cognitive wireless sensor networks."** arXiv preprint arXiv: 1302.2253 (2013).

SHEN, Guicheng, and BINGWU Liu. **"The visions, technologies, applications and security issues of Internet of Things."** E-Business and E-Government (ICEE), 2011 International Conference on. IEEE,2011.

SMITH, Craig; MIESSLER, Daniel. **Internet of Things Research Study**. 2014. HP Fortify On Demand. Disponível em: https://d-russia.ru/wp-content/uploads/2015/10/4AA5-4759ENW.pdf. Acesso em: 05 abr. 2021.

T. A. Zia, **"A Security Framework for Wireless Sensor**
Technology Advice Company http://technologyadvice.com/blog/healthcare/study-wearabletechnology-preventative-healthcare/ setembro, 2017.
TRENTINI, M.; PAIM, L. **Pesquisa em Enfermagem. Uma modalidade convergente-assistencial.** Florianópolis: Editora da UFSC

VASUDEVAN, R.A.; ABRAHAM, A.; SANYAL, S.; AGRAWAL, D.P.. Jigsaw-based secure data transfer over computer networks. International Conference On Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., [S.L.], v. 1, n. 1, p. 2-5, abr. 2004. IEEE. http://dx.doi.org/10.1109/itcc.2004.1286416.

XIAO, Qinghan; GIBBONS, Thomas; LEBRUN, Hervé. **RFID Technology, Security Vulnerabilities, and Countermeasures**. 2009. Disponível em: https://www.intechopen.com/books/supply_chain_the_way_to_flat_organisation/rfid_technology__security_vulnerabilities__and_countermeasures. Acesso em: 30 maio 2021.