TECNOLOGIAS EMERGENTES EM IOT: RSSF, RTLS, RFID

CONCEITOS E APLICAÇÕES PARA CIDADES INTELIGENTES E INDÚSTRIA 4.0

ipt INSTITUTO DE PESQUISAS TECNOLÓGICAS

TECNOLOGIAS EMERGENTES EM IOT: RSSF, RTLS, RFID

CONCEITOS E APLICAÇÕES PARA CIDADES INTELIGENTES E INDÚSTRIA 4.0

AUTORES:

ALESSANDRO SANTIAGO DOS SANTOS

LEANDRO AVANÇO

MATHEUS JACON PEREIRA

Av. Prof. Almeida Prado, 532 - Cidade Universitária - Butantã
05508-901 - São Paulo - SP ou Caixa Postal 0141 - 01064-970 - São Paulo - SP
Telefone (11) 3767-4000 - Fax (11) 3767-4099
www.ipt.br
ipt@ipt.br

GOVERNADOR
João Agripino da Costa Doria Junior

SECRETARIA DE DESENVOLVIMENTO ECONÔMICO
Patricia Ellen da Silva

DIRETOR PRESIDENTE DO IPT
Jefferson de Oliveira Gomes

DIRETORA FINANCEIRO, ADMINISTRATIVO, PESSOAS E SISTEMAS
Flávia Gutierrez Motta

DIRETOR DE OPERAÇÕES
Mário Boccalini Júnior

DIRETORA DE INOVAÇÃO E NEGÓCIOS
Zehbour Panossian

DIRETORA DO CENTRO DE TECNOLOGIA DA INFORMAÇÃO, AUTOMAÇÃO E MOBILIDADE (CIAM)
Maria Rosilene Ferreira

DIAGRAMAÇÃO, GRÁFICOS, ILUSTRAÇÕES E CAPA
Vinicius Franulovic

REVISÃO DE TEXTO, REFERÊNCIAS E CITAÇÕES BIBLIOGRÁFICAS
Lígia Micas
Edna Baptista dos Santos Gubito
Denise Oliveira de Paula

Esta publicação contém conteúdo de pesquisa apoiada pela FAPESP. Processo nº 2017/50343-2, Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).
As opiniões, hipóteses e conclusões ou recomendações expressas neste material são de responsabilidade dos autores e não necessariamente refletem a visão da FAPESP.

Dados internacionais de catalogação na publicação (CIP)
(Câmara Brasileira do livro, SP, Brasil)

Santos, Alessandro Santiago dos
Tecnologias emergenciais em IOT [Livro eletrônico] : RFFF, RTLS, RFID : conceitos e aplicações para cidades inteligentes e indústria 4.0 /
Alessandro Santiago dos Santos, Leandro Avanço, Matheus Jacon Pereira. -- 1. ed. -- São Paulo : IPT - Instituto de Pesquisas Tecnológicas do Estado de São Paulo, 2020. -- (IPT Publicação ; 3003 / coordenação Instituto de Pesquisas Tecnológicas do Estado de São Paulo)
4 Mb; PDF

Bibliografia
ISBN 978-65-5702-000-5

1. Aparelhos e dispositos eletrônicos
2. Circuitos elétricos 3. Dispositivos eletromecânicos 4. Indústrias 5. Dispositivos eletrônicos - Indústrias
6. Inovação tecnológica 7. Tecnologias da informação e comunicação I. Avanço, Leandro. II. Pereira, Matheus Jacon. III. Título IV. Série

20-35465 CDD-621.3815

Índices para catálogo sistemático:

1. Dispositivos eletônicos : Engenharia eletrônica
621.3815
Maria Alice Ferreira - Bibliotecária - CRB-87964

TECNOLOGIAS EMERGENTES EM IOT: RSSF, RTLS, RFID

CONCEITOS E APLICAÇÕES PARA CIDADES INTELIGENTES E INDÚSTRIA 4.0

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Desenvolvimento Econômico

ipt INSTITUTO DE PESQUISAS TECNOLÓGICAS

FAPESP

Fundação de Apoio ao Instituto de Pesquisas Tecnológicas Fipt

São Paulo
2020

SUMÁRIO

INTRODUÇÃO

As tecnologias da informação e comunicação têm impulsionado vários segmentos da sociedade na era digital, proporcionando diferentes perspectivas de atuação nos processos industriais e na melhoria da qualidade de vida dos cidadãos, assim como novas formas de negócios. Essas mudanças vêm sendo categorizadas como uma transformação digital empregada nos modelos tradicionais de trabalho, com geração de valor para os negócios, sejam eles nas indústrias, cidades ou empresas.

O desenvolvimento da indústria eletrônica acompanha esse avanço, elaborando novos dispositivos, tecnologias ou funcionalidades para atingir mais eficiência ou viabilizar a entrada em novos mercados com produtos inovadores.
A evolução dos smartphones e o posterior advento da Internet das Coisas (IoT, do inglês Internet of Things) proporcionaram um novo olhar para a indústria de dispositivos eletrônicos.

Um esforço nacional conduzido pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) criou mecanismos para a elaboração do plano nacional de IoT, que pretende estabelecer os cenários e prioridades brasileiras para o contexto de IoT. Nesse plano é mencionada a Internet das Coisas que, em sua definição mais ampla, engloba todos os objetos que transmitem informações através da internet, como computadores, tablets e smartphones. No entanto, a definição mais estrita, e comumente aceita, considera apenas os objetos capazes de detectar informações por sensores e transmiti-las, assim como atuar sem a presença constante de intervenção humana (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 2016a).
De forma geral, IoT é:

> *Rede de todos os objetos que se comunicam e interagem de forma autônoma via internet, permitindo o monitoramento e gerenciamento desses dispositivos via software para aumentar a eficiência de sistemas e processos, habilitar novos serviços e melhorar a qualidade de vida das pessoas. (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 2016a).*

A aplicação de IoT está diretamente relacionada com novos movimentos como as Cidades Inteligentes e a Indústria 4.0, sendo ela um elemento presente e atuante na perspectiva desses dois movimentos tecnológicos. Inclusive o plano nacional de IoT incluiu as indústrias e as cidades brasileiras como prioridades, constituindo áreas em que a IoT irá propiciar um maior impacto positivo.

Quando analisamos o contexto de Cidades Inteligentes, notamos que este é um movimento recente, que detém definições e objetivos variados.
Um estudo da União Internacional de Telecomunicações (ITU-T) realizou um levantamento mundial de definições sobre Cidades Inteligentes e encontrou mais de 100 definições. A partir delas, definiu um conceito sobre cidade inteligente e sustentável (INTERNATIONAL TELECOMMUNICATION UNION, 2015), como sendo:

> *Uma cidade sustentável e inteligente é uma cidade inovadora que usa tecnologias de informação e comunicação (TICs) e outros meios para melhorar a qualidade de vida, a eficiência da operação e dos serviços urbanos e a competitividade, garantindo que atenda às necessidades das gerações presentes e futuras com respeito aos aspectos econômicos, sociais, ambientais e culturais. (INTERNATIONAL TELECOMMUNICATION UNION, 2015).*

Quando analisamos o contexto da Indústria 4.0 também é verificado um esforço do governo brasileiro em conceituar e analisar as perspectivas da manufatura avançada no país. Estudo dos ministérios da Indústria, Comércio Exterior e Serviços e da Ciência, Tecnologia, Inovações e Comunicações, que resultou de consulta pública, apresentou quais seriam as prioridades e aptidões brasileiras no contexto da Indústria 4.0 Ministério da Indústria, Comércio Exterior e Serviços (2016b). Cabe salientar que, de forma geral, as definições de Indústria 4.0 (conceito alemão) e manufatura avançada (conceito americano), ainda como o da quarta revolução industrial, se equivalem, mesmo com vários autores discutindo as diferentes minúcias. No referido estudo é mencionada a seguinte definição de Indústria 4.0:

> *[...] redes globais que incorporarão suas máquinas, sistemas de armazenagem e instalações de produção em Sistemas Ciberfísicos (CPS), que serão capazes de trocar informações de forma autônoma entre seus componentes e variáveis externas, desencadeando ações e controlando o sistema de produção de forma independente. (ACATECH, 2013; GERMANY TRADE & INVEST INDUSTRIE, 2013; MCKINSEY GLOBAL INSTITUTE, 2015; DELOITTE GLOBAL, 2016 apud MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS, 2016b).*

Considerando os cenários de Cidades Inteligentes e Indústria 4.0, a aplicação de IoT torna-se um fator determinante para viabilizar os dois conceitos em questão. Diversas tecnologias emergentes vislumbram perspectivas de uso nesse contexto, a exemplo das Redes de Sensores Sem Fio (RSSF), da Identificação por Radiofrequência (RFID) e dos Sistemas de Localização em Tempo Real (RTLS). Neste trabalho são apresentadas as três tecnologias mencionadas e suas implicações em Cidades Inteligentes e Indústria 4.0, assim como uma análise de segurança com o uso de RFID, RSSF e RTLS nesses cenários.

Vale a pena destacar que o subtítulo do livro - **Transpondo a camada física para aplicações em Cidades Inteligentes e Indústria 4.0** - realça os pontos tecnológicos descritos neste trabalho, em que o principal foco é conectar o ambiente físico (chão de fábrica, meio ambiente, meios de transporte etc.) por meio de tecnologias de IoT, que transpõem os fenômenos que ocorrem na vida real, transformando-os em sinais digitais, os quais podem ser consumidos e interpretados por ferramentas computacionais. Outra interpretação, mais técnica, pode ser obtida pela analogia com as camadas de rede padronizadas do modelo de referência da ISO (**Figura 1**). Nela verificamos a separação lógica, em que a primeira camada é responsável por transpor os dados digitais para serem encaminhados para camadas superiores até a camada de aplicação, na qual a questão funcional é percebida.

Figura 1. Modelos de referência ISO das camadas de rede.

Fonte: Tanenbaum e Wetherall (2011, tradução nossa).

O CONTEXTO DE RSSF EM IOT

Podemos considerar uma definição simplificada de Rede de Sensores Sem Fio (RSSF) como sendo um conjunto de nós sensores interligados. Esses nós sensores são pequenos dispositivos eletrônicos, geralmente consistindo em um microcontrolador, uma unidade de rádio de curto alcance e um ou mais transdutores atuando como sensores (ROSALES; GARCIA; SANCHEZ, 2009).

Na literatura técnica científica, alguns outros tipos de redes sem fio podem gerar confusões de interpretação e enquadramento. Quando se trata de RSSF, também conhecida como Wireless Sensor Networks (WSN), é comum encontrar autores (HADI, 2017) que consideram as RSSF como subtipo de Mobile Ad hoc NETworks (MANET). De forma geral, uma MANET é composta por nós móveis que interagem diretamente sem intermediários como gateways (sorvedouros), utilizando de modelos de rede autoconfigurável e adaptável ao contexto de mobilidade dos nós. Já as RSSF utilizam um gateway como canal de encaminhamento dos dados para um repositório centralizado de armazenamento e processamento.

Tanto RSSF como MANET são utilizadas por soluções de IoT: desde o advento do conceito essas redes tiveram uma rápida evolução, principalmente com a incorporação de diferentes formas de comunicação. Como exemplo, lembramos que as redes Low Power Wide Area Network (LPWAN), entre elas LoRA WAN, SIGFOX, Nb-IoT, foram concebidas e potencializaram o uso desses dispositivos, uma vez que possibilitam um custo de implementação menor em relação à utilização de modelos tecnológicos de comunicação tradicionais, cobrindo maior área territorial. Essas tecnologias de comunicação são principalmente aplicáveis a RSSF, uma vez que os nós se comunicarão com um gateway LPWAN.
O **Quadro 1** apresenta as principais características e aplicações para MANET e RSSF.

Este material se concentrará no contexto apenas de RSSF, no entanto, mais detalhes sobre MANETS e diferenças com relação às RSSF podem ser vistos em (LOO; MAURI; ORTIZ, 2012).

O CONTEXTO DE RFID EM IOT

O conceito original para a Internet das Coisas foi introduzido pelo Massachusetts Institute of Technology (MIT), em 1999, utilizando o código eletrônico do produto como forma de identificação de um objeto. Desde então, a visão a respeito de tal conceito se modificou, tornando-se mais ampla, mas a associação com Identificação por radiofrequência (RFID) ficou diretamente ligada ao contexto.

De forma geral, a identificação por radiofrequência pode ser definida como um sistema em que circuitos eletrônicos são anexados a objetos a serem identificados e que utilizam radiofrequência como meio de comunicação.

Quadro 1. Comparação entre MANET e RSSF.

REDES	CARACTERÍSTICA	APLICAÇÕES TRADICIONAIS
MANET	• Rápida e de fácil implantação, com autoconfiguração. • Autônoma, não há necessidade de infraestrutura existente. • Nós móveis, com a topologia podendo ser muito dinâmica. • Nós atuando como host e roteador. • Energia, segurança e recursos de computacionais limitados. • Pode ser conectada a redes externas ou pode ser uma rede autônoma. • Comunicação direta entre os nós	• Comunicação em campo de batalha. • Busca e salvamento. • Aquisição de dados por robô. • Redes veiculares.
Redes de Sensores sem Fio	• Tolerantes a falhas. • Pode haver mobilidade dos nós, com uma topologia de rede dinâmica. • Maior escalabilidade de implantação. • Heterogeneidade de nós. • Capacidade de suportar condições ambientais adversas. • Operação desacompanhada. • Facilidade de uso e implantação em larga escala. • Dificuldade com consumo de energia. • Comunicação entre os nós apenas para encaminhamento do dado até o gateway.	• Monitoramento ambiental. • Monitoramento sísmico e estrutural. • Rastreamento de objetos. • Automação industrial. • Experiências de campo. • Aplicações biomédicas. • Monitoramento de tráfego. • Detecção de fogo.

Ao longo dos últimos anos, o uso de RFID tem aumentado em aplicações nos mais diversos setores de negócio, de sistemas logísticos a controle de acesso Bhatt e Glover (2006). Boas práticas de implementação passam pela adoção progressiva de RFID, a qual está dividida em cinco eras:

1. Proprietária (primeira era): foi iniciada com a redução do tamanho e dos custos da produção de transistores, o que permitiu o desenvolvimento de tags RFID pelas próprias empresas, para seu próprio uso no controle de seus produtos em estoque. Na ausência de um padrão, não havia condições para integração das soluções;

2. Regulamentação (segunda era): teve início quando as empresas necessitaram controlar os produtos fora do ambiente das empresas. As tags identificavam contêineres em transporte. Nesta era ocorreu o desenvolvimento de padrões para adoção universal da tecnologia. A implantação ainda era vista como um custo adicional ao processo pelas empresas;

3. RFID nas Empresas (terceira era): o marco foi a inclusão do RFID nos processos produtivos das empresas, com a identificação efetuada cada vez mais item a item, envolvendo o controle do processo de produção. A produção em escala de tags diminuiu ainda mais o custo de produção;

4. RFID nas Indústrias (quarta era): a consolidação dos requisitos de segurança e privacidade marca esta era. Em todos os níveis da cadeia de produção, os produtos são identificados e acompanhados. As informações dos produtos são utilizadas pelas áreas de negócios de forma estratégica. Além disso, sensores utilizando RFID e outras tecnologias começaram a coletar informações do ambiente para inclusão e melhoria dos processos das empresas;

5. Internet das Coisas (quinta era): inicia-se com a adoção massiva da tecnologia RFID e demais tecnologias ubíquas, quando empresas privadas poderão oferecer serviços para seus clientes de forma rápida e inteligente. O poder público poderá prover serviços para a população de forma eficiente, baseando-se em informações obtidas automaticamente pelos cidadãos. As tecnologias ubíquas, como RFID, não serão mais percebidas, assim como ocorre com a energia elétrica.

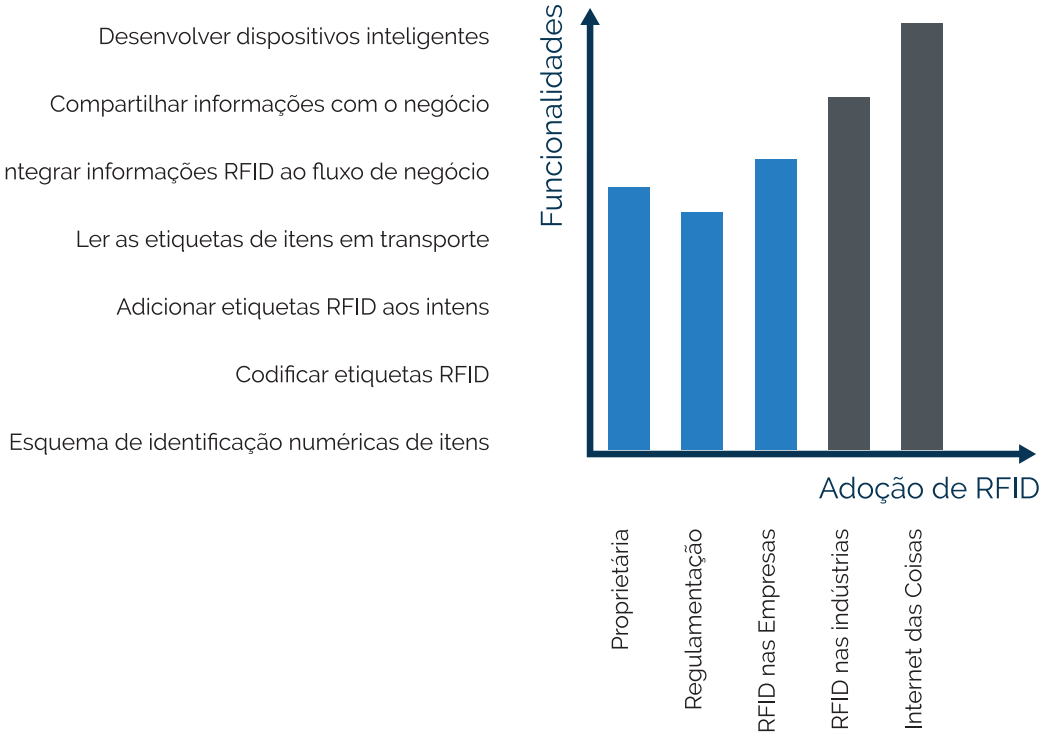
A **Figura 2** ilustra as eras do RFID de acordo com seu grau de adoção. As barras verticais em cinza mais escuro indicam as eras já superadas.

O cenário atual das empresas e das implementações com RFID indica que as eras Proprietária e de Regulamentação já foram superadas. Existem iniciativas que indicam uma transição ocorrendo entre a era RFID nas Empresas e a era RFID na Indústria, em que empresas já possuem a tecnologia implantada e definida em seus processos produtivos. Além disso, o planejamento e a instalação de sensores para coletar informações, como ruído, temperatura e velocidade do tráfego de veículos, pelas indústrias e poder público demonstram o início da era da Internet das Coisas. Esse início mostra a ocorrência simultânea das eras RFID nas Indústrias e Internet das Coisas.

O CONTEXTO DE RTLS EM IOT

O conceito de Internet das Coisas está cada vez mais presente na sociedade e o número de sensores instalados ao redor do mundo vem crescendo rapidamente, os quais empregam as mais variadas tecnologias (MULANI; PINGLE, 2016).

Figura 2. Eras do RFID



Fonte: Bhatt e Glover (2006, tradução nossa).

Nesse contexto de IoT, a geolocalização é um dos temas atualmente discutidos devido a sua importância para fins comerciais, segurança pública, medicina e indústria. Por exemplo, na área comercial, uma loja de departamentos poderia reconhecer a localização exata de um cliente, e com isso identificar o setor em que este se encontra (roupas, casacos ou calçados). Com essas informações, um aplicativo para smartphone poderia mostrar promoções, propagandas e descontos de maneira exclusiva (SILVA, 2016).

Na área da medicina, hospitais podem determinar a localização de médicos, enfermeiros, pacientes, familiares, medicamentos e equipamentos. Na indústria, a localização também encontra suas aplicações, entre elas rastrear equipamentos e ferramentas importantes do chão de fábrica. Atualmente, percebe-se, portanto, uma crescente automatização nos diversos processos produtivos (MENEGOTTO, 2015).

Quando se trata da localização outdoor[1] , o Sistema de Posicionamento Global (GPS, do inglês *Global Positioning System*) é frequentemente utilizado para localizar objetos. Entretanto, esta tecnologia não é apropriada para rastreamento indoor, pois requer linha de visão direta entre o objeto e os satélites.
Para a localização *indoor2* existem tecnologias que utilizam radiofrequência para realizar a detecção da posição dos objetos (MENEGOTTO, 2015). São elas: Wi-Fi, Bluetooth,

---

1- Outdoor: Ambiente externo ao ar livre. No contexto deste trabalho, ambientes com linha de visão direta aos satélites do sistema GPS.
2- Indoor: Ambiente interno. No contexto deste trabalho, ambientes sem linha de visão direta aos satélites do sistema GPS.

ZigBee, UWB e RFID. O RFID já está inserido em diversos setores: manufatura, varejo, aviação, indústria e transportes Leal et al. (2014). Devido ao seu baixo custo e à presente inserção em diferentes setores, esta tecnologia pode ser impulsionadora das aplicações que demandam rastreamento indoor de objetos, com a perspectiva da IoT.

O próximo passo na evolução da geolocalização passa, portanto, pela localização indoor: é nesse contexto que surge o conceito de RTLS (do inglês Real-Time Locating System). Neste trabalho são apresentadas as diversas tecnologias que podem ser utilizadas para aplicar o RTLS, no entanto, o foco está no uso de RTLS com a tecnologia de RFID, inclusive com a apresentação de experimentos de aplicação em ambiente industrial, logístico e comercial.

O CONTEXTO DE SEGURANÇA EM IOT

A exemplo do que ocorreu com outras tecnologias no passado, a preocupação com segurança não é normalmente levada em consideração em seus primeiros estágios de implementação, como foi, lamentavelmente, o caso do protocolo TCP/IP. A exploração de vulnerabilidades demandou ações e contramedidas para que seu uso não fosse prejudicado.

Os equipamentos utilizados para sistemas de IoT, como RFID e RSSF, não possuem recursos computacionais abundantes. Essa limitação de recursos nos dispositivos traz consequências à implementação dos mecanismos de proteção, fazendo com que as medidas de segurança tenham que ser adaptadas para utilização nestes equipamentos (FINKENZELLER, 2010). Além disso, o aumento da utilização de RFID traz preocupações com questões de segurança e privacidade, conhecidas e exploradas em outras tecnologias, que inicialmente não foram muito exploradas em RFID (TAGRA; RAHMAN; SAMPALL, 2010). De forma similar os sistemas RSSF são instalados em locais facilmente acessíveis, deixando-os susceptíveis acessos indevidos e vandalismo (KHATAWKAR et al., 2013).

Esses cenários motivaram a criação de um capítulo dedicado à questão de segurança sobre IoT, em que serão apresentadas as principais vulnerabilidades de RFID e sua associação com quesitos como: confidencialidade, integridade e disponibilidade.

REFERÊNCIAS

BHATT, H.; GLOVER, B. RFID Essentials. USA: O'Reilly, 2006. 276 p.

FINKENZELLER, K. RFID Handbook: fundamentals and applications. Munich, Germany: Wiley, 2010.

HADI, T. H. MANET and WSN: what makes them different?. International Journal of Computer Networks and Wireless Communications, v. 7, n. 6, p. 23-28, Dec. 2017./

INTERNATIONAL TELECOMMUNICATION UNION. Smart sustaninable cities: an analysis of definitions. Geneve: ITU, 2015.

KHATAWKAR, P. et al. Wireless sensor network security threats. In: INTERNATIONAL CONFERENCE ON ADVANCES IN RECENT TECHNOLOGIES IN COMMUNICATION AND COMPUTING, 5., 2013, Bangalore. Proceedings... Piscataway: IEEE, 2013. v. 35, p. 131–135. Disponível em: <http://dl.acm.org/citation.cfm?id=168607%5Cnhttp://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1039518%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0%5Cnhttp://books.google.com/books?hl=en&lr=&id=pA2XUtdwewAC&oi=fnd>. Acesso em: 3 mar. 2019.

LEAL, A. G. et al. Integrated environment for testing IoT and RFID technologies applied on intelligent transportation system in Brazilian scenarios. In: IEEE Brasil RFID, 2014, São Paulo. Proceedings... Piscataway: IEEE, 2014. p. 22–24. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7128956>. Acesso em: 3 out. 2018.

LOO, J.; MAURI, J. L.; ORTIZ , J. H. Mobile ad hoc networks: current status and future trends. Boca Raton: CRC Press, 2012.

MENEGOTTO, J. L. Sensoriamento da edificação: um sistema de localização baseado em Beacons BLE. In: ENCONTRO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO NA CONSTRUÇÃO, 7., 2015, Recife. Anais... Rio de Janeiro: Blucher, 2015. p. 264–274.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. Consulta Pública: identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil. Brasília: MDIC, 2016a.

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Perspectivas de especialistas brasileiros sobre manufatura avançada no Brasil: um relato de workshops realizados em sete capitais brasileiras em contraste com as experiências internacionais. Brasília: MDIC, 2016b.

MULANI, T. T.; PINGLE, S. V. Internet of things. International Research Journal of Multidisiplinary Studies, v. 2, n. 1, p. 1-4, 2016.

ROSALES, M. S.; GARCIA, G.; SANCHEZ, G. D. Efficient message authentication protocol for WSN. Wseas Transaction on Computers, v. 8, n. 6, p. 895-904, June, 2009.

SILVA. R. B. C. Interface homem-máquina para carro elétrico baseada em bluetooth low energy. 2016. Dissertação (Mestrado em Engenharia de Telecomunucações e Informática) - Escola de Engenharia. Braga/Guimarães, Universidade do Minho, Portugal, 2016.

TANENBAUM, A. S.; WETHERALL, D. J. Redes de computadores. 5. ed. São Paulo: Prentice Hall, 2011.

TAGRA, D.; RAHMAN, M.; SAMPALLI, S. Technique for preventing DoS attacks on RFID systems. In: CONFERENCE ON SOFTWARE, TELECOMMUNICATIONS AND COMPUTER NETWORKS (SoftCOM), 18., 2010, Damatia, Croatia. Proceedings... Piscataway: IEEE, 2010. p. 6–10, 2010. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5623669>. Acesso em: 4 abr. 2019.

1 RFID: O PRECURSOR DE IOT

As primeiras abordagens do termo IoT estavam diretamente relacionadas ao uso de identificação de itens por meio de radiofrequência, denominada RFID. Com o passar do tempo, a IoT evoluiu com convergência e inúmeras possibilidades de comunicação e usos. No entanto, a associação de RFID como uma tecnologia habilitadora de IoT sempre estará presente em vários cenários, principalmente em processos nos quais a rastreabilidade de itens reais pode ser um requisito para o negócio.

Este capítulo caracteriza a tecnologia RFID, assim como as perspectivas de usos e aplicações nos cenários de Internet das Coisas no contexto de Cidades Inteligentes e Indústria 4.0.

1.1 DEFINIÇÕES E COMPONENTES

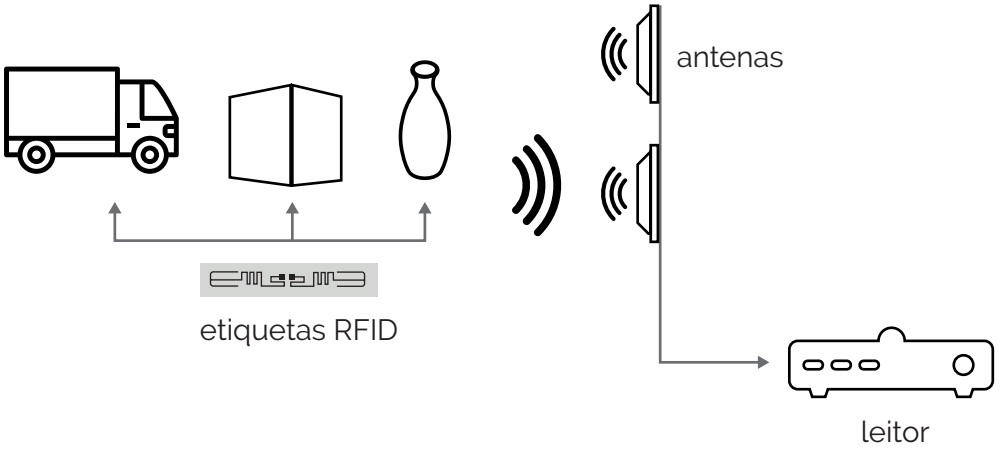
Segundo Bhatt e Glover (2006), o RFID pode ser definido como um sistema de identificação em que circuitos eletrônicos são anexados a objetos que se desejam identificar e que utilizam radiofrequência para a comunicação.

A utilização de radiofrequência para identificação foi utilizada pela primeira vez na Segunda Guerra Mundial pela Inglaterra. Foi desenvolvido um sistema com transmissor e receptor, instalado nos aviões de combate, que alterava o comportamento de sua resposta ao sistema de radar. Quando um avião inimigo passava pelo campo de atuação do radar, as imagens desses aviões não se alteravam. Por outro lado, quando um avião amigo era detectado pelo sistema de radar, as imagens na tela do radar pulsavam. Desta forma, a identificação de aviões amigos e inimigos tornou-se possível. Este sistema foi nomeado como Identificação de Amigo ou Inimigo (IFF, do inglês *Identification Friend or Foe*).

Os Sistemas RFID são compostos basicamente por três dispositivos: a etiqueta anexada ao objeto que se deseja identificar, que pode ser animado ou inanimado; o leitor, dispositivo responsável por detectar a presença da etiqueta e interrogá-la para obter as informações armazenadas do objeto; e a antena, um dispositivo passivo que é utilizado pelo leitor para transmitir os sinais de radiofrequência. A **Figura 3** demonstra um sistema RFID Básico.

A seguir será descrito em detalhes cada um dos dispositivos.

Figura 3. Sistema RFID Básico.



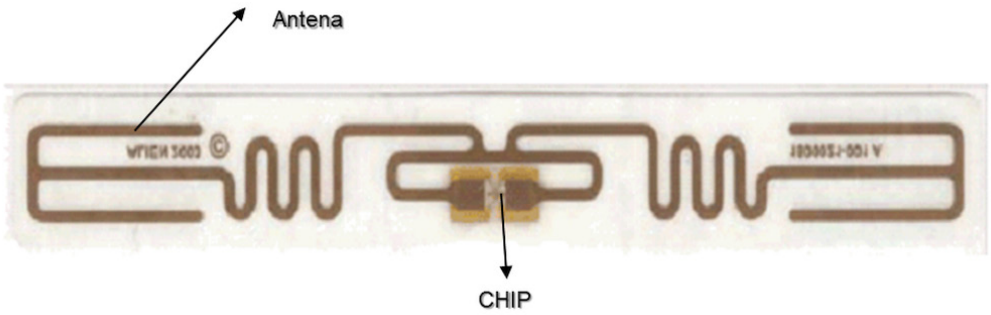
Fonte: Elaborado pelos autores.

1.1.1 ETIQUETAS

As etiquetas RFID são dispositivos eletrônicos responsáveis por identificar os objetos em que estão anexadas. Elas podem ser constituídas de uma antena, um microchip e uma fonte de energia, não sendo obrigatória a existência de todos esses elementos, com exceção da antena, que deve existir na mais simples etiqueta RFID (**Figura 4**).

O microchip é responsável por modular e demodular o sinal recebido pela antena, processar os comandos recebidos e responder as requisições desses comandos. Além disso, possui memória interna para armazenar as informações referentes ao objeto identificado. No entanto, o seu processamento é limitado devido a suas características construtivas, sendo que sua capacidade de armazenamento pode chegar a 1 kB (BHATT; GLOVER, 2006).
A antena, único item obrigatório em uma etiqueta, é especificada de acordo com o uso e a frequência de operação, conforme **Tabela 1**.

Figura 4 – Etiqueta RFID.



Fonte: Elaborado pelos autores.

A classificação das etiquetas é feita conforme sua fonte de energia, podendo ser denominadas como passivas, semipassivas e ativas.

Tabela 1. Características das principais faixas de frequência RFID.

FAIXA DE FREQ.	BANDA	ALCANCE	VANTAGENS	DESVANTAGENS	APLICAÇÕES
LF	125-134 kHz	Menos de 0,5 metros	Boa operação próxima a metais e água.	Curto alcance de leitura.	Rastreamento de animais, controle de acesso, autenticação de produtos, bagagens em linhas aéreas, smart cards e bibliotecas.
HF	13,56 MHz	Menos de 1 metro	Baixo custo das etiquetas e bom funcionamento.	Necessita de leitores com potência elevada.	Identificação de itens, bagagens em linhas aéreas, smart cards e bibliotecas.
UHF	860-960 MHz	Até 9 metros	Baixo custo das etiquetas com tamanho reduzido.	Não opera bem próxima a metais e líquidos.	Controle de fornecimento logístico, cobrança automática veicular e pedágio eletrônico.
Microondas	2,45 e 5,8 GHz	Acima de 10 metros	Alta velocidade de transmissão de dados.	Não opera bem próxima a metais e líquidos.	Controle de fornecimento logístico, cobrança automática veicular e pedágio eletrônico.

Fonte: Hessel et al. (2013).

•**Passivas:** as etiquetas passivas possuem a característica de não necessitarem de baterias ou outras fontes de energia interna para seu funcionamento. Elas somente precisam estar presentes no campo eletromagnético da antena do leitor RFID, que gera uma corrente elétrica no circuito eletrônico interno da etiqueta, o qual deve fornecer energia suficiente para habilitar suas funções de leitura, escrita e transmissão. Pelo fato de aproveitarem a energia advinda da transmissão do leitor, sua potência é limitada e, consequentemente, seu alcance também, que geralmente se limita a 9 metros entre antena do leitor e etiqueta;

•**Semipassivas:** possuem uma tecnologia intermediária entre as passivas e ativas. As etiquetas passivas caracterizam-se por possuírem uma bateria interna de baixo

custo para alimentar os circuitos internos, que não é utilizada pelo transmissor, e só entram em funcionamento quando irradiadas pela antena de um leitor RFID, portanto sua forma de comunicação com o leitor é análoga às passivas. Como estas não utilizam a energia do campo eletromagnético fornecido pelo leitor para a operação do circuito interno, há uma sobra de energia para a resposta ao leitor. Logo, elas são menos suscetíveis a interferências e alcançam maiores distâncias de leitura quando comparadas às etiquetas passivas;

•**Ativas:** caracterizam-se por possuir um transmissor e uma bateria interna para alimentar a transmissão. Por isso, podem melhorar de maneira significativa o alcance da comunicação entre leitor e etiqueta. Geralmente são utilizadas em soluções mais complexas devido a sua maior capacidade de armazenamento, processamento e alcance de transmissão. Porém, são mais caras e necessitam de trocas periódicas da bateria interna, como as etiquetas semipassivas.

1.1.2 ANTENA

A antena conduz a comunicação entre o leitor e a etiqueta RFID, além de determinar a área de cobertura de um sistema RFID, de acordo com suas características de desempenho, alcance e configuração.

Os leitores suportam, comumente, até quatro antenas, e a principal limitação do número de antenas em uma solução RFID é a perda de sinal nos cabos de conexão. Na maior parte das instalações as antenas distam no máximo 2 metros dos leitores. Distâncias maiores são possíveis, porém devem ser utilizadas técnicas para amenizar as perdas de potência (HESSEL et al., 2013).

As antenas podem ser de leitura linear ou circular:

•**Antena de leitura linear:** oferece um maior alcance e leitura, no entanto a orientação adequada entre etiqueta e antena é fundamental para o bom funcionamento. Portanto ela só é recomendada em soluções em que as etiquetas tiverem seu posicionamento fixo e controlado;

•**Antena de leitura circular:** possui menor alcance de leitura que as antenas lineares, porém a orientação entre etiqueta e antena não interfere nos resultados. Logo, é indicada para utilização em soluções em que a orientação das etiquetas não é conhecida ou controlada.

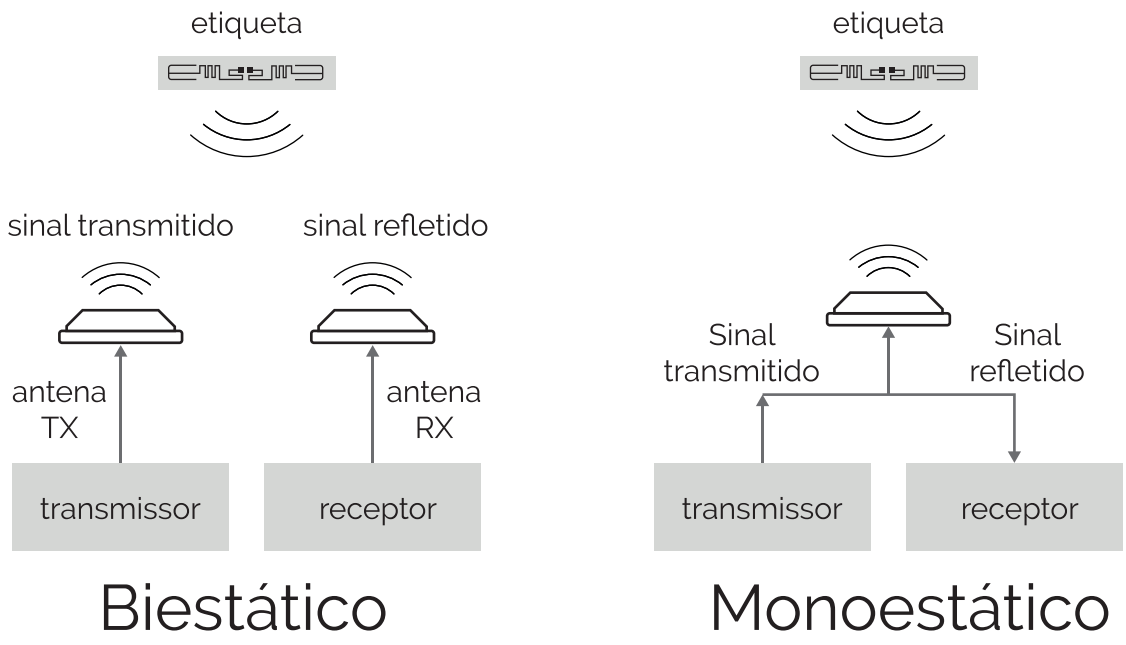
Existem duas configurações de implementação para as antenas:

1. Biestática: uma antena é usada para a transmissão e outra para a recepção;
2. Monoestática: quando a mesma antena realiza transmissão e recepção.

A Figura 5 demonstra o funcionamento dos dois tipos de configuração.

1.1.3 LEITOR

Figura 5. Tipos de configuração para antenas RFID.



Fonte: Elaborado pelos autores.

O leitor é o responsável por interrogar as etiquetas e processar a resposta recebida. É constituído de uma ou mais antenas, um controlador e uma fonte de energia. Pode possuir desde um controlador simples, similar ao utilizado nas etiquetas e presente em equipamentos portáteis, até um controlador mais complexo, similar ao utilizado em microcomputadores e servidores de aplicação.

Os tipos mais comuns de leitores são:
• **Portáteis:** possuem grande mobilidade e são utilizados em locais com condições climáticas extremas e de difícil acesso;
• **De Posição Fixa:** são instalados em locais específicos. Geralmente empregados em portais de identificação para o uso em esteiras automáticas, portas e docas de carregamento, entre outros sistemas;
• **Módulos para embarcado ou embutido:** são leitores montados em placas de circuito impresso de outros equipamentos ou módulos acoplados fisicamente. Podem ser usados em sistemas de rastreamento de objetos e smartphones, entre outros.
Existem algumas especificações a serem consideradas para a escolha de um leitor RFID para determinada aplicação (HESSEL et al., 2012). São elas: frequência de operação, protocolos suportados, potência de saída das antenas, número de antenas suportadas, configurações de software e atualizações disponíveis.

1.1.4 COMUNICAÇÃO

A comunicação entre antenas e etiquetas ocorre por meio de dois tipos de acoplamento: indutivo ou eletromagnético.

• **Acoplamento indutivo:** utilizado por etiquetas HF, ocorre quando o leitor energiza a bobina existente em sua antena, e um campo magnético é induzido. Este campo, ao atingir a antena da etiqueta, promove o acoplamento, conforme ilustrado na **Figura 6**. Neste momento o leitor e a etiqueta efetuam a comunicação via protocolos preestabelecidos, e, por fim, a troca das informações é realizada com sucesso;

• **Acoplamento eletromagnético:** utilizado em etiquetas UHF, ocorre quando o sinal emitido pela antena do leitor induz uma corrente elétrica na antena da etiqueta. Esta corrente inicializa o microchip, que responde aos comandos enviados utilizando a mesma frequência recebida, conforme **Figura 7**. Este processo é também chamado de retrorreflexão (*backscatter*).

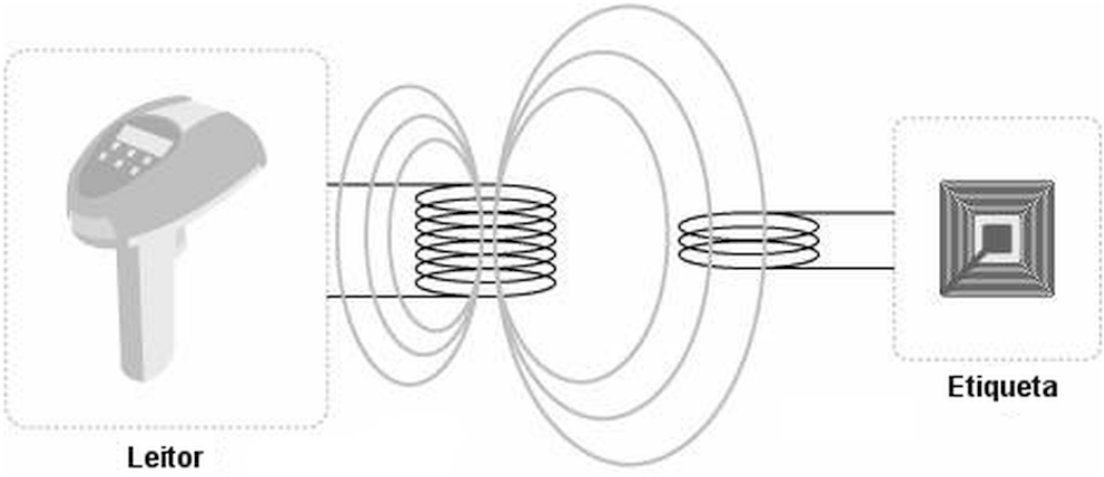
Com o intuito de evitar interferências com outras tecnologias que utilizam as mesmas faixas de frequência e melhorar o desempenho das soluções, os Sistemas RFID empregam a técnica do espalhamento espectral.

O espalhamento espectral é uma técnica que espalha o sinal a ser transmitido em uma largura de faixa de frequência maior do que a largura de faixa de frequência da informação. A utilização desta técnica permite que os sistemas trabalhem com potências menores. Em compensação, utilizam uma largura de faixa de frequência maior. As técnicas mais comuns para implementação do espalhamento espectral são: sequência direta e salto em frequência.

• **Sequência direta:** é uma técnica que combina a informação do sinal com uma sequência binária de frequência maior. A combinação resultante é então usada para modular a portadora do sinal a ser transmitido. O código binário trata-se de uma sequência de bits pseudoaleatória de comprimento fixo reaproveitada continuamente pelo sistema.
O salto em frequência é uma técnica que efetua o espalhamento da energia mudando a frequência da portadora do sinal várias vezes por segundo, conforme uma sequência de frequências atribuídas a canais gerados de forma pseudoaleatória;

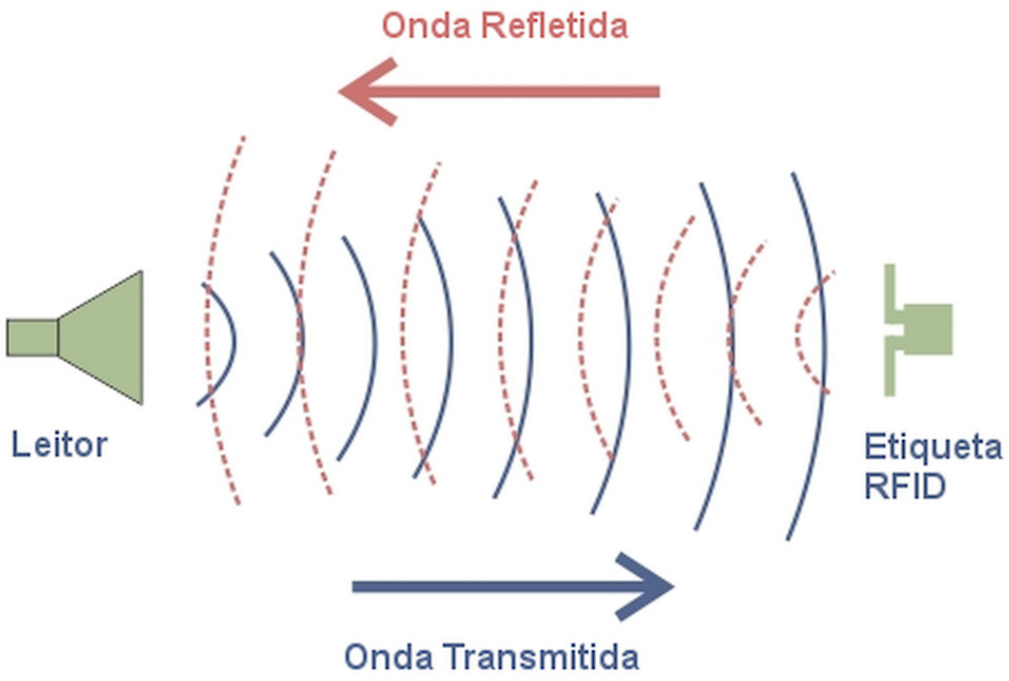
• **Salto em frequência:** no espalhamento espectral com salto em frequência (FHSS, do inglês frequency hopping spread spectrum) a banda de frequência pode ser dividida em canais com largura de 250 kHz ou 500 kHz, conforme nível de sinal esperado em cada canal. Para RFID, a largura do canal é de 500 kHz (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2008). A sequência pseudoaleatória é gerada por um circuito gerador de pulsos pseudoaleatórios, que determina a sequência de canais a ser utilizada para transmissão das informações. Depois de um certo período a sequência de canais se repete. Não se pode, portanto, afirmar que a sequência é aleatória, mas, sim, pseudoaleatória.
A técnica FHSS possui algumas vantagens: resistência a ruídos e interferências, resis-

Figura 6. Acoplamento indutivo.



Fonte: Bhatt e Glover (2006, tradução nossa).

Figura 7. Acoplamento eletromagnético.



Fonte: Griffin e Zhou (2012, tradução nossa).

tência a distorções por multipercurso e compartilhamento da faixa de frequência por diversos usuários. Porém, possui as seguintes desvantagens: ocupação de uma maior faixa de frequência, exigência de sincronismo entre transmissor e receptor e baixa capacidade de transmissão.

1.2 NORMAS E REGULAMENTAÇÃO

O desenvolvimento e a padronização da tecnologia RFID são decorrentes do esforço de diversas organizações, entre as quais podemos citar GS1, ECMA e ISO/IEC.

O estado atual do desenvolvimento da tecnologia foi atingido com a colaboração de empresas dos mais variados setores produtivos. A partir daí foram definidos requisitos técnicos e operacionais da tecnologia RFID, que foram então organizados e publicados como normas pela *International Organization for Standardization* (ISO) e *International Electrotechnical Commission* (IEC).

A publicação das normas permitiu o desenvolvimento de equipamentos e sistemas que operassem de forma integrada, independentemente do fabricante, ampliando assim a possibilidade de uso e, consequentemente, facilitando a adoção na cadeia de produção. Entre as normas publicadas pela ISO para a tecnologia RFID destacam-se as famílias de normas ISO/IEC 14443 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2008) e ISO/IEC 18000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013a).

A família de normas ISO/IEC 14443 apresenta as definições para os cartões de proximidade usados para identificação baseados em RFID. A comunicação deste protocolo ocorre na frequência de 13,56 MHz e possui uma distância de operação entre 0,3 metro e 0,5 metro. Esta norma divide-se em quatro partes:

- Parte 1 – O detalhamento técnico de características físicas;
- Parte 2 – Interface de sinais e potência de radiofrequência;
- Parte 3 – Protocolos de inicialização e anticolisão;
- Parte 4 – Protocolos de transmissão.

A família de normas ISO/IEC 18000 apresenta as definições para utilização de RFID em sistemas de identificação sem proximidade. Está dividida em sete partes, cada uma delas definindo parâmetros para uma faixa de frequência específica. A distância de operação é de até 10 metros. As partes e as faixas de frequências correspondentes cobertas por esta norma são:

- Parte 1 – Referência para definição de arquitetura e parâmetros;

- Parte 2 – abaixo de 135 kHz;
- Parte 3 – 13,56 MHz;
- Parte 4 – 2,45 GHz;
- Parte 5 – 5,8 GHz (descontinuada);
- Parte 6 – de 860 MHz a 960 MHz;
- Parte 7 – 433 MHz.

Cada uma das partes estabelece os parâmetros de comunicação físicos e lógicos da interface aérea, ou seja, a comunicação em radiofrequência.
A parte 6 da norma ISO/IEC 18000, que compreende a faixa de frequência 860 MHz a 960 MHz, foi dividida em mais quatro normas, denominadas:

- ISO/IEC 18000-61 – Tipo A;
- ISO/IEC 18000-62 – Tipo B;
- ISO/IEC 18000-63 – Tipo C;
- ISO/IEC 18000-64 – Tipo D.

As principais diferenças entre as normas da parte 6 estão relacionadas à codificação no enlace de comunicação e no algoritmo de colisão. A norma ISO/IEC 18000-61 – Tipo A estabelece a utilização na comunicação da Codificação por Intervalo de Pulso (PIE, do inglês *Pulse Interval Encoding*) e do algoritmo de colisão ALOHA adaptativo. A norma ISO/IEC 18000-62 – Tipo B estabelece a utilização na comunicação da codificação Manchester e do algoritmo de colisão Árvore Binária Adaptativo. A norma ISO/IEC 18000-63 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013b) – Tipo C estabelece a utilização na comunicação da codificação PIE e do algoritmo de colisão Slotted randômico. Já a norma ISO/IEC 18000-64 – Tipo D estabelece a utilização na comunicação da Codificação por Posição de Pulso (PPE, do inglês *Pulse Position Encoding*) ou da codificação de subportadora Miller.

A parte 63 foi originalmente desenvolvida e publicada pela GS1 no documento EPC *Global Class 1 Generation 2 version 1.2* UHF RFID (GS1 EPCGLOBAL, 2013). A GS1 propôs níveis de classes para tags RFID, sendo que cada classe possui funcionalidades específicas, conforme **Quadro 2**.

A tecnologia RFID baseada nas famílias de normas ISO 14443 e ISO 18000 podem ser encontradas em nosso dia a dia quando nos deslocamos pelas cidades. Os cartões do Bilhete Único utilizados na cobrança do transporte público na cidade de São Paulo seguem as instruções da norma ISO 14443. O protocolo de comunicação para a cobrança automática do Sistema de Arrecadação de Pedágios regulamentado pelo Governo do Estado de São Paulo foi desenvolvido com base nas normas ISO/IEC 18000-63 e *EPC Global Class 1 Generation 2.*

Além desses exemplos, a tecnologia de Comunicação por Campo Próximo, popularmente conhecida por *Near Field Communication* (NFC), também é outro forma de uso para RFID. O NFC utiliza para comunicação aérea os protocolos definidos nas ISO/IEC 14443 ou

Quadro 2. Classes de tags RFID.

CLASSE	FUNCIONALIDADE
Classe 0	Tags UHF somente leitura, passivas, pré-programadas.
Classe 1	Tags UHF ou HF, de escrita única, de leituras múltiplas.
Classe 2	Tags passivas, de leitura e escrita em qualquer ponto da cadeia de processos.
Classe 3	Leitura e escrita com sensores integrados capazes de gravar parâmetros como temperatura, pressão e movimento; pode ser semipassiva ou ativa.
Classe 4	Tags ativas de leitura e escrita com transmissores integrados; pode se comunicar com outras tags e leitores.
Classe 5	Semelhante às tags da Classe 4, mas com funcionalidade adicional; pode fornecer energia para outras tags e se comunicar com outros dispositivos que não leitores.

Fonte: Elaborado pelos autores.

ISO/IEC 18000, dependendo somente da escolha do fabricante, e opera na frequência de 13,56 MHz. O que diferencia o NFC das demais implementações de RFID ocorre no nível de aplicação, pois neste caso o número de informações transmitidas e recebidas é maior. Para atender a essa necessidade a ECMA desenvolveu os protocolos NFCIP-1 e NFCIP-2.

O NFCIP-1 foi publicado originalmente como padrão ECMA-340, posteriormente publicado como a norma ISO/IEC 18092 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013c). Essa norma especifica a comunicação sem fio entre dispositivos próximos em taxas de comunicação definidas.

O NFCIP-2 foi publicado originalmente como padrão ECMA-352, posteriormente publicado como a norma ISO/IEC 21481 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012). Essa norma amplia a aplicação da norma ISO/IEC 18092, adicionando a funcionalidade de selecionar os modos de comunicação a serem adotados no processo de leitura e escrita.

Outras normas relacionadas a RFID foram definidas e publicadas pela ISO/IEC.
As normas ISO 11784 e 11785 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 1996a; 1996b) definem a estrutura de códigos de identificação e parâmetros de ativação e transmissão de informações. São utilizadas para identificação animal, po-

pularmente conhecida como “brinco de boi”, e operam na faixa de frequência de 129 a 139,4 kHz. Essas normas foram substituídas pela norma ISO 14223 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2011).

A norma ISO/IEC 15693 apresenta as definições para os cartões de vizinhanças (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018). A comunicação desta norma ocorre na frequência de 13,56 MHz e possui uma distância de operação entre 1 metro e 1,5 metro. Essa distância é bastante superior quando comparada à atingida pela norma ISO/IEC 14443. No entanto, as funcionalidades oferecidas pela norma ISO/IEC 18000, que permitem maior distância de operação, ocasionaram uma adoção não tão expressiva.

1.3 RFID E O USO EM CIDADES INTELIGENTES E INDÚSTRIA 4.0

A tecnologia RFID está bastante difundida em diversos setores da indústria para identificação individual de itens.
Lojas de departamento têm utilizado RFID para identificação de produtos, permitindo aos usuários que escolham os produtos em um formato “self-service”, sem a necessidade do auxílio de um vendedor, seja no momento da seleção ou do pagamento.
Nas Cidades Inteligentes, destaca-se o uso de RFID para pagamento do transporte público, a exemplo do Bilhete Único na cidade de São Paulo, que utiliza cartões sem contato com RFID. Ainda no setor de mobilidade, o estado de São Paulo adotou a tecnologia RFID para pagamento de pedágio nas rodovias estaduais.
Para a indústria, destaca-se o uso de RFID no controle de estoque das mais diversas áreas, de setores governamentais a indústrias siderúrgicas, passando pela indústria de eletrodomésticos.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Regulamento sobre equipamentos de radiocomunicação de radiação restrita. Brasília: ANATEL, 2008.

BHATT, H.; GLOVER, B. RFID Essentials. USA: O'Reilly, 2006. 276 p.

GRIFFIN, J.; ZHOU, C. Ranging for backscatter RFID. Los Angels: Disney Research, 2012.

GS1 EPCGLOBAL. EPC Class 1 Gen 2 UHF RFID: Epc radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz. Brussels, 2013. 152 p.

HESSEL, F. et al. Implementando RFID na cadeia de negócios. Porto Alegre: EDIPUCRS, 2012. 344 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Electrotechnical Commission. ISO/IEC. ISO/IEC 14443-1: Identification cards — contactless integrated circuit cards — proximity cards — part 1. Geneve: ISO, 2008. 70 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Electrotechnical Commission. ISO/IEC. ISO/IEC 18000-6: Information technology — radio frequency identification for item management — part 6. Geneve: ISO, 2013a. 16 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Electrotechnical Commission. ISO/IEC. ISO/IEC 18000-63: Information technology — radio frequency identification for item management — part 63. Geneve: ISO, 2013b. 308 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Electrotechnical Commission. ISO/IEC. ISO/IEC 18092: Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1). Geneve: ISO, 2013c. 44 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Electrotechnical Commission. ISO/IEC. ISO/IEC 21481: Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2). Geneve: ISO, 2012. 4 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Electrotechnical Commission. ISO/IEC 15693-1: Cards and security devices for personal identification -- Contactless vicinity objects -- Part 1: Physical characteristics. Geneve: ISO, 2018. 5 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 11784: Radio frequency identification of animals -- Code structure. Geneve: ISO, 1996a. 2 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 11785: Radio frequency identification of animals -- Technical concept. Geneve: ISO, 1996b. 13 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 14223-1: Radiofrequency identification of animals -- Advanced transponders -- Part 1: Air interface. Geneve: ISO, 2011. 25 p.

2 RTLS: SISTEMAS DE LOCALIZAÇÃO EM TEMPO REAL

1. INTRODUÇÃO

A localização de objetos e pessoas nada mais é que detectar sua posição espacial. Durante a história da evolução humana desenvolveram-se muitas técnicas e instrumentos para essa finalidade, como por exemplo bússola, astrolábio, quadrante e sextante, entre outros. Cada instrumento proporcionou melhorias em seus períodos históricos, porém eles não possuíam a precisão com a qual estamos habituados atualmente, nem sequer faziam cobertura global.

Hoje existem sistemas de localização que oferecem cobertura global e que recebem a denominação de Sistema de Navegação Global por Satélite (GNSS, do inglês *Global Navigation Satellite System*).

O mais popular entre eles é o GPS, que é um sistema de radionavegação criado pelo Departamento de Defesa dos EUA, também conhecido pela sigla em inglês *NAVigation Satellite with Time and Ranging* (NAVSTAR-GPS). Seu desenvolvimento iniciou-se com o propósito de ser o sistema de navegação das forças armadas norte-americanas, porém hoje ele é aberto para o uso civil e permite que o dispositivo receptor seja localizado em tempo real na superfície terrestre sob quaisquer condições climáticas. Isso é possível graças à complexa cobertura satelital que garante o alcance mínimo de quatro satélites em qualquer ponto da superfície (SILVA, 2016).

Apesar de Sistemas GNSS, como GPS, serem utilizados para localização e serem amplamente difundidos, esta tecnologia não é apropriada para rastreamento indoor, pois requer linha de visão direta entre o objeto e os satélites. O próximo passo na evolução da geolocalização passa, portanto, pela localização indoor. É nesse contexto que surge o conceito de RTLS (do inglês *Real-Time Locating System*), o que ocorre em 1998, nos Estados Unidos, por Tim Harrington, Jay Werb e Bert Moore em um congresso do Grupo ID Global. Os Sistemas de Localização em Tempo Real (RTLS) são automatizados e monitoram a atividade dos objetos presentes em seu campo de leitura, o que permite não só localizar objetos, mas também pessoas em ambientes fechados (PEREIRA; AVANÇO, 2017). Portanto, quando se menciona RTLS, o contexto considerado é para sistemas de localização indoor.

Embora este capítulo trate de diversas tecnologias, o foco será dado à localização indoor com RFID, uma vez que a disseminação em cenários logísticos e de identificação de produtos já é muito presente, principalmente em setores nos quais a localização indoor é realmente interessante para aumentar a competitividade e a eficiência operacional.

2.1 TECNOLOGIAS PARA LOCALIZAÇÃO INDOOR

Os RTLS *indoor* possuem em sua infraestrutura tecnologias baseadas em radiofrequência. Na sequência serão apresentadas as principais tecnologias utilizadas para o rastreamento *indoor* e suas características essenciais.

2.1.1 WI-FI

A rede Wi-Fi (do inglês, *wireless fidelity*) foi desenvolvida em 1999 pela empresa Interbrand atendendo a solicitação da Wi-Fi Alliance. Para garantir a interoperabilidade da rede o Wi-Fi adotou a norma IEEE 802.11, à qual foram adicionadas, posteriormente, as normas 802.11b, 802.11g, 802.11n e 802.11ac.

Atualmente esta rede opera nas frequências de 2.4 GHz e 5.0 GHz. Para que a tecnologia funcione, de um lado temos os vários dispositivos móveis (entre eles smartphones, notebooks, televisores inteligentes) e, de outro, os pontos de acesso. O ponto de acesso permite que todos os dispositivos a ele ligados possam se comunicar dentro da mesma rede, que tem um alcance efetivo de cerca de 35 metros em ambientes internos e 110 metros nos fechados.

Uma das vantagens de obter o posicionamento de objetos com o Wi-Fi é a existência em massa de redes Wi-Fi em locais públicos e privados. Se for possível condicionar as possíveis posições do dispositivo móvel a um espaço limitado, o sistema de localização torna-se mais preciso, sendo mais fácil prever sua localização. Para tornar esses sistemas mais precisos em ambientes *indoor* fornece-se a planta do local em causa, permitindo, assim, reduzir a distorção do sinal Wi-Fi criada pelos materiais existentes no local (paredes, portas, pilares, eletrodomésticos, entre outros). Desta forma, consegue-se condicionar as áreas que cada dispositivo móvel pode percorrer, evitando a transposição de condicionantes físicas, como as paredes. Esses sistemas de localização tanto podem ser alojados e processados nos dispositivos móveis (localização implícita) ou então em um ou mais servidores (localização explícita).

Para criar um sistema de localização *indoor* utilizando as redes Wi-Fi são necessárias duas fases distintas: uma fase de treino (off-line) e a fase de determinação da localização (on-line). A primeira fase, como o próprio nome indica, consiste em treinar a rede por meio da recolha e registro das potências dos sinais Wi-Fi e o identificador *Service Set Identifier* (SSID) do respetivo AP através de um dispositivo móvel. Depois desta recolha

de dados é criado um mapa rádio para cada AP, que contém a potência do sinal e a respectiva posição na planta. A segunda fase permite que quando se proceder à localização de um objeto será feita a comparação dos valores das potências dos sinais Wi-Fi recebidos no dispositivo móvel com os valores guardados nas diferentes posições em cada mapa rádio. Depois, por meio de uma técnica de localização (determinística ou probabilística), é calculada a posição mais provável do dispositivo móvel.

2.1.2 ZIGBEE

A tecnologia foi desenvolvida pela organização sem fins lucrativos ZigBee Alliance, que adotou como protocolo padrão do ZigBee o IEEE 802.15.4 Physical Layer (PHY) e o Medium Access Control (MAC).

O ZigBee se destina a aplicações que não necessitam de altas taxas de transmissão na comunicação. Além disso, é uma tecnologia de baixo custo e consome pouca energia no seu funcionamento, o que é fundamental nas aplicações de IoT.
Devido às suas características, o ZigBee é aplicado normalmente na monitorização de usuários, automatização de residências e na localização indoor. O usuário pode recolher informações relacionadas a sua saúde ao interagir com um dispositivo ZigBee portátil. Este dispositivo pode passar a monitorizar a pressão arterial e a frequência cardíaca, entre outros fatores. Como se trata de uma tecnologia sem fios, os dispositivos móveis transmitem esses dados a um servidor local, como por exemplo o computador pessoal do usuário, que irá analisar os dados recebidos.

O ZigBee permite a localização de objetos utilizando radiofrequência, sendo que o posicionamento de um nó pode ser resumido da seguinte maneira: o nó com a localização desconhecida envia um sinal, que é recebido pelos outros nós. Quando recebem esse sinal, os outros nós que estão espalhados pela área de abrangência do RTLS medem a sua intensidade (RSSI), o ângulo formado na chegada (AoA) e o tempo de chegada (ToA e TDoA). Esses métodos estão explicados nas seções 2.2.2 e 2.2.3 deste capítulo.
O RSSI é mais utilizado para calcular a posição de um nó devido a sua simplicidade e porque se o relógio dos dispositivos não for preciso e sincronizado não é possível utilizar AoA, ToA e TDoA.

2.1.3 BLUETOOTH

O Bluetooth é uma tecnologia usada para comunicações de rádio de curtas distâncias, com a finalidade de substituir as conexões por fios entre diversos dispositivos, como telefones, computadores e assistentes digitais pessoais. A entidade responsável pela sua especificação e promoção é denominada *Bluetooth Special Interest Group* (SIG).
Em 2010 surgiu uma tecnologia de emissão de sinais de radiofrequência que possibilita a emissão e recepção de sinais consumindo baixas quantidades de energia. Trata-se

da tecnologia denominada *Bluetooth Smart, Bluetooth Low Energy ou Bluetooth 4.0*, que permite projetar dispositivos de emissão BT, a serem alimentados por fontes de energia como as pequenas baterias de 3 volts. O Bluetooth Smart possibilitou o desenvolvimento de emissores pequenos e econômicos que, desde então, vêm ocupando um espaço maior no projeto de sistemas de localização *indoor* (MENEGOTTO, 2015).

Uma das características que diferencia o Bluetooth tradicional do Bluetooth 4.0 é que a conexão entre os dispositivos não precisa ser realizada através de pareamento, o que permite a descoberta passiva e contínua de dispositivos e aplicativos. A interoperabilidade entre fornecedores e a possibilidade de ampliar o rádio de alcance são outras características que tornam a versão 4.0 atrativa em relação ao BT tradicional.

Assim, a tecnologia vem se inserindo como uma alternativa adicional para os sistemas de localização. Ela permite o desenvolvimento de aplicativos que ajudem a gerenciar dinamicamente dados contextuais. Na prática, exemplos de sua aplicação podem ser encontrados em situações nas quais seja útil rastrear, de forma dinâmica, recursos humanos e físicos, verificando e fornecendo informações de contexto em tempo real. Como contexto entende-se um modo de indicar o conjunto de dados que descrevem a identidade, o estado, a atividade e a forma de interagir que caracterizam usuários e objetos numa determinada situação espaçotemporal (MENEGOTTO, 2015).

2.1.4 RFID

Conforme já apresentado anteriormente, o RFID é uma tecnologia que realiza troca de dados utilizando comunicação por radiofrequência. O uso de RFID é comum em ambientes internos complexos, tais como edifícios de escritórios e hospitais, fornecendo uma abordagem consideravelmente mais barata e flexível para identificar dispositivos e pessoas.

A **Tabela 2** apresenta as principais diferenças entre as diversas tecnologias baseadas em radiofrequência descritas neste capítulo.

2.2 RTLS BASEADO EM RFID

RTLS (do inglês Real-Time Locating System) são sistemas automatizados que monitoram a atividade das etiquetas RFID presentes em seu campo de leitura. A arquitetura de um RTLS é composta de alguns elementos básicos. São eles: aplicação, middleware, etiquetas RFID e sensores de localização. A **Figura 8** demonstra os elementos básicos em uma implementação genérica.

Tabela 2. Comparação entre as tecnologias.

	WIFI	ZIGBEE	BLUETOOTH 4.0	RFID
Padrão	IEEE 802.11 a/b/g/n	IEEE 802.15.4	GFSK	ISO 18000
Frequência de operação	2.4 Ghz	868/915 MHz e 2.4 GHz	Depende do meio	12.5 KHz - 915 MHz e 2.4 GHz
Topologia de rede	Depende do meio	Todas	1 Mbps	Direta
Velocidade de transmissão	10 - 105 Mbps	250 Kbps	Até 50 m	384 Kbps
Alcance	10 - 110 m	10-300m	Muito baixo	10 cm - 100m
Consumo energético	Alto	Muito baixo	Meses a anos	Muito baixo
Bateria	Horas	Meses a anos	65000	Ativas (meses a anos) Passivas (não necessita)
Número máximo de nós	32	65000	Alto	Ilimitado
Custo do usuário	Baixo	Alto	Baixo	Baixo
Custo de infraestrutura	Baixo	Baixo		Baixo

Fonte: Elaborado pelo autor.

Figura 8. Elementos básicos de um RTLS.

Fonte: Elaborado pelo autor.

A aplicação é o único elemento responsável pela interação com o usuário final do sistema. Cabe a essa camada abstrair as informações fornecidas pelos demais elementos, facilitando a interpretação e a experiência final.

O elemento básico middleware é responsável por gerenciar os dispositivos físicos do sistema (leitores de radiofrequência, sensores etc) e obter deles as informações solicitadas pelo elemento de aplicação. Ou seja, entre os elementos relacionados com software, é o que está em baixo nível e mais próximo aos dispositivos de hardware.

As etiquetas RFID são responsáveis por identificar os objetos que se deseja localizar. Elas podem assumir as mais diversas formas e encapsulamentos, dependendo da natureza do objeto identificado.

O último elemento, e o mais importante, são os sensores de localização, que podem ser de diversas tecnologias. Aqui iremos abordar a tecnologia RFID, já presente nas etiquetas, pois seu uso é comum em ambientes internos complexos, tais como edifícios de escritórios e hospitais. O RFID fornece uma abordagem flexível e relativamente mais barata para identificação de pessoas e dispositivos. Logo, é conveniente utilizá-lo em RTLS. Com os objetos identificados com etiquetas RFID é possível localizar e monitorar usando técnicas de rastreamento indoor. As principais são: Variação da Intensidade do Sinal (RSSI, do inglês *Received Signal Strength Indication*); Ângulo de Chegada (AoA, *Angle of Arrival*); e Tempo de Recebimento (ToA, *Time of Arrival)*.

2.2.1 VARIAÇÃO DE INTENSIDADE DO SINAL - RSSI

A resposta de uma etiqueta a uma interrogação é um sinal de radiofrequência com uma determinada intensidade (RSSI). Desta forma, o RTLS compara o RSSI advindo das etiquetas com um mapa de intensidade já registrado em sua memória. Assim, provê o cálculo das localizações Hessel et al. (2013). Para os sistemas RFID passivos, em que o sinal de transmissão é retrorrefletido (*backscattered*) pela etiqueta, a intensidade do sinal de resposta (RSSI) é determinada pela equação (1), definida por Zhang, Li e Amin (2010).

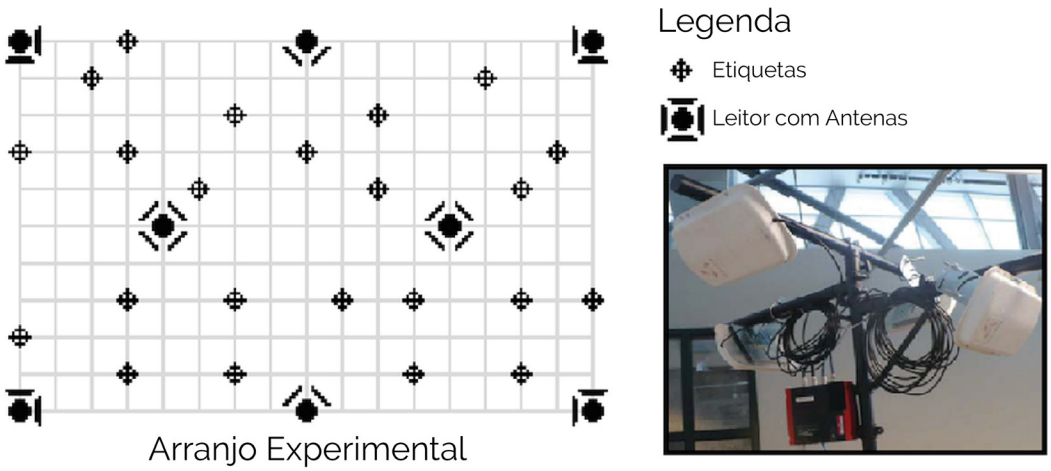
$$RSSI = P_{TX,\ etiqueta} \eta G^2_{etiqueta} G^2_{TX,leitor} \left(\frac{\lambda}{4\pi d} \right) \qquad (1)$$

Em que
$P_{TX,\ etiqueta}$ é o ganho da antena RFID,
η é a eficiência da retrorreflexão,
$G_{etiqueta}$ é o ganho da etiqueta,
$G_{TX,leitor}$ é o ganho do leitor,
λ é o comprimento de onda do sinal portadora,
d é a distância entre a antena e a etiqueta RFID.

Conhecendo os valores das variáveis da equação (1), sabendo que tipicamente Ƞ é igual a 1/3 ou -5dB, pode-se determinar a distância entre antena e etiqueta (*d*), e, desta forma, obter o mapa de intensidade de sinal e executar os cálculos das localizações (ZHANG; LI; AMIN, 2010).

Brennan e Kolaja (2014) propuseram um método que utiliza RSSI para estimar a localização de etiquetas e validaram-no através de dois experimentos. No primeiro, realizam a localização com oito e vinte antenas, conforme arranjo experimental das **Figura 9 e 10**, em uma sala de 10 metros x 16 metros.

Figura 9. Arranjo experimental.



Fonte: Brennan e Kolaja (2014, tradução nossa).

Figura 10. Primeiro experimento.

Fonte: Brennan e Kolaja (2014).

O segundo experimento é realizado com o mesmo arranjo experimental, porém com o intuito de validar o modelo em distâncias maiores. Para isso, utilizaram um ginásio de esportes (**Figura 11**), que foi a maior área viável encontrada.

Outros autores, como Colin, Moretto e Hayoz (2014), utilizam RTLS baseado em RSSI. Eles realizaram um experimento com etiquetas passivas de localização conhecida em um corredor de hospital, e através das etiquetas estimaram a localização de um robô, conforme **Figura 12**.

Figura 11. Segundo experimento.

Fonte: Brennan e Kolaja (2014).

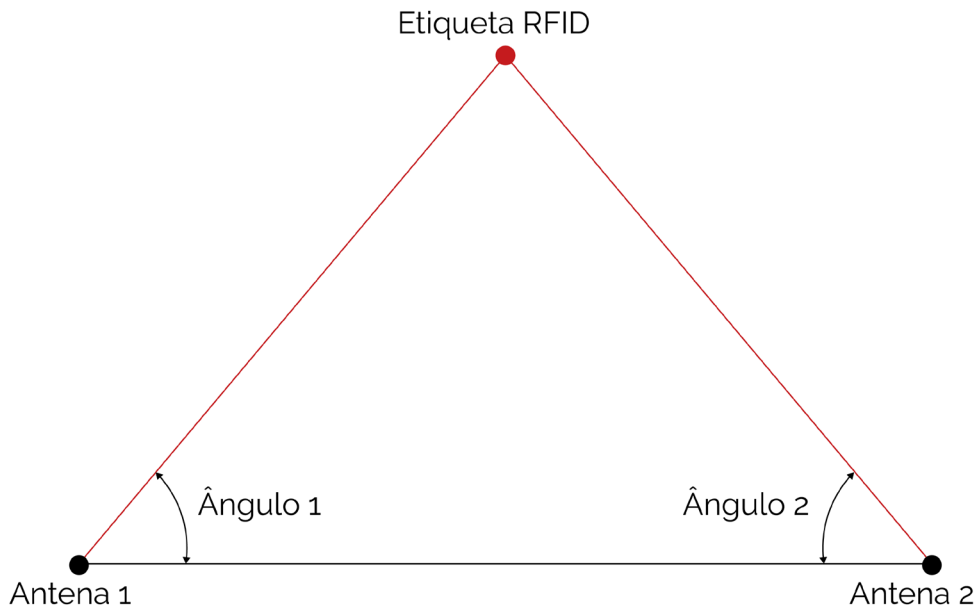
Figura 12. Experimento em corredor de hospital usando RSSI.

Fonte: Colin, Moretto e Hayoz (2014, tradução nossa).

2.2.2 ÂNGULO DE CHEGADA - AOA

AoA consiste em calcular a intersecção de duas ou mais linhas de direção provenientes de uma antena até uma etiqueta RFID, conforme **Figura 13**.
Dois ângulos medidos com antenas, no mínimo, são necessários para encontrar a localização de um alvo em duas dimensões Bouet e Dos Santos (2008).

Figura 13. Localização por AOA de objeto usando duas linhas de direção.



Fonte: adaptado de Bouet e Dos Santos (2008, tradução nossa).

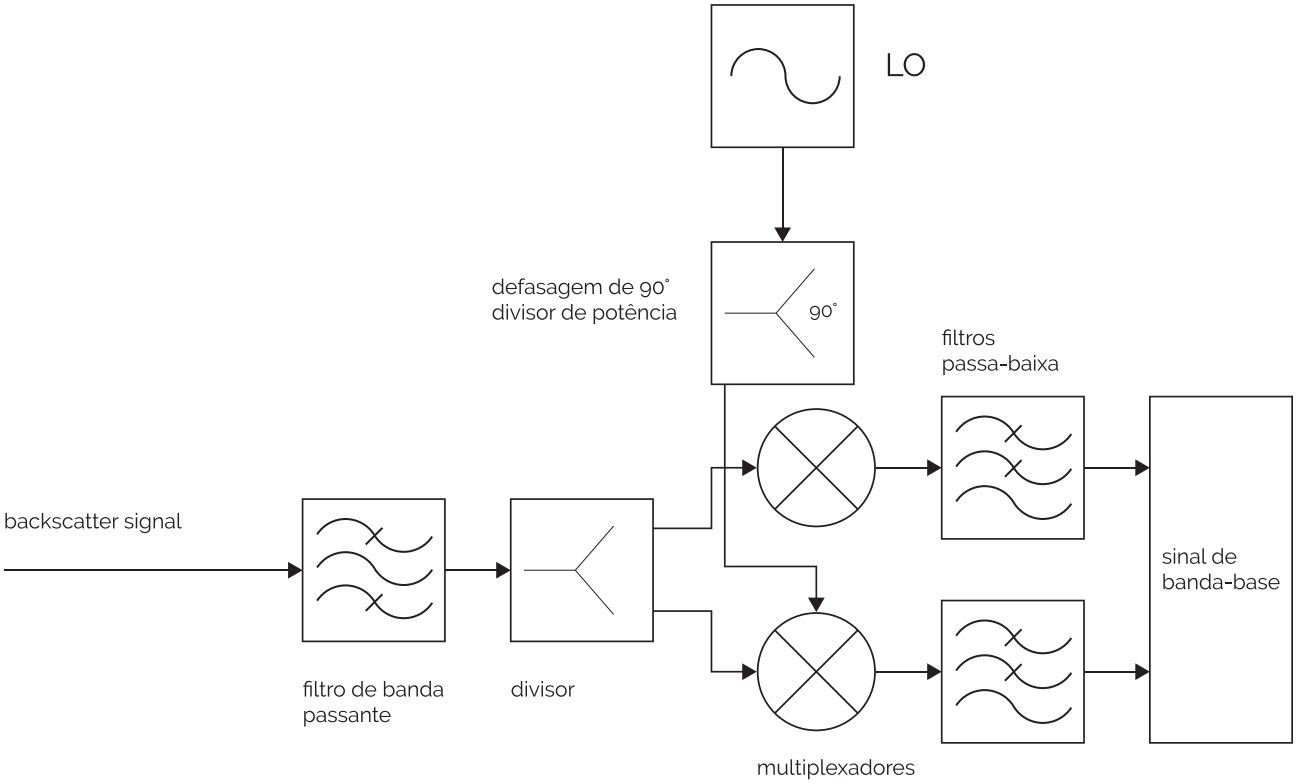
Zhou, Zhang e Mo (2011) apresentaram um método AoA de localização de etiquetas RFID UHF passivas, com a obtenção da diferença de fase entre o sinal retrorrefletido da etiqueta (*backscatter signal*) e o sinal do oscilador local (LO, do inglês *local oscillator*) do leitor RFID. Em um sistema RFID UHF passivo padrão, o leitor usa o sinal do LO para converter o sinal da etiqueta para a banda-base, conforme mostrado na **Figura 14**.

Então, com a subtração entre o sinal de LO do leitor pelo sinal retrorrefletido da etiqueta chega-se à diferença de fase (φ),

$$\varphi = -\frac{2\pi f R}{c} + \varphi_0 \qquad (2)$$

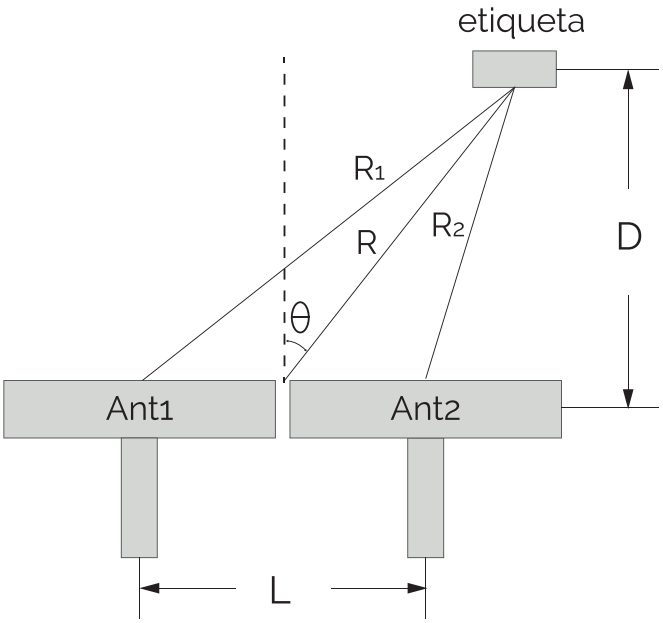
f é a frequência da portadora, φ_0 é a diferença de fase causada pelo hardware do leitor, c é a velocidade da luz no vácuo e R, a distância entre a antena e a etiqueta RFID.

Figura 14. Diagrama de conversão de sinal de um leitor RFID.



Fonte: adaptado de Zhou, Zhang e Mo (2011, tradução nossa).

Figura 15. Arranjo experimental do método AOA proposto.



Fonte: Traduzido de Zhou, Zhang e Mo (2011, tradução nossa).

Portanto, conhecendo φ é possível estimar a distância entre antena e etiqueta R. Porém, o ângulo de chegada da linha de direção entre antena e etiqueta ainda não é conhecido. Para isso, o método proposto por Zhou, Zhang e Mo (2011) considera a diferença de fase de duas antenas, como ilustra o arranjo experimental da **Figura 15**.

Considerando $L \ll R$, e o sentido horário positivo, tem-se que:

$$R_1 - R_2 \cong -L \sin\theta \qquad (3)$$

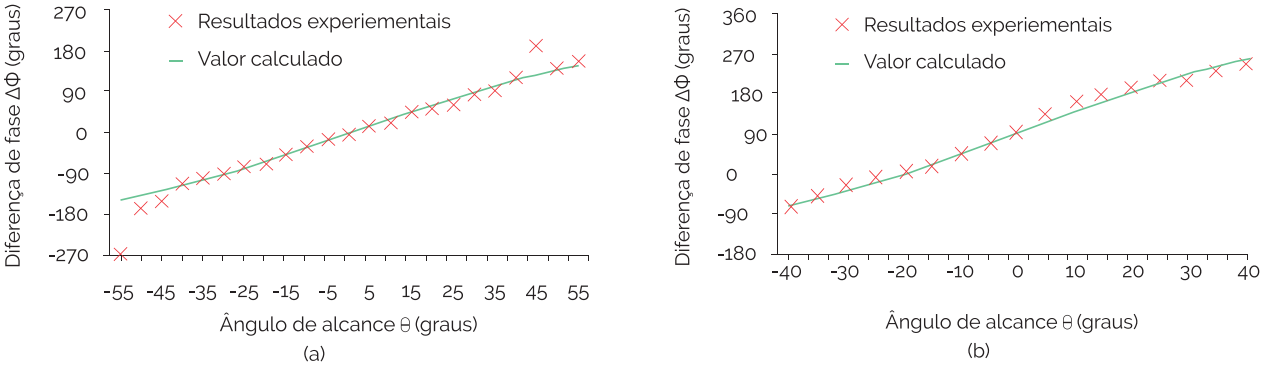
Então, por meio das propriedades trigonométricas e equações (2) e (3), os autores definem o ângulo de alcance θ como:

$$\theta = \sin^{-1}\left[\frac{\lambda}{2\pi L}(\Delta\varphi - \Delta\varphi_0)\right] \qquad (4)$$

Em que Δφ é a diferença de fase do sinal de retorno da etiqueta das duas antenas ($\varphi_2 - \varphi_1$), $\Delta\varphi_0$ é a diferença de fase causada pelo hardware das duas antenas e λ é o comprimento de onda do sinal da portadora. Se as antenas são exatamente iguais, pode-se desprezar $\Delta\varphi_0$. Portanto, pode-se usar diferença de fase de duas antenas para estimar a localização por AoA, desde que $L \ll R$.

A **Figura 16** apresenta os resultados do experimento ilustrado na **Figura 15**, comparando dados coletados experimentalmente com o valor calculado matematicamente em duas situações diferentes: (a) usa-se uma única antena em duas posições distantes em 0,164 metro; (b) duas antenas diferentes distantes em 0,225 metro.

Figura 16. Resultados do Experimento.

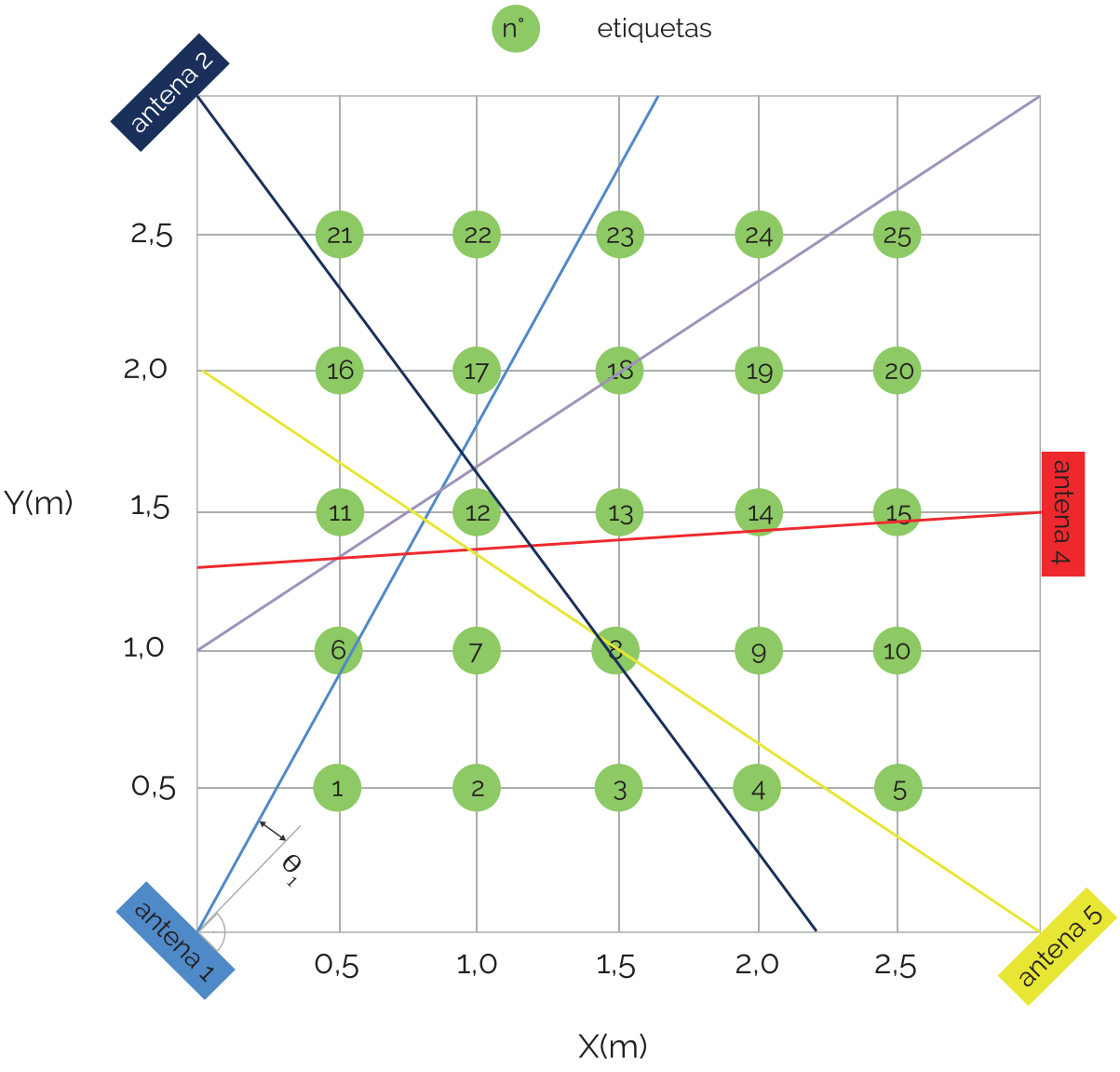


Fonte: Zhou, Zhang e Mo (2011, tradução nossa).

A comparação entre o valor calculado e os dados experimentais mostra que a técnica de Zhou, Zhang e Mo (2011) é precisa quando o ângulo de alcance se encontra entre -40º e 40º. Outros trabalhos empregam a técnica proposta por Zhou, Zhang e Mo (2011), a exemplo de Cremer et al. (2014), que realizaram a localização de etiquetas UHF passivas em uma sala de 3 metros x 3 metros usando cinco antenas com polarização circular, conforme arranjo da **Figura 17**.

Scherhaufl, Pichler e Stelzer (2015) utilizaram AoA para localizar seis etiquetas RFID UHF, com protocolo de interface aérea EPC Gen-2 (ISO/IEC 18000-63), a partir de oito antenas. O experimento foi realizado em laboratório, como pode ser visto na **Figura 18**.

Figura 17. Arranjo experimental.



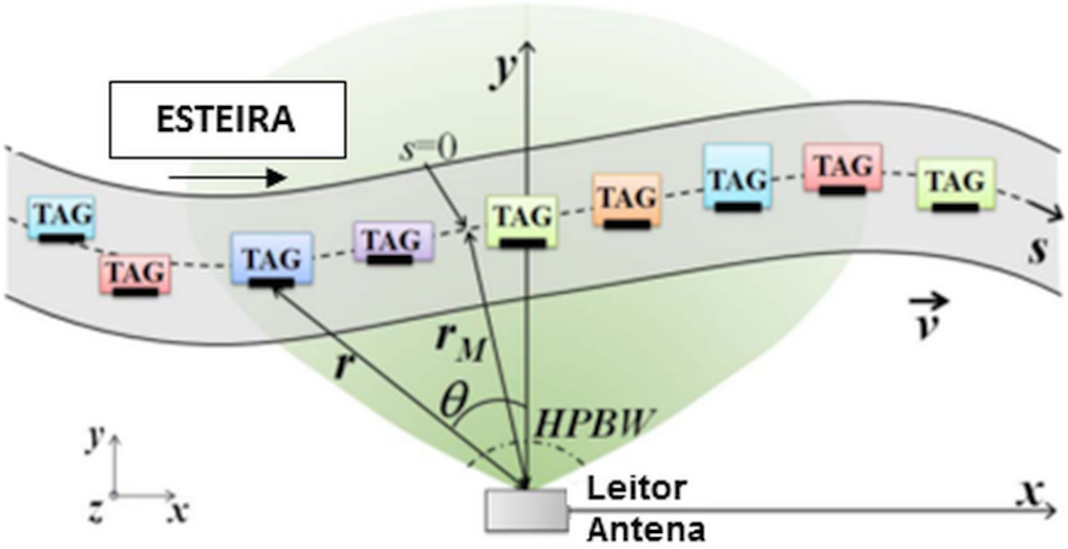
Fonte: Cremer et al. (2014, tradução nossa).

Da mesma forma, Buffi, Nepa e Lombardini (2015) realizaram um experimento em que se obtém o ângulo de chegada de etiquetas RFID em movimento na esteira. A ilustração da **Figura 19** apresenta o arranjo do experimento.

Figura 18. Experimento de Scherhaufl, Pichler e Stelzer.

Fonte: Scherhaufl, Pichler e Stelzer (2015).

Figura 19. Arranjo experimental proposto por Buffi, Nepa e Lombardini.



Fonte: Buffi, Nepa e Lombardini (2015, tradução nossa).

2.2.3 TEMPO DE CHEGADA - TOA

A distância entre um ponto de referência e um alvo é proporcional ao tempo de propagação de um sinal de radiofrequência. A técnica de ToA, também conhecida como triangulação, calcula a distância entre a antena e a etiqueta RFID através do intervalo de tempo entre a emissão do sinal de radiofrequência e seu retorno à antena RFID.
Nessa técnica, para encontrar a exata posição de um objeto são necessárias, no mínimo, três antenas Hessel et al. (2013). Zhang, Li e Amin (2010) definem a distância entre antena e etiqueta (R) como:

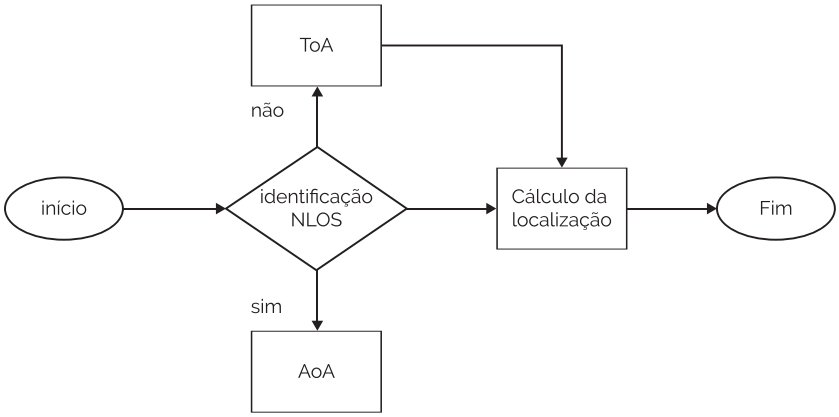
$$R = c.\frac{(T-Tp)}{2} \qquad (5)$$

T é o tempo de propagação do sinal de radiofrequência, Tp é o tempo de processamento circuito da etiqueta e c, a velocidade da luz no vácuo.

Em se tratando de etiquetas passivas, não é necessário sincronizar os relógios do leitor com a etiqueta. Porém, nas ativas, se faz necessária a sincronização dos relógios, o que é impraticável na maior parte dos sistemas RFID ativos e torna essa técnica inviável para esses casos Zhang, Li e Amim (2010). Além disso, é sabido que obstáculos entre a comunicação NLOS (do inglês *non-line-of-sight*) alteram a trajetória dos sinais, que, por sua vez, alteram o tempo de propagação, o que consequentemente diminui a exatidão do cálculo da localização Bouet e Dos Santos (2008).

Em virtude dessas dificuldades, poucos trabalhos que empregam essa técnica são encontrados. Um deles foi elaborado por Kim et al. (2011), os quais propuseram um método de localização que combina ToA com AoA. Por meio de sensores de NLOS, o método identifica obstáculos entre antena e etiqueta e, nesses casos, utiliza o cálculo da localização por AoA. O diagrama da **Figura 20** ilustra o método.

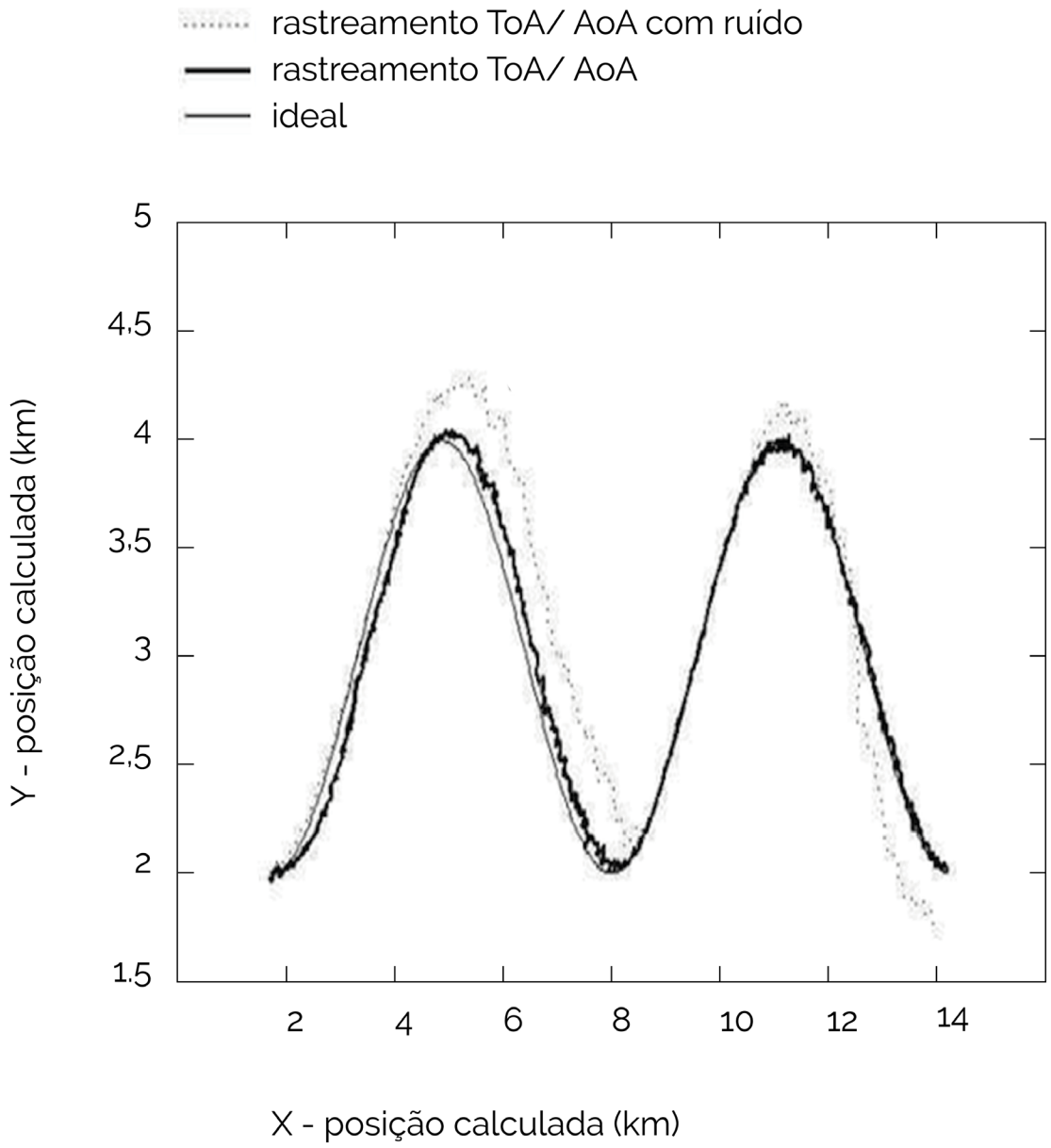
Figura 20. Diagrama do método combinando AOA e TOA.



Fonte: adaptado de Kim et al. (2011, tradução nossa).

Verificou-se a exatidão desse método com uma simulação em que se deslocou uma etiqueta no plano xy. Seus resultados são apresentados na **Figura 21**. A linha simples representa a trajetória ideal, enquanto a linha em negrito mostra a trajetória calculada pelo método ToA/AoA. Já na linha tracejada foi inserido um ruído com distribuição Gaussiana na simulação.

Figura 21. Comparação dos resultados da simulação.



Fonte: adaptado de Kim et al. (2011, tradução nossa).

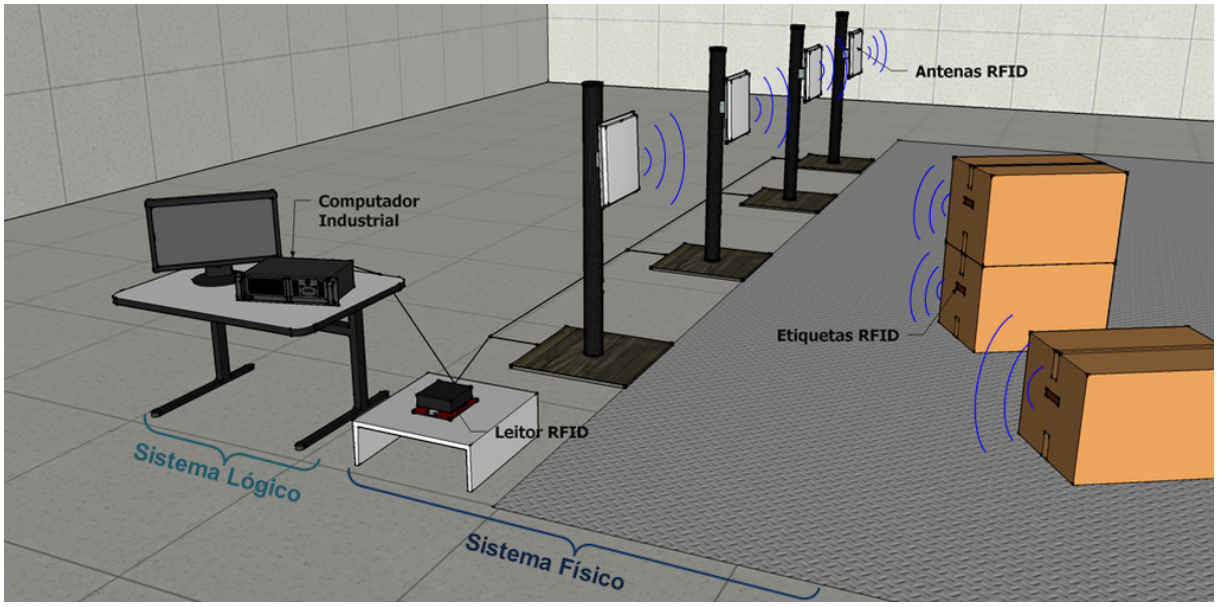
2.3 EXPERIMENTOS DE APLICAÇÃO DE RTLS COM RFID

Nas aplicações de IoT, como já foi dito, a geolocalização é um dos temas mais relevantes para fins comerciais, segurança pública, medicina e indústria. Nas aplicações *indoor*, temos diversas técnicas de localização, conforme descrito na seção 2.1. Porém, as interferências na comunicação causadas pelos ambientes de aplicações reais não foram consideradas.

Tendo em vista esse cenário, Pereira (2016) desenvolveu o Sistema de Localização de Etiquetas RFID (SLER), que é um RTLS capaz de rastrear objetos identificados utilizando as técnicas de localização RSSI, AoA e ToA.

O SLER é composto por um subsistema físico, que são os equipamentos utilizados na sua construção (Computador Industrial; Leitor, Antenas e Etiquetas RFID), além de um subsistema lógico, que é um software instalado no computador industrial, responsável por gerenciar os equipamentos e realizar os cálculos de rastreamento.
A **Figura 22** ilustra o SLER e seus subsistemas.

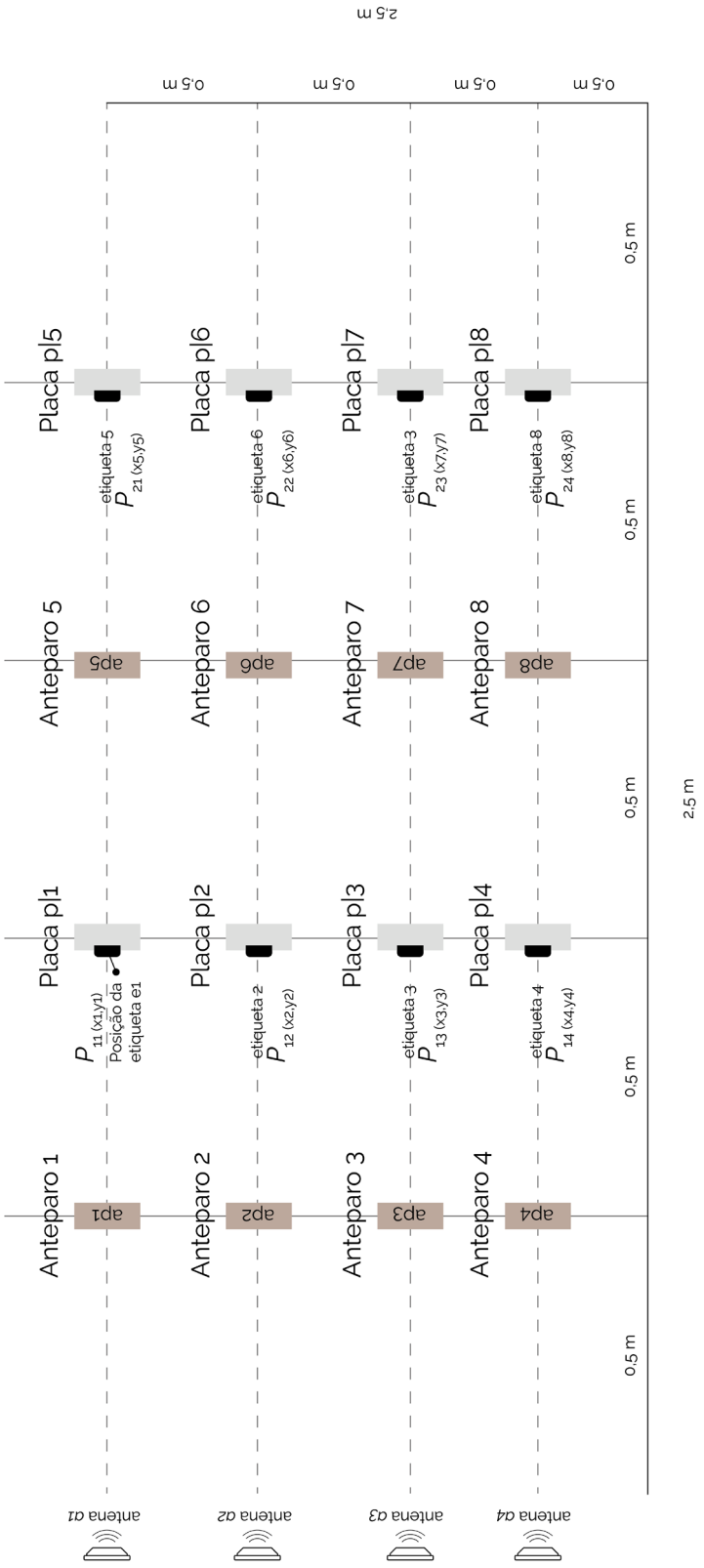
Figura 22. Ilustração dos subsistemas do SLER.



Fonte: Pereira (2016).

Para verificar as interferências na comunicação de ambientes reais no SLER, este foi submetido a experimentos em um ambiente laboratorial. A Figura 23 mostra o arranjo experimental, com oito anteparos (ap) à frente das etiquetas RFID, usados para verificar a influência de obstáculos na comunicação entre etiquetas e antenas RFID. Também é possível verificar oito placas (pl), sobre as quais a etiqueta RFID é fixada, podendo-se, assim, constatar a influência dos materiais usados na fabricação dos objetos.

Figura 23. Arranjo Experimental.

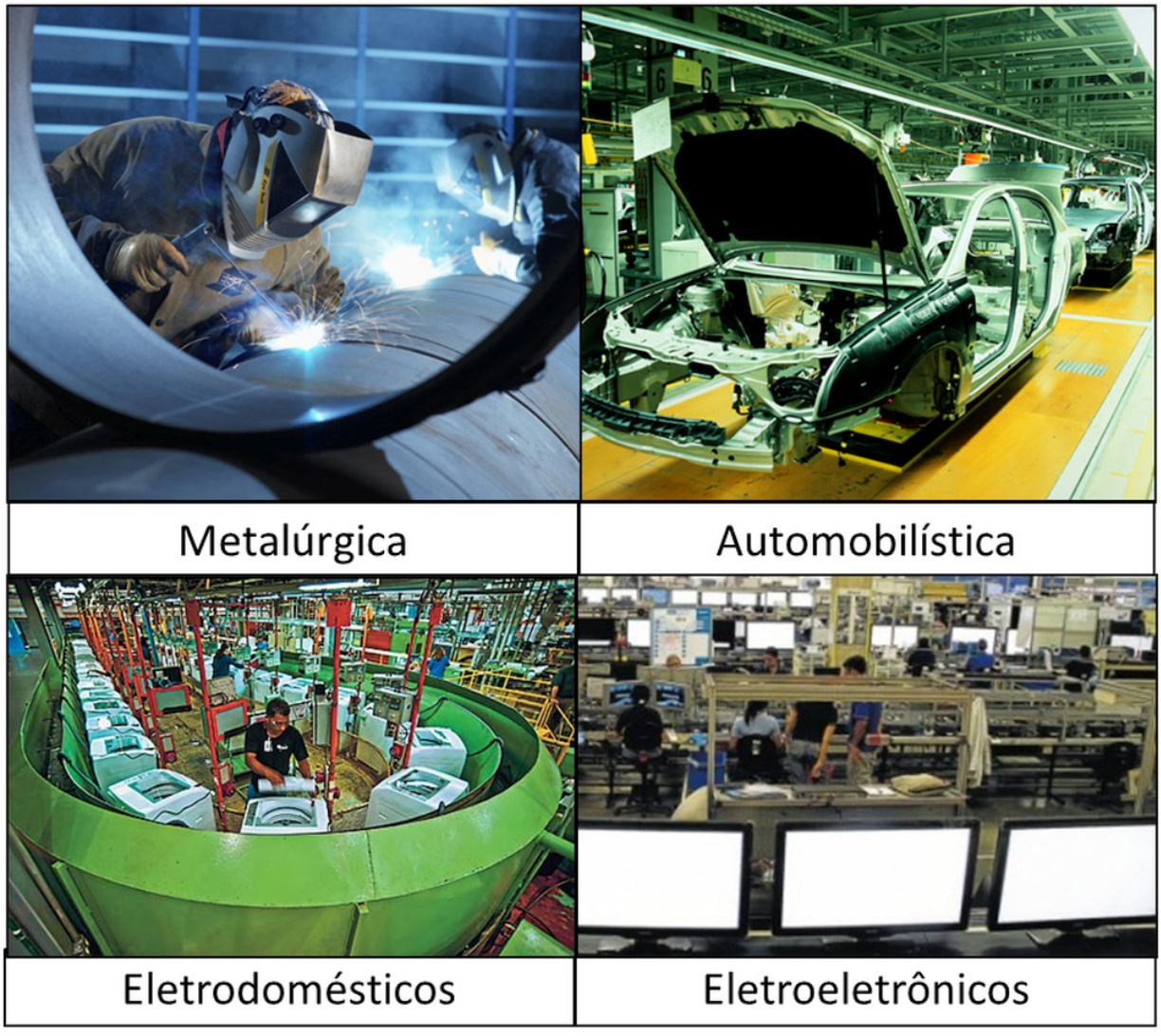


Fonte: Pereira (2016).

Por fim, para verificar cenários de IoT, foram simulados três ambientes: industrial, logístico e comercial.

• **Ambiente industrial**: O ambiente industrial proposto por Pereira e Avanço (2017) compreende as indústrias metalúrgica, automotiva, de eletrodomésticos e de eletroeletrônicos (**Figura 24**). Nesses locais, o RFID já é usado para o controle do processo produtivo, identificando item a item.

Figura 24. Tipos de indústria



Fonte: Pereira (2016).

Nessas indústrias, os obstáculos na comunicação são gerados basicamente por metais, e as etiquetas são fixadas no metal ou em algumas superfícies plástica (PEREIRA, 2016). Para simular essa situação no laboratório, Pereira e Avanço (2017) utilizou ap e pl compostos dos materiais do **Quadro 3**.

Quadro 3. Anteparos e placas para os Ambientes simulados.

AMBIENTE	ITEM	MATERIAIS
Industrial	Anteparo	Aço e alumínio.
Industrial	Placa	Aço, alumínio, policarbonato e PVC.
Logística	Anteparo	Aço, alumínio, eucalipto e papelão.
Logística	Placa	Eucalipto e papelão.
Comercial	Anteparo	Pínus, eucalipto, MDF e MDP.
Comercial	Placa	Pínus, eucalipto, MDF e MDP.

Fonte: Pereira e Avanço (2017).

• **Ambiente de logística e armazenagem:** As maiores fontes interferentes nesse ambiente (**Figura 25**) se dão pela presença de obstáculos gerados por empilhadeiras (metais), paletes de madeira e caixas de papelão. Além disso, as etiquetas são fixadas nas embalagens de papelão ou nas superfícies dos paletes (PEREIRA, 2016). Portanto, os materiais de *ap* e *pl* estão no **Quadro 4**.

Figura 25. Exemplo de Ambiente de Logística e Armazenagem.

Fonte: Pereira (2016).

• **Ambiente comercial e doméstico:** Esses ambientes compreendem os locais onde a presença de mobiliário é inerente. São eles: hotéis, residências, escritórios e hospitais. Nesses espaços, a maior fonte de obstrução de comunicação entre antena e etiqueta RFID é a própria mobília. Com os três ambientes caracterizados realizaram-se três ensaios, um por ambiente, com diferentes configurações de obstáculos e placas conforme **Quadro 4**.

Quadro 4. Configurações de Ensaio.

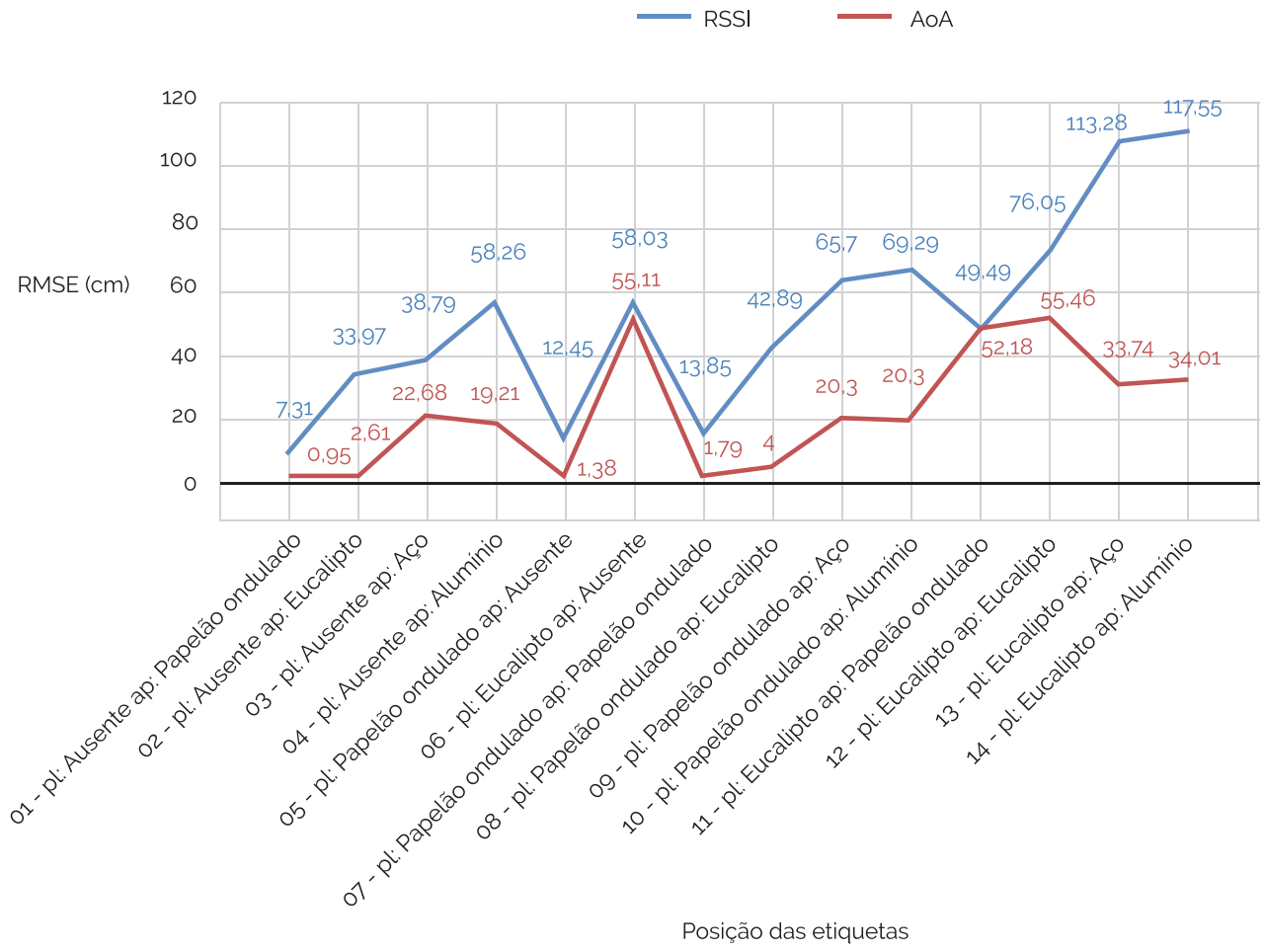
	ENSAIO 01 - INDUSTRIAL		ENSAIO 02 - LOGÍSTICA		ENSAIO 03 - COMERCIAL	
CONF.	AÇO	AUSENTES	PAPELÃO	AUSENTES	MDF	AUSENTES
1	Alumínio	Ausentes	Eucalipto	Ausentes	MDP	Ausentes
2	Ausentes	Policarbonato	Aço	Ausentes	Pínus	Ausentes
3	Ausentes	PVC	Alumínio	Ausentes	Eucalipto	Ausentes
4	Ausentes	Aço	Ausentes	Papelão ondulado	Ausentes	MDF
5	Ausentes	Alumínio	Ausentes	Eucalipto	Ausentes	MDP
6	Aço	Policarbonato	Papelão ondulado	Papelão ondulado	Ausentes	Pínus
7	Alumínio	Policarbonato	Eucalipto	Papelão ondulado	Ausentes	Eucalipto
8	Aço	PVC	Aço	Papelão ondulado	MDF	MDF
9	Alumínio	PVC	Alumínio	Papelão ondulado	MDP	MDF
10	Aço	Aço	Papelão ondulado	Eucalipto	Pínus	MDF
11	Alumínio	Aço	Eucalipto	Eucalipto	Eucalipto	MDF
12	Aço	Alumínio	Aço	Eucalipto	MDF	MDP
13	Alumínio	Alumínio	Alumínio	Eucalipto	MDP	MDP
14	Aço	Ausentes	Papelão ondulado	Ausentes	Pínus	MDP
15	-	-	-	-	Eucalipto	MDP
16	-	-	-	-	MDF	Pínus
17	-	-	-	-	MDP	Pínus
18	-	-	-	-	Pínus	Pínus
19	-	-	-	-	Eucalipto	Pínus
20	-	-	-	-	MDF	Eucalipto
21	-	-	-	-	MDP	Eucalipto
22	-	-	-	-	Pínus	Eucalipto
23	-	-	-	-	Eucalipto	Eucalipto
24	-	-	-	-	MDF	Ausentes

Fonte: Pereira (2016).

As **Figuras 26, 27 e 28** apresentam gráficos dos resultados dos três ensaios realizados, nos quais tem-se o RMSE (Root Mean Square Error) para cada configuração.
Figura 26 – Resultados ambiente industrial.

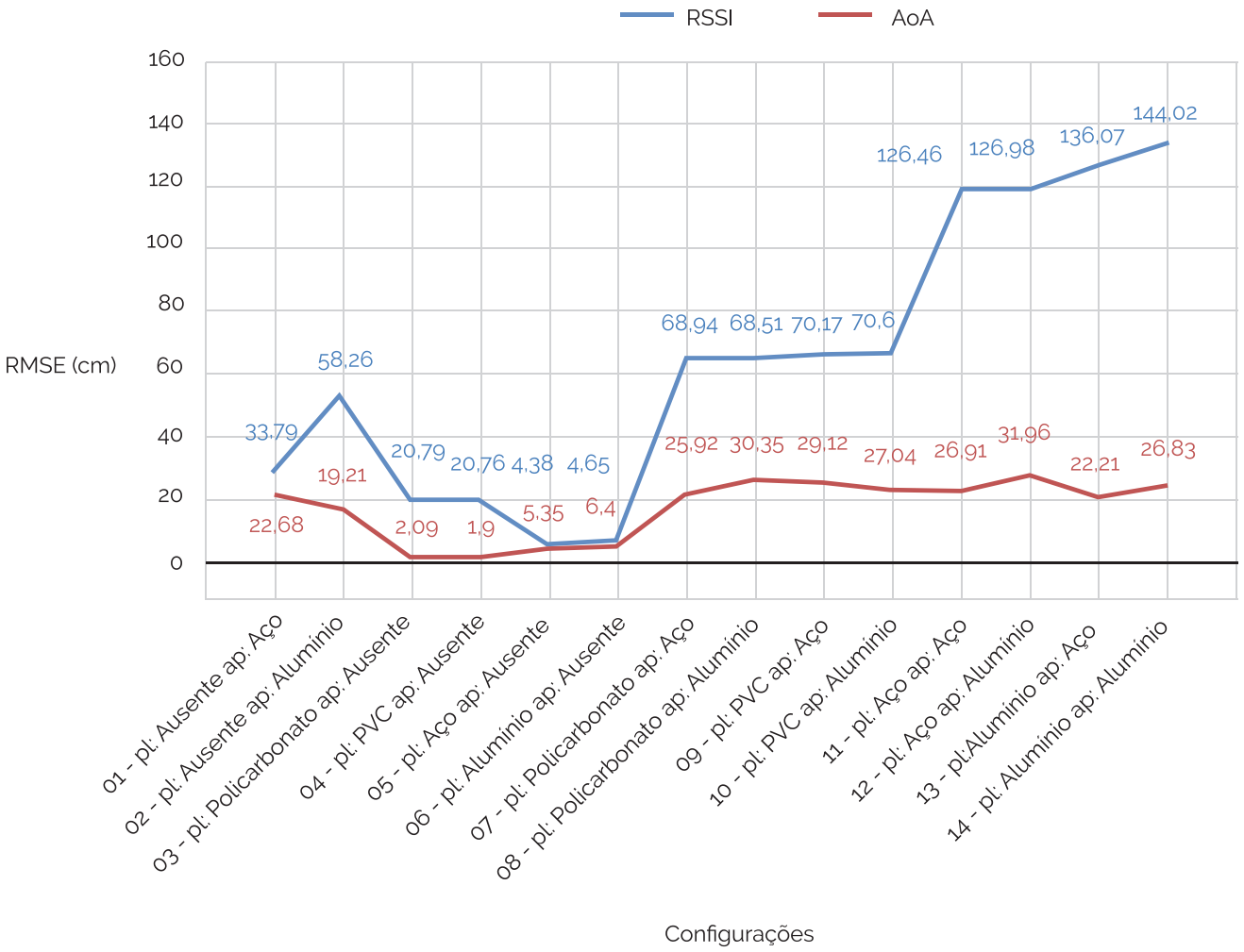
Pereira (2016) constata o não funcionamento da técnica ToA quando são utilizados equipamentos comerciais na construção de um RTLS baseado em RFID, como é o caso do SLER. Isso ocorre devido à resolução de tempo dos leitores RFID comerciais que não são suficientes para a realização dos cálculos. Portanto não há resultados para essa técnica, restando apenas as técnicas AoA e RSSI.

Figura 26. Resultados ambiente industrial.



Fonte: Pereira (2016).

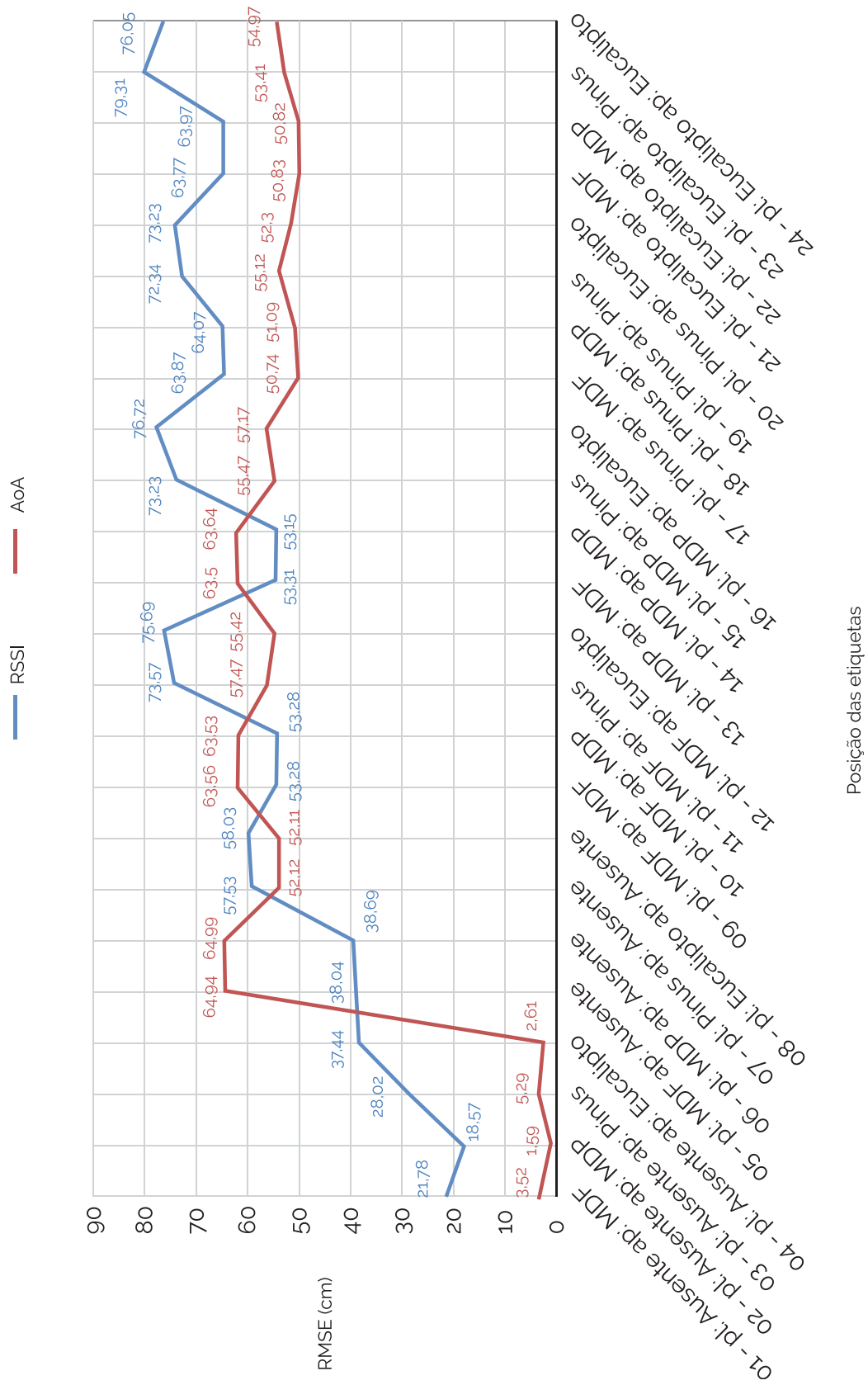
Figura 27. Resultados ambiente de logística.



Fonte: Pereira (2016).

Observamos nos gráficos das **Figuras 26, 27 e 28** que em algumas situações a localização fica inviável, com RMSE superiores a 50 centímetros. Porém, de maneira geral a técnica AoA é mais exata. Entretanto ainda é possível usar RSSI em determinadas situações em que a exatidão é menos requerida, pois ela tem uma maior facilidade de implementação.

Figura 28. Resultados ambiente comercial



Fonte: Pereira (2016).

2.4 RTLS BASEADO EM RFID E SUAS APLICAÇÕES EM CIDADES INTELIGENTES E INDÚSTRIA 4.0

De maneira geral, a comunidade acadêmica apresenta um grande número de aplicações de sucesso em RTLS que empregam RFID. Brennan e Kolaja (2014) expuseram um método de localização baseado na potência do sinal das etiquetas (RSSI). Zhou, Zhang e Mo (2011) utilizaram o ângulo de chegada do sinal de radiofrequência das etiquetas (AoA) para prover a localização de etiquetas RFID. Já Kim et al. (2011) propuseram um método de localização que combina AoA com ToA (método que utiliza o tempo de propagação dos sinais).

No entanto, os melhores resultados advêm de estudos laboratoriais em ambientes controlados ou de simulações computacionais. Quando se analisa situações reais, considerando obstáculos de ambientes reais, a exatidão dos sistemas cai consideravelmente. Em algumas situações a utilização desses sistemas se torna inviável. Como é o caso do trabalho proposto por Pereira (2016), que compara duas técnicas consolidadas de localização *indoor* de etiquetas RFID, avaliando os efeitos das interferências de ambientes reais. Portanto, a realização de um site survey é fundamental para a instalação de qualquer projeto de RTLS.

O *site survey* é uma inspeção técnica realizada nos locais onde serão instaladas as aplicações que usam equipamentos de radiofrequência de uma rede sem fio. Através do *survey* é possível prever de antemão as situações em que a determinação da localização dos objetos não é viável, e assim tomar medidas para contornar essas situações. Apesar dos problemas de exatidão causados pelas interferências, os RTLSs baseados em RFID são viáveis em grande parte dos casos, principalmente quando implementados através de *site surveis*, tendo como ponto favorável o baixo custo quando comparados a outros sensores de localização *indoor*.

Quando as interferências chegarem a níveis que tornem inviável a localização, pode-se combinar o RFID com outras tecnologias, como: reconhecimento de imagem, sensores de passagem, sensores de obstáculos, os próprios portais RFID delimitando a passagem em locais demarcados (salas, galpões, quadrantes em um centro de destruição), entre outras. Evidentemente, nesses casos os sistemas terão um maior custo de implementação.

Tendo em vista essas perspectivas e desafios, vemos no futuro dois cenários promissores em que os RTLSs baseados em RFID podem ser fundamentais. São eles: as Cidades Inteligentes e a Indústria 4.0.

a) Cidades Inteligentes

O mundo vem passando por um rápido processo de urbanização nas últimas décadas, e existem projeções que indicam que dois terços da população mundial serão urbanas em 2050 (UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, 2014). Portanto esse crescimento não planejado ameaça o desenvolvimento sustentável e

pressiona as infraestruturas das cidades em torno do mundo. A infraestrutura é crucial para muitos aspectos das áreas urbanas, a exemplo do setor de transportes, em que suas modalidades necessitam ser cada vez mais eficientes, modernas e integradas com tecnologias da informação (TIC). Essa integração de infraestrutura com a TIC, como sabemos, é fundamental para o desenvolvimento das Cidades Inteligentes.

Devido a essa superpopulação já presente e às projeções futuras, é cada vez mais emergencial o surgimento de novos meios de transportes para pessoas e "coisas", e, consequentemente, tecnologias para suas respectivas geolocalizações. Nesse contexto, os RTLSs possuem um vasto campo de exploração.

Como já mencionado neste capítulo, em ambiente outdoor os sistemas GNS, principalmente o GPS, já estão consolidados. Deixam, assim, espaço para a integração de sistemas de localização baseados em RFID para os ambientes indoor, de maneira a complementar as áreas de sombra presentes na cobertura atual das cidades. É preciso pontuar, no entanto, a importância de se lembrar das limitações de exatidão dos sistemas de localização indoor de acordo com o local e aplicação almejados.

b) Indústria 4.0

O desenvolvimento dos conceitos de Indústria 4.0 e manufatura avançada, ou ainda IIoT (do inglês *Industrial Internet of Things*), nos últimos anos tem exercido um impacto considerável sobre muitas soluções tecnológicas, e como não seria diferente, também nos RTLSs.

A nova visão induzida pela próxima revolução industrial almeja maior produtividade, identificação das etapas do processo, redução significativa nas falhas, queda de custos e melhoria da eficiência dos fluxos de produtos dentro e fora do processo produtivo. Nesse contexto, a localização *indoor* com RFID tem muito a contribuir, fornecendo um melhor rastreio dos fluxos internos e externos da produção com um baixo custo. Além do mais, hoje o setor industrial já utiliza etiquetas RFID para identificação de produtos. Nesses casos haveria apenas a adição de uma nova aplicação, pois grande parte do investimento inicial já faz parte do arcabouço industrial.

REFERÊNCIAS

BOUET, M.; DOS SANTOS, A. L. RFID tags: Positioning principles and localization techniques. In: IFIP WIRELESS DAYS, 1., 2008, Dubai. Proceedings... Piscataway: IEEE, 2008. p. 1–5.

BRENNAN, D.; KOLAJA, J. Real time location system using passive UHF RFID. In: INTERNATIONAL CARPATHIAN CONTROL CONFERENCE (ICCC), 15., 2014, Velke Karlovice. Proceedings... Piscataway: IEEE, 2014. p. 58-62.

BUFFI, A.; NEPA, P.; LOMBARDINI, F. A Phase-Based Technique for Localization of UHF-RFID Tags Moving on a Conveyor Belt: Performance Analysis and Test-Case Measurements. IEEE Sensors Journal, v. 15, n. 1, p. 387–396, Jan. 2015.

COLIN, E.; MORETTO, A.; HAYOZ, M. Improving indoor localization within corridors by UHF active tags placement analysis. In: IEEE RFID TECHNOLOGY AND APPLICATIONS CONFERENCE (RFID-TA), 2014, Tampere. Proceedings... Piscataway: IEEE, 2014. p. 181-186.

CREMER, M. et al. Improved UHF RFID localization accuracy using circularly polarized antennas. In: IEEE RFID TECHNOLOGY AND APPLICATIONS CONFERENCE (RFID-TA), 2014, Tampere. Proceedings... Piscataway: IEEE, 2014. p. 175-180.

HESSEL, F. et al. Implementando RFID na Cadeia de Negócios. 3. ed. Porto Alegre: ediPUCRS, 2013. 344 p.

KIM, D. K. et al. TDOA/AOA localization in RFID system using dual indirect Kalman filter. In: IEEE/SICE INTERNATIONAL SYMPOSIUM ON SYSTEM INTEGRATION (SII), 2011, Kyoto. Proceedings... Piscataway: IEEE, 2011. p. 440-445.

LAIRD TECHNOLOGIES. S9028PCR RFID Panel Antena. 2015. Disponível em: <http://www.lairdtech.com/products/s9028pcr>. Acesso em: 13 jan. 2016.

MENEGOTTO, J. L. Sensoriamento da edificação: um sistema de localização baseado em Beacons BLE. In: ENCONTRO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO NA CONSTRUÇÃO, 7., 2015, Recife. Anais... Rio de Janeiro: Blucher, 2015. p. 264–274.

PEREIRA, M. J. Análise das interferências do ambiente nas técnicas de rastreamento indoor de etiquetas RFID para Internet das Coisas. São Paulo, 2016. 162 f. Dissertação (Mestrado Profissional em Engenharia da Computação – Rede de Computadores) - Coordenadoria de Ensino Tecnológico, Instituto de Pesquisas Tecnológicas do Estado de São Paulo, São Paulo, 2016.

PEREIRA, M. J.; AVANÇO, L. Localização indoor baseada em sistemas RFID para o ambiente industrial e de logística. In: SIMPÓSIO BRASILEIRO DE AUTOMAÇÃO INTELIGENTE, 13., 2017, Porto Alegre. Anais... Campinas: Sociedade Brasileira de Automática, 2017. v. 1, p. 1583-1588.

SCHERHAUFL, M.; PICHLER, M.; STELZER, A. Robust localization of passive UHF RFID tag arrays based on phase-difference-of-arrival evaluation. In: IEEE TOPICAL CONFERENCE ON WIRELESS SENSORS AND SENSOR NETWORKS (WiSNet), 2015, San Diego, CA. Proceedings... Piscataway: IEEE, 2015. p. 47-49.

SILVA. R. B. C. Interface Homem-Máquina para Carro Elétrico baseada em Bluetooth Low Energy. Dissertação (Mestrado em Engenharia de Telecomunucações e Informática) - Escola de Engenharia, Universidade do Minho, Braga/Guimarães, Portugal, 2016.

UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS. Population Division. World Urbanization Prospects: The 2014 Revision Highlights. New York: DESA, 2014. (ST/ESA/SER.A/352).

ZHANG, Y.; LI, X.; AMIN, M. Principles and techniques of RFID positioning. In: BOLIC, M. et al. (Org.). RFID Systems: Research Trends and Challenges. Hoboken: Wiley, 2010. p. 389–415.

ZHOU, J.; ZHANG, H.; MO, L. Two-dimension localization of passive RFID tags using AOA estimation. In: IEEE INTERNATIONAL INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE, 2011, Binjiang. Proceedings... Piscataway: IEEE, 2011. p. 1-5.

3 REDES DE SENSORES SEM FIO

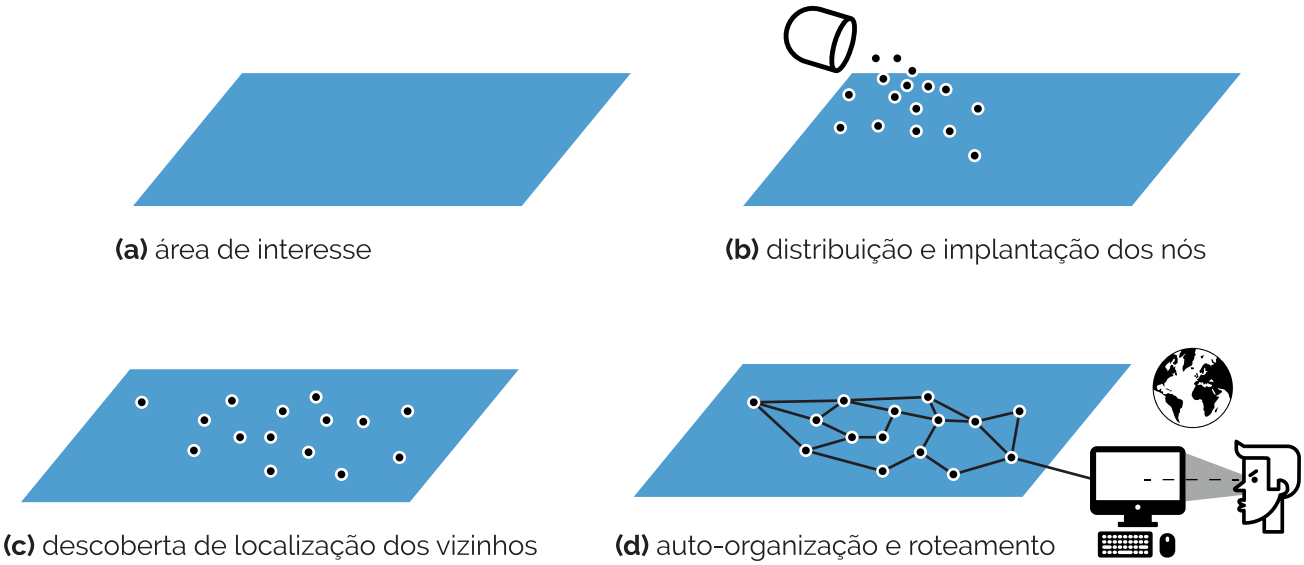
Uma rede de sensores é um sistema baseado em eventos, com vários nós sensores que transferem dados por um elemento especial, o qual se comporta como canal para encaminhar as informações para outras redes (LEE; NA; HUH, 2012). A taxonomia de uma rede de sensores utiliza as seguintes terminologias (TILAK; ABU-GHAZALEH; HEINZELMAN, 2002, tradução nossa):

- **Sensor:** dispositivo que detecta fenômenos físicos, faz medições ambientais e implementa características para a comunicação de dados, geralmente sem fio;
- **Observador:** usuário final interessado em obter informações divulgadas pela rede de sensores sobre o fenômeno. O observador pode indicar interesses (ou consultas) para a rede e receber respostas a essas perguntas. Vários observadores podem existir em uma rede de sensores;
- **Fenômeno:** entidade de interesse para o observador que está sendo detectada e analisada pela rede de sensores. Vários fenômenos podem ser observados concorrentemente na mesma rede;
- **Sorvedouro:** dispositivo destino das informações coletadas pelos sensores da rede. Em muitos casos, ele também se comporta como um elemento canal para encaminhar as informações para outras redes e enviar dados ao observador.

O cenário de rede de sensores envolve uma área geográfica de observação que terá os fenômenos monitorados por sensores estrategicamente colocados, que enviarão as informações ao observador. Assim, em um cenário tradicional, escolhe-se a área alvo (**Figura 29a**) e realiza-se a colocação dos sensores (**Figura 29b**), os quais se utilizarão de algoritmos para um reconhecimento da vizinhança (**Figura 29c**) e, por meio de auto-organização, estabelecerão uma rota de comunicação para transmitir o fluxo de dados ao observador (**Figura 29d**).

Nas próximas subseções são apresentados os desafios e métricas de desempenho de RSSF, assim como sua caracterização, a arquitetura de comunicação de dados e a do nó sensor e o detalhamento das características de nós sensores.

Figura 29. Cenário e etapas de implantação de RSSF.



(a) área de interesse

(b) distribuição e implantação dos nós

(c) descoberta de localização dos vizinhos

(d) auto-organização e roteamento

Fonte: Ruiz (2003).

3.1 DESAFIOS, MÉTRICAS E CARACTERIZAÇÃO DA RSSF

As características técnicas presentes em RSSF promovem desafios que devem ser trabalhados, a fim de aperfeiçoar a eficiência de RSSF. Nesse sentido, alguns fatores são levados em consideração na construção dos componentes (AKYILDIZ et al., 2002), como: custo de produção, tolerância a falhas, escalabilidade, requisitos construtivos para o hardware, topologia da rede, meio de transmissão de sinais, consumo de energia, local e condições ambientais de uso. Para definição e monitoramento da eficiência de um RSSF faz-se necessária a avaliação de métricas de desempenho, já que estas qualificam o nível de eficiência de fatores importantes (TILAK; ABU-GHAZALEH; HEINZELMAN, 2002, tradução nossa). Algumas métricas são:

• **Eficiência energética:** como os nós sensores são munidos de bateria, este recurso é fundamental para determinar a eficiência da RSSF em manter ativa a coleta de informações do fenômeno observado, que é determinada pela vida útil da rede. Este fator pode ser medido com métricas que avaliam o tempo até que a metade dos nós "morra" ou mesmo o tempo que o observador deixa de receber informação proveniente da RSSF;

• **Latência:** tempo de atraso no recebimento das informações que o observador está interessado em saber. Este fator está ligado diretamente aos requisitos da aplicação;

• **Exatidão:** a obtenção de informações corretas é o principal objetivo do observador, sendo que a exatidão é determinada pela aplicação. A infraestrutura deve ser adaptável para que o aplicativo obtenha a exatidão desejada com mínimo gasto energético;

• **Tolerância** a falhas: os sensores podem falhar devido a condições físicas, ou em razão da falha de um componente ou por ter ficado sem energia. Pode ser difícil substituir os sensores existentes, assim a rede deve ser tolerante a falhas, e se adaptar de tal forma que pequenas falhas sejam transparentes e não comprometam a aplicação;

• **Escalabilidade:** facilidade de crescimento e incorporação de novos elementos nas redes de sensores. Para redes de grande escala, este é um fator crítico, sendo que técnicas de localização de interações de grupos hierarquizados ou agregados podem favorecer a questão.

As redes de sensores podem ser utilizadas para diversos fins e conforme sua aplicação os modelos ou formas de uso podem variar, determinando assim, diferentes caracterizações (RUIZ, 2003). Resumidamente, as redes são caracterizadas segundo sua configuração, o tipo de sensoriamento, o tipo de comunicação ou mesmo o tipo de processamento que executa.

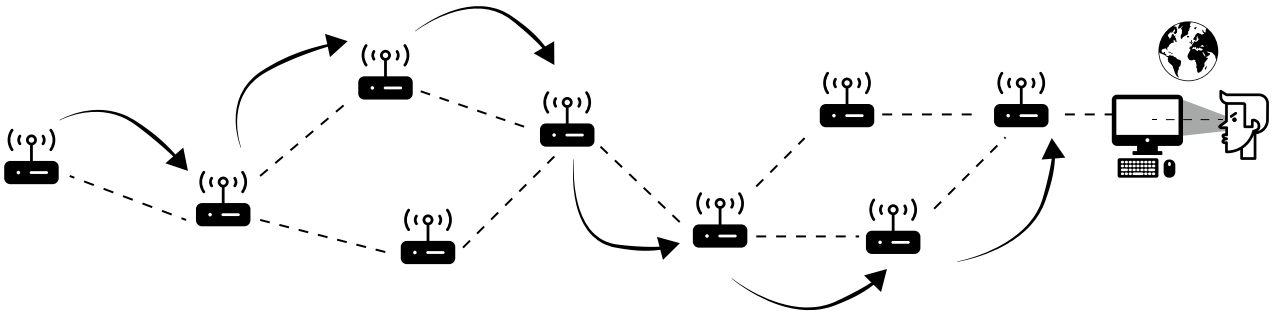
3.2 ARQUITETURA DE COMUNICAÇÃO DE DADOS

Em linhas gerais, a arquitetura de comunicação em RSSF pode ser compreendida em duas categorias: aplicação e infraestrutura (TILAK; ABU-GHAZALEH; HEINZELMAN, 2002). A categoria aplicação está relacionada com a maneira como as informações fluem do sensor até o observador. Estas podem ocorrer de forma cooperativa, pela qual um nó sensor se comunica com outros nós para obter a informação de interesse do observador, em um esquema de retransmissão multissalto, enquanto no modelo não cooperativo o dado flui sem a necessidade de utilização e cooperação de outros nós (**Figura 30** - Transmissão cooperativa em RSSF e **Figura 31**- Transmissão NÃO cooperativa em RSSF).

A categoria infraestrutura está associada à maneira de configurar, manter e operar a rede de sensores de forma otimizada e satisfatória para o observador. Pela característica dinâmica das RSSF, os modelos de comunicação de infraestrutura estão intrinsecamente ligados às métricas de desempenho da aplicação.

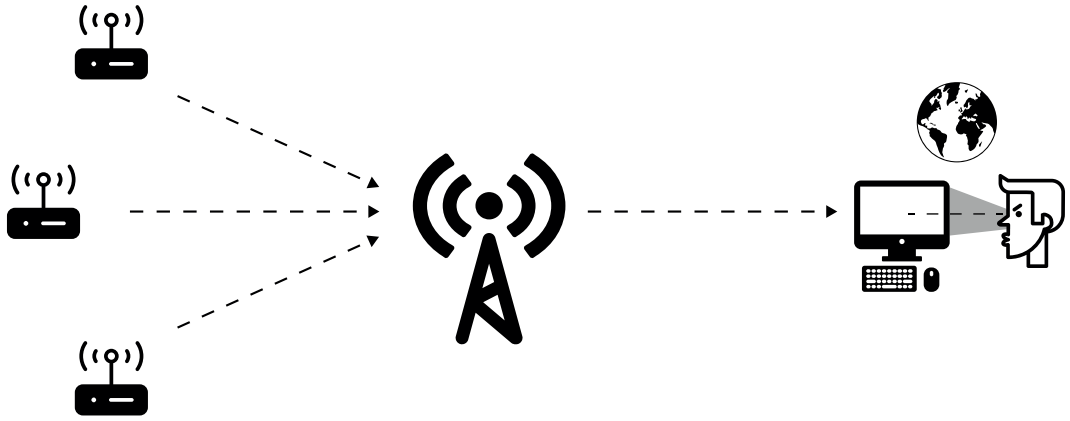
Em ambas, os protocolos de comunicação são fundamentais para obter o melhor resultado das RSSF. Nesse sentido, vários protocolos de comunicação estão disponíveis para uso, sendo que cada um tem seu objetivo, vantagem e desvantagem. Conceitualmente, os protocolos de comunicação são organizados em camadas, seguindo o modelo OSI (TANENBAUM; WETHERALL, 2011). Novos protocolos surgem, e atualizações acrescen-

Figura 29. Transmissão cooperativa em RSSF



Fonte: Elaborado pelo autor.

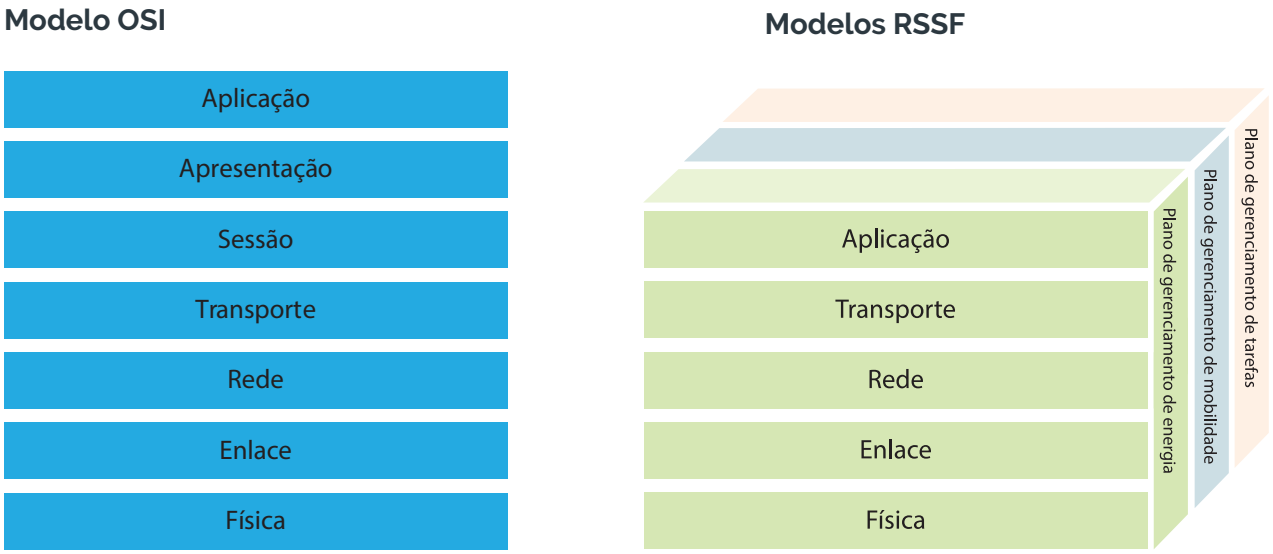
Figura 30. Transmissão NÃO cooperativa em RSSF



Fonte: Elaborado pelo autor.

tam novas características aos protocolos existentes, mas particularmente o modelo de RSSF segue a implementação dos modelos da pilha de protocolos, conforme apresentado na **Figura 12**: física, enlace, rede, transporte e aplicação. Além destes, existem protocolos multicamadas que estão associados aos planos de gerenciamento, seja no contexto de gerenciamento de tarefas, na questão de energia ou da mobilidade (AKYILDIZ et al., 2002).

Figura 32. Modelos de referência OSI e modelos para RSSF.



Fonte: Tanenbaum e Wetherall (2011, tradução nossa).

Fonte: Akyildiz et al. (2002, tradução nossa).

Os protocolos de camada física têm a função de realizar a transmissão física do sinal, sendo responsável pela seleção de frequência, escolha de portadora, detecção de sinal, modulação e encriptação de dados. Nos casos de RSSF, as comunicações podem ser por modelos óticos, infravermelho ou radiofrequência, sendo este último o mais comum.

Os protocolos de camada de enlace são responsáveis pela multiplexação dos fluxos de dados, detecção de frame de dados, acesso ao meio de comunicação e controle de erro de transmissão, dentre outras funções. A função característica desta camada é o Controle de Acesso ao Meio (MAC, do inglês *Medium Access Control*), pois se a RSSF for densa, vários nós podem estar acessando o meio ao mesmo tempo para transmitir dados. Assim, mecanismos e estratégias devem ser empregados para minimizar as colisões e aperfeiçoar as transmissões e recepções de dados.

Os protocolos de camada de rede têm como missão rotear mensagens de uma origem a um destinatário, encontrando um caminho viável e adequado às métricas de desempenho prioritárias para o tipo de aplicação e necessidades do observador.

Existem diversas formas de roteamento de informações entre os nós, e a eficiência da rede esta diretamente ligada à forma como os dados são efetivamente roteados.
Os tipos de roteamento são categorizados como: roteamento com centralização de dados, agregação de dados, hierárquico, baseado na localização, baseado na qualidade de serviços ou no fluxo de rede (AKKAYA; YOUNIS, 2005).

Os principais e mais conhecidos protocolos de camada de rede para RSSF são tipificados nessas categorias.

Os protocolos de camada de transporte nem sempre são empregados em RSSF, sendo que estes devem ser adaptáveis à perda de dados, ou com perdas minimizadas nos protocolos de camada de rede. No entanto, algumas aplicações necessitam de entrega 100% confiável de dados, de maneira que técnicas para aumentar a confiabilidade são empregadas em protocolos de transporte específicos.

Os protocolos de camada de aplicação no contexto de RSSF oferecem uma liberdade maior com relação às funcionalidades e responsabilidades. No entanto, algumas caracterizações podem ser encontradas, como por exemplo: protocolos de gerenciamento, designação de tarefas, disseminação de dados, alerta e aviso de dados.

O **Quadro 5** apresenta uma lista de exemplos de protocolos de comunicação em RSSF categorizados por camadas.

Quadro 5. Protocolos para RSSF.

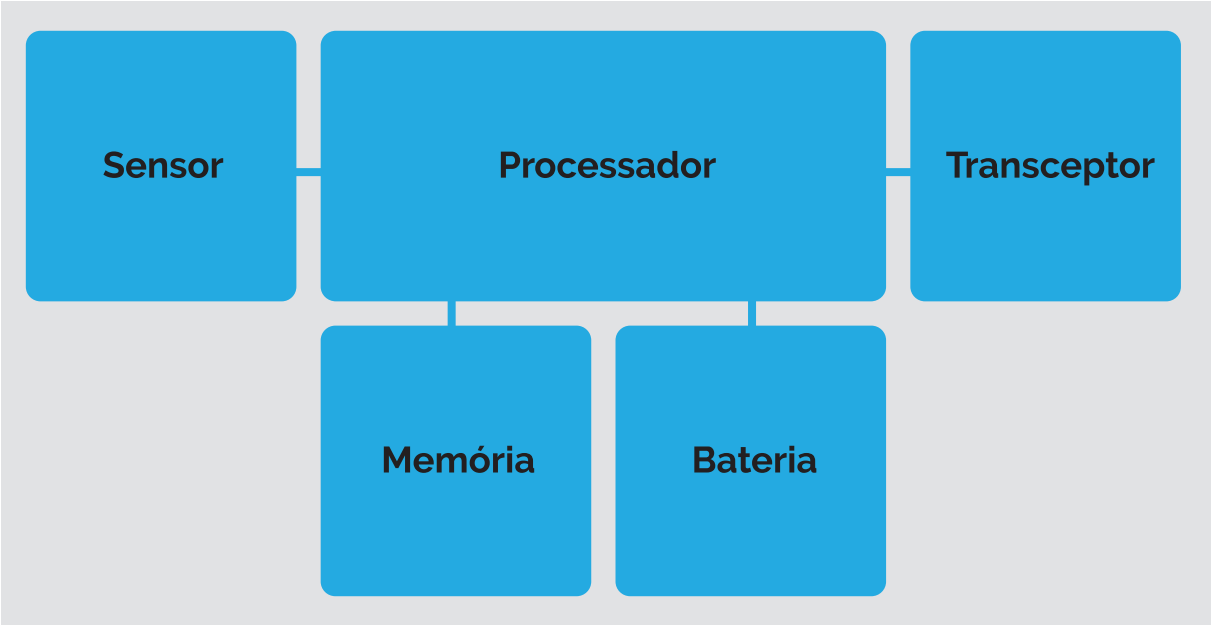
CAMADAS	PROTOCOLOS
Aplicação	SMP, TADAP, SQDDP
Transporte	PFSQ, ESRT, RMST
Rede	DD, SPIN, SAR, MULTI, STORM, PROC, TinyBeaconing, LEACH, LEACH-C, TEEN, PEGASIS, ICA, GEOMOTE, GEAR, GPSR,SPEED, SAR, GAF, MECN, SMECN, ACQUIRE, COUGAR, CADR, GDR, Directed Diffusion, Gossiping,
Enlace	S-MAC, ARC, T-MAC, B-MAC, DE-MAC, TRAMA
Física	Transmissão em radiofrequência (RF), ótico e infravermelho.

Fonte: elaborado pelos autores com dados de Ruiz et al. (2004), Akkaya e Younis (2005); Akyildiz (2002).

3.3 NÓ SENSOR

O nó sensor de RSSF geralmente tem dimensões pequenas. Apesar de não ser um requisito, podem existir sensores de maior porte. A tendência, no entanto, é serem cada vez menores. Em consequência disso, os componentes possuem recursos funcionais mais limitados. O hardware pode ser construído com diversas técnicas de circuito e abordagem arquiteturais (HEMPSTEAD et al., 2008). Porém conceitualmente seguem o mesmo princípio funcional (Figura 33): processador, memória, sensor, bateria, transceptor.

Figura 33. Blocos Funcionais do hardware de nós de RSSF.



Fonte: Elaborado pelo autor.

A bateria é o bloco funcional que fornece energia para o hardware do nó sensor, sendo caracterizado de alguns modos (SAVVIDES; PARK; SRIVASTAVA, 2001):

- **Modo linear:** a bateria é considerada um repositório de energia que se esvazia linearmente com o consumo dos componentes do hardware;
- **Modo dependente:** o recurso de energia da bateria é calculado com base na taxa de consumo e na taxa de redução de energia, que pode variar conforme as operações tradicionais da rede de sensores.;
- **Modo relaxado:** considera o fenômeno visto em baterias da vida real, no qual a tensão da bateria se recupera quando a taxa de descarga é reduzida.

O transceptor é o bloco funcional responsável pela comunicação. Os modos de comunicação de RSSF usam canais de radiofrequência, óticos ou infravermelhos. O modo ótico promove o menor consumo de energia, no entanto, os sensores devem estar dentro

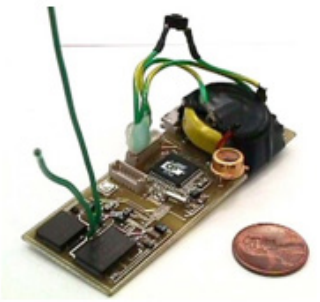
da visada e ter distância apropriada para comunicação. Os modelos com infravermelho também necessitam de visada e distância apropriadas, mas possuem o hardware mais econômico. O modelo de radiofrequência utiliza ondas eletromagnéticas em um espectro de frequência em conformidade com as regulamentações de telecomunicações.

Este é o modelo com maior consumo de energia. No entanto, as características técnicas como comunicação unidirecional, distância de transmissão regulada pela potência, assim como diversas técnicas de modulação, favorecem o emprego desta tecnologia, sendo este último o modelo mais utilizado em RSSF.

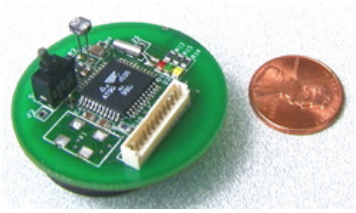
Os blocos funcionais processador e memória representam o módulo computacional do hardware do nó sensor, que processa instruções e dados, manipula e armazena dados na memória. O processador é a unidade responsável pela "inteligência" do equipamento, obtendo informações do bloco sensor e estabelecendo o elo entre o sensoriamento e a retransmissão de informações. Uma de suas principais características em RSSF é o baixo consumo de energia.

O sensor é o componente responsável pela digitalização das características do ambiente, gerando informação que representa o fenômeno a ser observado. Existem diversos tipos de sensores, e talvez seja mais lógico classificá-los de acordo com o fenômeno físico que captam (RAKOČEVIĆ, 2011). Exemplos deles são sensores mecânicos, térmicos, elétricos, magnéticos, radiantes, químicos e bioquímicos.
Os primeiros estudos acadêmicos em RSSF utilizavam nós sensores com componentes discretos, ou mesmo montados de acordo com a aplicação em foco. Exemplos deste cenário podem ser encontrados em projetos da Universidade da Califórnia, como: COTS Dust, Smart Dust (WARNEKE et al., 2001), WINS (POTTIE; KAISER, 2000) e JPL Sensor Webs (DELIN, 2002) do Jet Propulsion Lab da NASA (**Figura 34a e Figura 34b**).

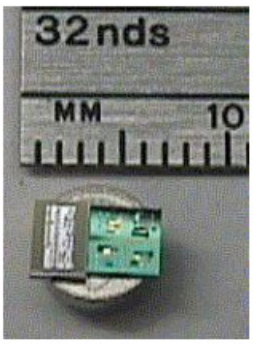
Figura 34a. Sensores de projetos acadêmicos de pesquisa.



COTS Dust: UC Berkeley



COTS Dust: UC Berkeley



Smart Dust: UC Berkeley

Fonte: Delin (2002); Pottie e Kaiser (2000); Warneke et al. (2001).

Figura 34b. Sensores de projetos acadêmicos de pesquisa.

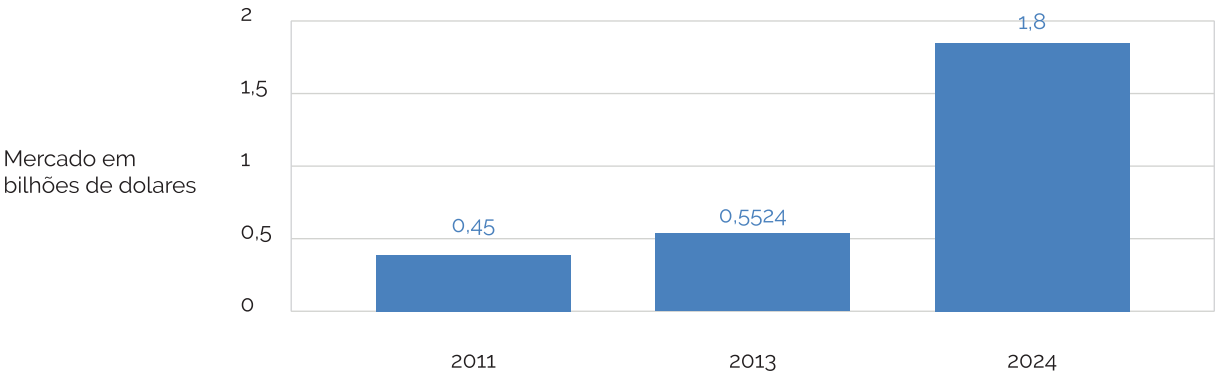
SensorWebs: JPL

WINS: Rockwell

Fonte: Delin (2002); Pottie e Kaiser (2000); Warneke et al. (2001).

Com o desenvolvimento da microeletrônica esses equipamentos tornaram-se mais populares e com maior aplicabilidade, sendo que a previsão futura é promissora e com demanda crescente. O Relatório Wireless Sensor Networks 2014-2024 apontou um crescimento futuro quatro vezes maior que o atual até 2021, chegando a um mercado de 1,8 bilhões de dólares (HARROP; DAS, 2014).

Figura 35. Evolução e projeção de mercado para RSSF.



Fonte: Adaptado de Harrop e Das (2014, tradução nossa).

Atualmente vários projetos utilizam nós sensores de RSSF provenientes de linhas de produção de empresas comerciais, os quais utilizam os sensores embarcados nos kits para montar cenários experimentais. Exemplos de kits podem ser visualizados na **Figura 36**, que apresenta as plataformas: IRIS (MEMSIC, 2014a); LOTUS (MEMSIC, 2014b); MICA (MEMSIC, 2014c); TelosB (MEMSIC, 2014d) e WaspMote (LIBELIUM, 2014).

Figura 36. Exemplos de nós de RSSF modernos.

MICAZ: MEMSIC

Microcontrolador Atmel ATmega128L, Padrão de comunicação IEEE 802.15.4; 2.4 até 2.48 GHz; Taxa de dados de 250kbps. Sensores: luminosidade, temperatura, umidade relativa, pressão barométrica, acelerômetro, acústico, magnético

LOTUS: MEMSIC

Processor de 32 bits Cortex M3 ® de 10 - 100MHz; 64kB SRAM, 512KB FLASH, FLASH 64MB Serial; Rádio 802.15.4 Integrado; Taxa de dados de 250 kbps, LED Indicador de Status; Sensores: luminosidade, temperatura, umidade relativa, pressão barométrica, acelerômetro, acústico, magnético

IRIS: MEMSIC

Microcontrolador ATmega1281, Padrão de comunicação IEEE 802.15.4; 2.4 até 2.48 GHz; Taxa de dados de 250 kbps. Sensores: luminosidade, temperatura, umidade relativa, pressão barométrica, acelerômetro, acústico, magnético

TELOSB: MENSIC

Microcontrolador TI MSP430 com 10kB RAM; Rádio com IEEE 802.15.4 com taxa de dados de 250 kbps. Sensores integrados: luminosidade, temperatura e umidade

WASPMOTE: LIBELIUM

Microcontrolador ATmega1281, com frequência de 14.7456 MHz; SRAM: 8KB; EEPROM: 4KB; FLASH: 128KB; SD Card: 2GB. Sensores diversos, como: CO, CO2, NO2, O3, CH4, H2S, NH3; temperatura, luminosidade, uumidade, material particulado (MP10), ultrassom, ruído; campos magnéticos, acelerômetro, GPS, etc.

Fonte: Libelium (2014); Memsic (2014a; 2014b; 2014c; 2014d).

Além dos exemplos anteriores, as condições de uso em ambiente externo impõem novos requisitos construtivos para os nós sensores. Sendo assim, existe a possibilidade de construir um encapsulamento apropriado para o nó sensor ou utilizar produtos encapsulados que já estão adaptados a essas condições (**Figura 37**).

Figura 37. Nós sensores encapsulados e preparados para uso externo.

ĒKO PRO SERIES: MEMSIC
Grau de proteção: IP66 (protegido contra poeira e jatos de água de alta pressão); Temperatura de operação:-40°C a +60°C (duração da bateria degradada acima 50°C); Umidade de operação: 0 a 100% RHI, condensação; Temperatura de armazenamento:-45°C a +70°C (sem bateria)

Fonte: Memsic (2011)

WASPMOTE PLUG-AND-SENSE: LIBELIUM
Grau de proteção: IP65; Resistência ao impacto: IK08; Isolação da tensão AC: 690 V; Isolação da tensão DC: 1000 V; A temperatura ambiente de operação: -10° C a 50 ° C;

Fonte: Libelium (2014).

3.4 PERSPECTIVAS DE RSSF PARA CIDADES INTELIGENTES E INDÚSTRIA 4.0

Redes de sensores sem fio têm sido impulsionadas pelo mercado por uma nova tendência que envolve a melhoria de qualidade de vida das pessoas em um movimento caracterizado como Cidades Inteligentes e uma maior competividade das empresas em um processo caracterizado como Indústria 4.0. Esses dois cenários são tecnologicamente utilizados dentro de um conceito de Sistemas Ciberfísicos, definido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) como sistemas inteligentes que integram redes de componentes físicos com modelos computacionais, formando uma infraestrutura estruturante, altamente interconectada e integrada, e fornecendo novas funcionalidades para melhorar a qualidade de vida e possibilitar avanços tecnológicos em áreas críticas.

Uma camada sensorial captura o fenômeno físico desejado, transformando-o em sinal digital, que é transmitido e integrado a uma plataforma cibernética. Ela processa e realiza análises com modelos de decisão computacional, podendo retroalimentar a camada sensorial que, por sua vez, pode atuar no meio físico, criando um ciclo integrado entre o meio físico e o cibernético (CPS, do inglês Ciberphysical systems). As RSSF têm um papel importante na composição da camada sensorial, sendo muitas vezes enquadrada em um contexto de Internet das Coisas.

As RSSF sempre tiveram sua implementação muito alinhada com a aplicação, não sendo comum que uma mesma infraestrutura de RSSF seja utilizada para aplicações diferentes, sem que haja adaptações e aprimoramentos. Hoje, a questão de uso de padrões internacionais e modelos de interoperabilidade tornaram-se um requisito para várias implementações de soluções com RSSF, recebendo uma "roupagem" de Internet das Coisas. Nesse contexto, soluções de RSSF no padrão 802.15.4 ganham mais simpatia, mas é comum ver a opção por redes mais populares como 802.11 *(Wi-Fi*). No mundo das indústrias, a conectividade com padrões, protocolos e tipos de redes industriais tornou-se essencial para o sucesso de uma implementação que envolva a adaptação ou a migração de um processo produtivo para os moldes da Indústria 4.0. Já no mundo das cidades, a possibilidade de instrumentar todo município com tecnologias instaladas em grande área territorial, comunicando-se de forma sem fio, amplia os horizontes de utilização dessa tecnologia, com grande benefício para a sociedade.

3.4.1PERSPECTIVAS PARA A INDÚSTRIA 4.0

A aplicação de RSSF no mundo industrial é factível e aplicável principalmente no controle e monitoramento funcional de uma variedade de aplicações, a exemplo de controle de processos, prevenção de acidentes, monitoramento de áreas contaminadas, sistemas inteligentes de transporte, aplicações de diagnóstico de falhas em equipamentos e máquinas e monitoramento de processos industriais por câmeras inteligentes de reconhecimento de imagens em tempo real. Como mencionado por Güngör e Hancke (2013), todas essas aplicações envolvem desafios significativos no contexto de conectividade, confiabilidade, latência e eficiência energética.

As RSSF normalmente oferecem uma implementação menos onerosa, com maior escalabilidade, flexibilidade, mobilidade dos sensores e facilidade na implantação. No entanto, ter possibilidade de usar tanto mecanismos de comunicação sem fio como também com fio é importante para expandir a capacidade de uso no ambiente industrial, uma vez que o ambiente onde os sensores são instalados pode exigir requisitos estruturais de maior resistência, com difícil acesso ou mesmo com interferência eletromagnética. Dependendo do cenário, podem ser encontradas dificuldades para comunicação sem fio, com maior aplicabilidade para redes cabeadas. Pode haver casos, no entanto, em que o cenário é inverso.
Toda essa instrumentação com RSSF proporcionará uma nova gama de informações dos processos, de maneira on-line, possibilitando o tratamento e processamento de dados,

com mecanismos computacionais inteligentes (*Big Data*, Inteligência Artificial, computação cognitiva etc.), os quais permitirão trabalhar novas formas de produção, de maneira rápida e flexível, ajustando a capacidade e diminuindo os custos. Essa situação seria inserida em um contexto de Sistemas Ciberfisícos, em que a RSSF teria um papel fundamental na formação da camada sensorial dos fenômenos e parâmetros industriais. Nos cenários industriais, o uso de RSSF muitas vezes está encapsulado como o nome de soluções de IIoT (*Industrial Internet of Things*).

Cabe ressaltar um processo cultural natural na inserção de novas tecnologias em ambiente industrial, principalmente as capitaneadas pela área de Tecnologia da Informação (TI), caso da Internet das Coisas. Neste setor, historicamente a Tecnologia de Automação (TA) é utilizada na indústria de forma distinta, técnica e culturalmente, da TI. A TA tem ampliado o uso de recursos de TI em sua operação e essa aproximação é denominada de Convergência TI/TA, afetando principalmente as concepções tecnológicas das soluções. Apesar dessa aproximação, ainda existe uma distância cultural entre os dois ambientes. A tomada de decisão, todavia, não é integrada, cabendo uma maior sinergia para obter a melhor alternativa de infraestrutura, seja de TA, de TI ou de ambas. A alta administração das indústrias sempre tem buscado ações para otimizar a operação dos ambientes industriais, diminuindo eventuais falhas e consequentemente melhorando o retorno do investimento realizado e o desempenho financeiro, ainda que olhem as inovações neste setor de forma bem conservadora.

3.4.2 CIDADES INTELIGENTES

O tema Cidades Inteligentes tem sido discutido frequentemente e com inúmeros casos emergindo em diversas partes do mundo, sempre objetivando, em termos gerais, a melhoria da qualidade de vida dos cidadãos. As soluções ou concepções apresentam diversos cenários de infraestrutura, arquitetura e modelos de implementação, uma com aspectos mais tecnológicos, outras com caráter mais social ou sustentável, e assim por diante. No contexto aqui discutido, que é tecnológico, a importância da RSSF está diretamente ligada à capacidade de "sentir" a cidade, por meio de sensores que tocam fisicamente a urbe. Da mesma forma como aplicado no contexto da Indústria 4.0, as RSSF têm sua função principal na camada sensorial de Sistemas Ciberfísicos.

A instrumentação da cidade normalmente envolve uma vasta região territorial, sendo necessário um planejamento mais rigoroso no que tange à distribuição e ao posicionamento dos dispositivos sensores, esclarecendo vários pontos técnicos, como por exemplo:

- Os padrões e tecnologias de comunicação a serem utilizados para cada cenário de uso;
- A manutenção e manipulação física dos sensores, que em cidades são onerosas e podem gerar complexidade logística e operacional quando se aplicam à implantação

de quantidade expressiva de sensores;
• A questão energética, pois quanto maior a periodicidade, a quantidade e a estratégia de transmissão do dado coletado pelos sensores, maior será o consumo de energia do dispositivo, e dependendo do sensor, nem sempre ele terá provimento de energia ilimitada;
• O gerenciamento e a governança de todo o ecossistema sensorial, questão que nem sempre é bem equacionada na implementação de RSSF;
• As questões da segurança, pois na concepção de soluções elas são tratadas em momentos avançados do planejamento ou durante a execução do projeto.

A abrangência de áreas que são cobertas pelo contexto de Cidades Inteligentes é enorme, sendo possível encontrar diversas subdivisões que se estendem e derivam do termo tradicional inglês, como: smart health, smart building, smart transportation; smart water, smart grid (energia), smart environment etc. A complexidade de cada subdivisão impacta razoavelmente na forma como as soluções surgem nas cidades, sendo normal encontrar soluções não integradas ou que não têm uma interface bem definida com outros meios digitais disponíveis na mesma cidade, seja no nível municipal, estadual ou federal. Claro que o potencial de melhoramento das cidades com o conceito de Sistemas Ciberfísicos é notório, mas o modelo de negócio, gestão e melhor uso da tecnologia é um processo de amadurecimento, pelo qual cada cidade tem que passar, considerando a sua vocação e apetite por inovação.

Pelo ponto de vista funcional, o sensoriamento viabilizado pelas RSSF cria uma nova camada de informação, a qual amplia e cria uma renovada perspectiva de análises das cidades. Desta forma, padrões, comportamentos e situações que antes eram desconhecidos passam, com o processamento de enormes quantidades de dados de fontes variadas e com modelos computacionais de interpretação, a oferecer novas fronteiras para a gestão de cidades.

Por fim, tanto o ambiente de cidades quanto o ambiente das indústrias ainda estão em estágios embrionários, e o amadurecimento e utilização de tecnologias já bem trabalhadas como RSSF e outras do ambiente ciberfísico tendem a agregar valor e minimizar os problemas e riscos em um ambiente tão inovador. Vale lembrar que as saídas de estágios embrionários necessariamente deverão passar por fases de crescimento e amadurecimento tecnológico e humano. Se formos realizar uma analogia com os seres humanos, pontuamos que demoramos meses para gatinhar, pelo menos um ano para andar, anos para aprender a ler e interpretar a escrita, e muitos anos mais para nos especializarmos em assuntos complexos. Se transpormos este modelo para as cidades, o cenário não é muito diferente em termos de cronologia, mas não somos tão tolerantes com prazos excessivamente longos para o avanço tecnológico. Esse entendimento tem que ser levado em consideração quando pensamos nos resultados a serem obtidos em soluções sobre Cidades Inteligentes e Indústria 4.0. Isto é, não é possível exigir uma solução madura e altamente eficiente logo na partida da concepção, mas tampouco esperar muito para ver o progresso e a evolução dos sistemas. Encontrar um cenário harmonioso, sabemos, não é um desafio fácil.

REFERÊNCIAS

AKKAYA, K.; YOUNIS, M. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, v. 3, n. 3, p. 325-349, Nov. 2005.

AKYILDIZ, I. F.et al. A survey on sensor networks. IEEE Communications Magazine, v. 40, n. 8, p. 102-114, Aug. 2002.

DELIN, K. A. The sensor web: a macro-instrument for coordinated sensing. Sensors, v. 2, n. 7, p. 270-285, July 2002.

GÜNGÖR, V. Ç.; HANCKE, G. P. Industrial wireless sensor networks: applications, protocols, and standards. Boca Raton: CRC Press, 2013.

HARROP, P.; DAS, R. Wireless Sensor Networks (WSN) 2014-2024: forecasts, technologies, players. [S.l.: s.n.], 2014.

HEMPSTEAD, M. et al. Survey of hardware systems for wireless sensor networks. Journal of Low Power Electronics, v. 4, n. 1, p. 11-20, Apr. 2008.

LEE, G.; NA, S. H.; HUH, E. N. Modeling for congestion prediction in wireless sensor network using traffic demands analysis. Montreux, Switzerland: Wseas Press, 2012. p. 206-211.

LIBELIUM. Waspmote Technical Guide - Document version: v5.5. Disonível em: <http://www.libelium.com/downloads/documentation/waspmote_technical_guide.pdf>. Acesso em: 01 nov. 2014.

MEMSIC. eKo Pro Series System. San Jose, California: 2011. Disponível em: <https://www.memsic.com/userfiles/files/Datasheets/WSN/ek2100_eko_pro_kit_datasheet.pdf>. Acesso em: 5 ago. 2019.

MEMSIC. IRIS Datasheet. San Jose, California: Memsic, 2014a.

MEMSIC. LOTUS Datasheet. San Jose, California: Memsic, 2014b.

MEMSIC. MICAz Datasheet. San Jose, California: Memsic, 2014c.

MEMSIC. TelosB Datasheet. San Jose, California: Memsic, 2014d.

POTTIE, G. J.; KAISER, W. J. Wireless integrated network sensors (WINS). Communications of the ACM, v. 43, n. 5, p. 51-58, May 2000.

RAKOČEVIĆ, G. Sensors. In: Application and multidisciplinary aspects of wireless sensor networks. London: Springer-Verlag, 2011. p. 13-31.

ROSALES, M. S.; GARCIA, G.; SANCHEZ, G. D. Efficient message authentication protocol for WSN. Wseas Transaction on Computers, v. 8, n. 6, p. 895-904, June 2009.

RUIZ, L. B. et al. Arquitetura de redes de sensores sem fio. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 2004, Gramado. Mini curso... Porto Alegre: Sociedade Brasileira de Computação, 2004. p. 167-218. Disponível em: <http://www.sbrc2004.ufrgs.br/cfps/minicursos_selecionados.html>. Acesso em: 5 maio 2018.

RUIZ, L. B. Maná: Uma arquitetura para gerenciamento de redes de sensores sem fio. Belo Horizonte: [s.n.], 2003.

SAVVIDES, A.; PARK, S.; SRIVASTAVA, M. On modeling networks of wireless microsensors. ACM SIGMETRICS Performance Evaluation Review, v. 29, n. 1, p. 318-319, 2001.

TANENBAUM, A. S.; WETHERALL, D. J. Redes de computadores. 5. ed. São Paulo: Prentice Hall, 2011.

TILAK, S.; ABU-GHAZALEH. N. B.; HEINZELMAN, W. A taxonomy of wireless micro-sensor network models. ACM SIGMOBILE Mobile Computing and Communications, v. 6, n. 2, p. 28-36, Apr. 2002.

WARNEKE, B., et al. Smart Dust: communicating with a cubic-millimeter computer. Computer, v. 34, p. 44-51, Jan. 2001.

4 TECNOLOGIAS CHAVE SOB UMA PERSPECTIVA DE SEGURANÇA DA INFORMAÇÃO

Todos os sistemas computacionais de alguma forma coletam, processam e transmitem informações em algum momento. As informações em conjunto com os processos, sistemas e meios de transmissão são importantes elementos para atingir os objetivos da empresa. Considerando os aspectos relacionados a Cidades Inteligentes e Indústria 4.0 vários fatores de segurança devem ser aprimorados para minimizar os riscos às informações e aos serviços públicos, assim como os riscos que afetem os resultados e competitividade das indústrias.

Sem levar em consideração que a tecnologia empregada para o manuseio da informação possui vulnerabilidades, o uso da informação a expõe aos riscos e vulnerabilidades inerentes a seu processo de manuseio.

O conceito de segurança da informação considera o elemento informação importante para os objetivos da empresa. Assim, deve ser protegida por meio de políticas, processos e controles.

Segundo a norma NBR ISO 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013) a segurança da informação, ou seja, suas políticas, processos e controles, está amparada em três principais pilares, a saber:

- Confidencialidade, para garantir que a informação esteja disponível somente a entidades autorizadas, não permitindo acessos não autorizados;
- Integridade, para garantir que a informação esteja completa e precisa, ou seja, sem adulterações em qualquer ponto do fluxo de trabalho, durante todo o seu ciclo de vida;
- Disponibilidade, para garantir que a informação esteja disponível aos interessados autorizados, sempre que necessário, ou quando for requisitado.

Além disso, para atender a necessidade de auditoria e legislação, outros pilares também podem ser considerados, como:

- Irretratabilidade, para garantir que a informação foi gerada por fonte autêntica e não permitir repúdio quanto à origem e autoria;
- Privacidade, para garantir que o dono ou gerador da informação tenha sua identidade preservada;
- Conformidade, para garantir que a informação gerada atenda aos requisitos regulatórios e legais.

Nos aspectos de segurança podemos traçar um paralelo dos pilares de segurança relacionados à IoT, no entanto, cada tecnologia apresenta desafios e aspectos diferentes de vulnerabilidades que podem ser discutidos de várias maneiras. Neste capítulo cada tecnologia habilitadora de IoT - RFID, RSSF e RTLS - será observada e analisada sob a ótica dos pilares de segurança, com as devidas indicações de artigos e referências que tratam os aspectos técnicos com mais detalhes.

4.1 RFID, RSSF E RTLS: UMA PERSPECTIVA DE SEGURANÇA DA INFORMAÇÃO

As características construtivas dos componentes das soluções que utilizam RFID não permitem implementar contramedidas sofisticadas contra ataques de segurança.
As soluções utilizadas em RSSF possuem bastantes semelhanças com as soluções de RFID, quando comparamos os recursos computacionais.

As soluções de segurança precisam se adaptar a esta realidade de recursos escassos. Um exemplo de adaptação efetuada trata-se dos protocolos leves de criptografia, desenvolvidos para prover segurança e privacidade em dispositivos com baixo poder computacional Juels (2006).

Segundo Hong, Yong e Zhang (2012), as vulnerabilidades dos sistemas RFID podem ser classificadas em três categorias:

1) Ameaças físicas:
- Acesso físico ao leitor;
- Acesso físico à tag;
- Cópia da tag;
- Interferência eletromagnética.

2) Ameaças de canal:
- Escuta do sinal transmitido;
- Reprodução de comunicação;
- Atraso na comunicação;
- Interferência por canal adjacente.

3) Ameaças de sistema:
- Falsificação de leitores;
- Rastreamento;
- Decodificação de senhas.

Segundo Khatawkar et al. (2013), as vulnerabilidades em RSSF podem ser exploradas em dois diferentes pontos de vista:

1) Mecanismos básicos: as características de propagação em um meio compartilhado como a comunicação sem fio já oferecem desafios. A instalação dos dispositivos em um

ambiente hostil e relativamente mais perigoso, sem proteção física, permite a exploração destas características de forma maliciosa;

2) Mecanismos de segurança: envolvem os protocolos de comunicação e criptografia e os elementos importantes da arquitetura como a distribuição e o controle de chaves criptográficas.

Complementarmente, Ashraf et al. (2009) propuseram um framework para classificação das ameaças em RSSF. O framework divide-se em múltiplos níveis. Assim, para cada um dos níveis do framework a seguir, podem ser relacionadas vulnerabilidades, ameaças e tipo de ataque:

- Rede;
- Enlace;
- Escoamento;
- Nó;
- Outros (desastres naturais e catástrofes).

As soluções de RTLS podem ser baseadas na tecnologia RFID, assim, entende-se que as vulnerabilidades de RFID também podem ser aplicadas às soluções para RTLS.
Nas próximas subseções serão apresentadas as características dos pilares de segurança aplicáveis a RFID, RSSF e RTLS, assim como experimentos que demonstram as situações de risco ou vulnerabilidade.

4.1.1 DISPONIBILIDADE

Em Segurança da Informação o pilar Disponibilidade tem como objetivo garantir a disponibilidade da informação aos interessados autorizados, sempre que necessário ou quando for requisitado.

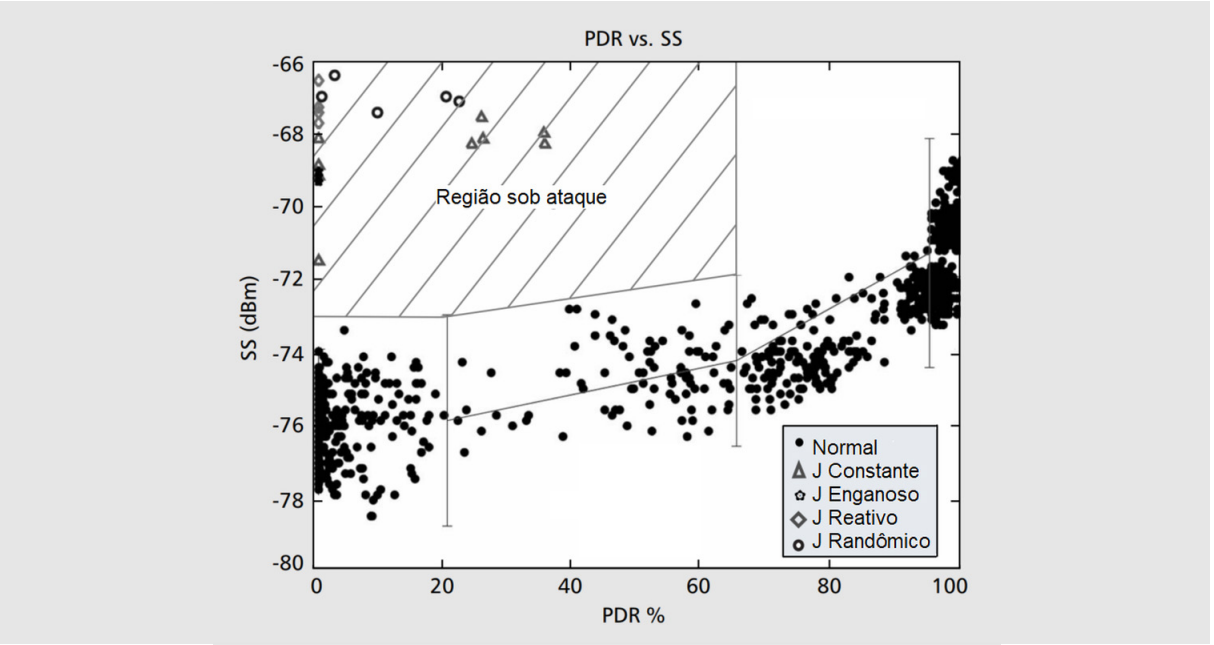
O trabalho realizado por Xu et al. (2006) apresenta um estudo do ataque jamming em redes de sensores sem fio. Os ataques jamming são interferências em radiofrequência geradas intencionalmente e podem ser classificados como:

- **Jammer constante:** quando o atacante envia um sinal de radiofrequência contínuo na frequência de operação do sistema que se pretende atacar;
- **Jammer enganoso:** quando o atacante envia pacotes com características normais constantemente. Assim, o sistema interpreta uma comunicação legítima acontecendo e aguarda indefinidamente para realizar a comunicação;
- **Jammer randômico:** quando o atacante envia pacotes com características normais de forma randômica,.Nos momentos do envio malicioso os demais participantes da comunicação aguardam como se houvesse comunicação legítima acontecendo;
- **Jammer reativo:** o atacante ouve o canal e só envia sinal para ocupar o canal quando percebe que os participantes da comunicação iniciam a comunicação, assim ele

ocupa quase que a totalidade do tempo de comunicação com conteúdo malicioso, não permitindo o correto funcionamento da rede.

A **Figura 38** mostra a comparação dos diferentes tipos de ataques jamming em RSSF. Cada tipo de ataque gera um efeito na intensidade do sinal (SS, do inglês *Signal Strhengh*) e na taxa de pacotes entregues (PDR, do inglês *Packet Delivery Ratio*).

Figura 38. Comparação de diferentes tipos de ataques jamming em RSSF.



Fonte: Xu et al. (2006, tradução nossa).

Xu et al. (2006) mostraram que as técnicas para identificação de ataque jamming em RSSF podem ser aprimoradas quando são realizadas análises multimodais, envolvendo mais de um parâmetro estatístico básico, obtidos na comunicação.

O trabalho realizado por Feldhofer, Aigner e Baier (2010) apresenta o desenvolvimento de protótipo de tags RFID baseados em microcontroladores e FPGA. Foram desenvolvidos dois conjuntos de protótipos, sendo um conjunto construído com microcontrolador e outro conjunto com FPGA. Cada conjunto possui um modelo para operar nas faixas de frequência de 13,56 MHz e outro operando na faixa de frequência de 868 MHz.
A **Figura 39** mostra um modelo de cada protótipo.

O propósito desses protótipos é explorar o funcionamento de tag RFID de forma customizável. No cenário proposto são explorados os ataques de negação de serviço que monitora a potência do sinal eletromagnético no canal adjacente ao utilizado para comunicação. Com essas informações são gerados sinais de interferência que interrompem a comunicação em momentos críticos do processo de comunicação entre leitor e tag RFID.

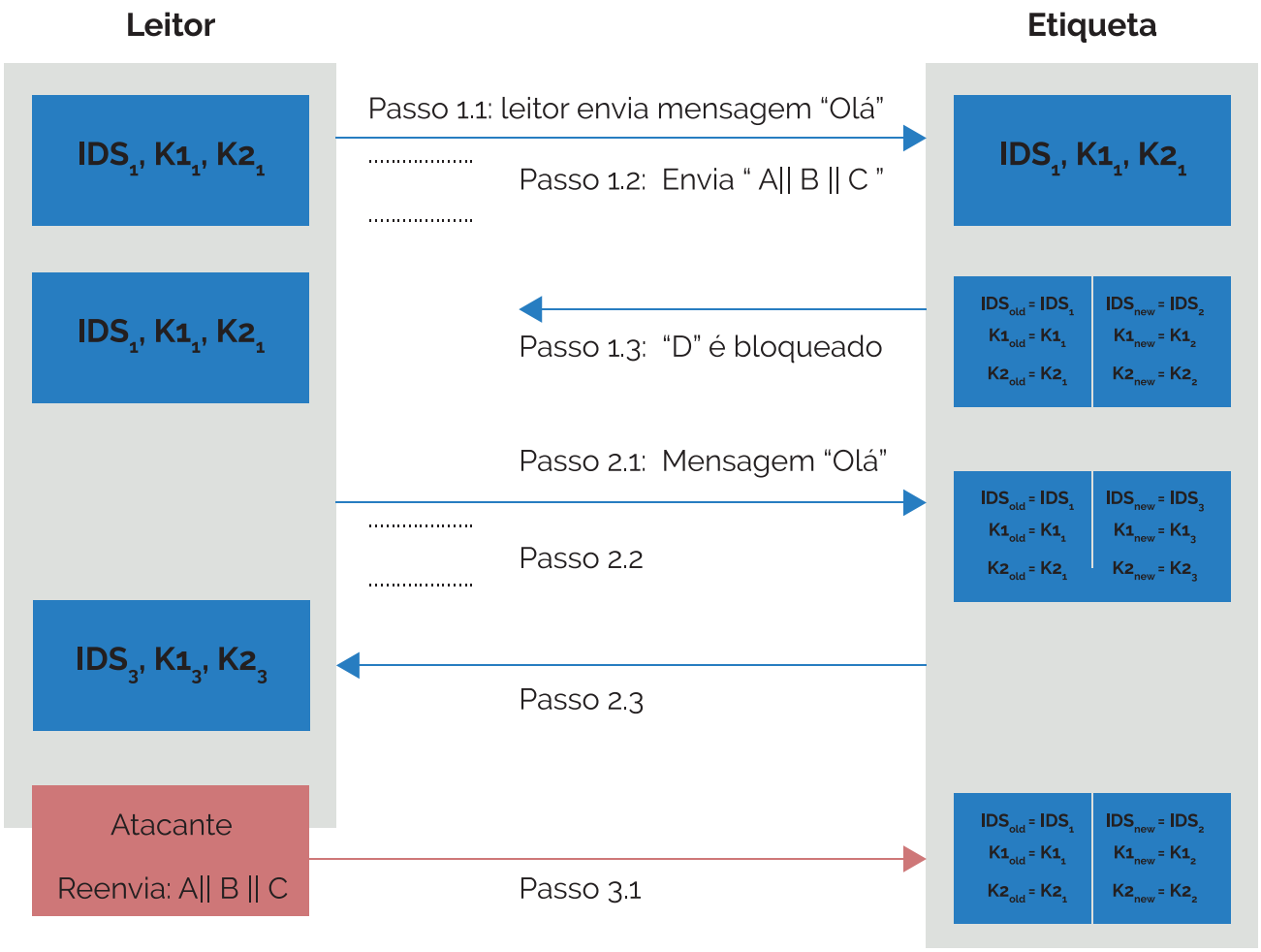
Figura 39. Protótipos de tag RFID.

Fonte: Feldhofer, Aigner e Baier (2010).

O trabalho realizado por Tagra, Rahman e Sampalli (2010) efetua um estudo para demonstrar o ataque de negação de serviço por dessincronização em sistemas RFID.
Esse ataque explora uma vulnerabilidade existente no protocolo de autenticação Gossamer, que faz parte de uma família de protocolos denominada Protocolos Ultra Leves de Autenticação Mútua (UMAP, do inglês *Ultra Light Mutual Authentication Protocols*).
Os protocolos dessa família utilizam operações lógicas binárias, como XOR, OR e AND, e operações aritméticas, como a adição, para implementar autenticação segura.
O processo de autenticação do protocolo Gossamer é realizado em três estágios: Identificação da Tag, Autenticação Mútua e Atualização de Chaves. Cada tag possui um identificador estático, um pseudoíndice e duas chaves de autenticação. No estágio Identificação da Tag, a tag responde à interrogação realizada pelo leitor com o possível pseudoíndice. Se o valor coincidir, o processo passa para o próximo estágio. No estágio Autenticação Mútua, utilizando as chaves enviadas pela tag, o leitor gera um código temporário e o envia para a tag, que decifra o código. A tag atualiza então suas chaves, gera um novo código temporário e envia para o leitor. Se a comparação do novo código recebido com um código gerado localmente for positiva, ocorrerá a autenticação. No estágio Atualização de Chaves, leitor e tag gravam as chaves utilizadas com sucesso durante a última comunicação Tagra, Rahman e Sampalli (2010).

Na **Figura 40** estão demonstrados os passos para gerar um ataque de negação de serviço no sistema RFID que utiliza o protocolo de autenticação Gossamer. No passo 1.1, o leitor envia a mensagem “Olá” para a tag. A tag responde com IDS1, K11 e K21. No passo 1.2, o leitor confirma as informações recebidas e envia as informações “A || B || C”.

Figura 40. Ataque ao protocolo Gossamer.



Fonte: Tagra, Rahman e Sampalli (2010, tradução nossa)

No passo 1.3, a tag confirma o recebimento das informações, atualiza suas chaves para IDS2, K12 e K22 e as envia com "D" para o leitor. A mensagem "D" é interceptada pelo atacante e não permite que o leitor receba essa informação.

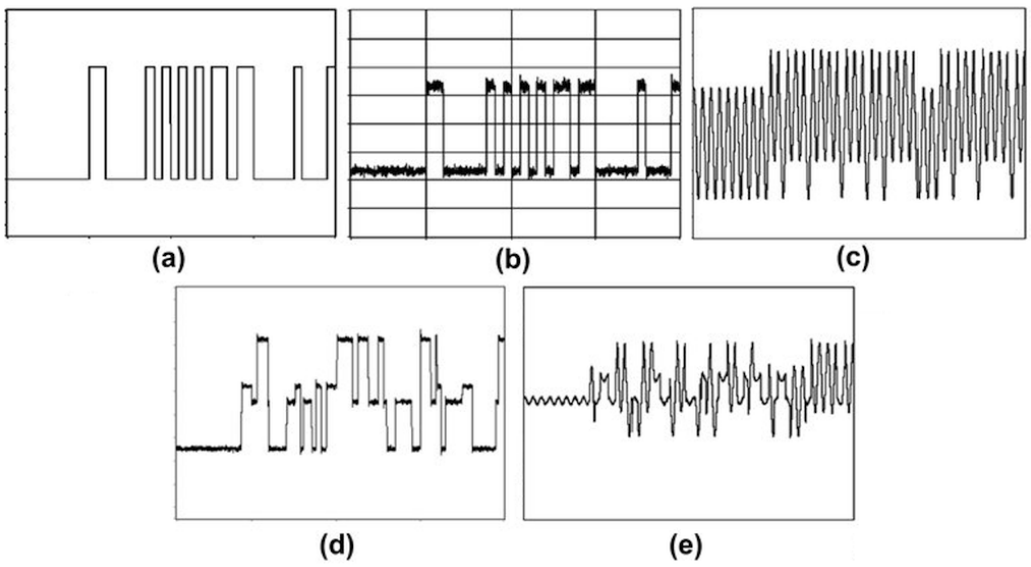
Como a informação final não chegou ao leitor, as chaves foram atualizadas somente na tag. No passo 2.1, o leitor envia novamente a mensagem "Olá". A tag responde com IDS2, K12 e K22, porém o leitor rejeita e força a tag a usar a chave antiga, ou seja, IDS1, K11 e K21. A comunicação ocorre sem problemas nos passos 2.3 e 2.4. Ao final as chaves IDS3, K13 e K23 são atualizadas no leitor e na tag. No passo 3.1, o leitor atacante reenvia as mensagens capturadas nos passos 1.1 e 1.2, fazendo com que a tag atualize novamente suas chaves. A partir desse momento, as chaves atuais e antigas não coincidirão entre leitor legítimo e tag, resultando na interrupção da comunicação.

A proposta de Tagra, Rahman e Sampalli (2010) para evitar o ataque previamente descrito envolve armazenar as chaves antigas e novas no leitor em um banco de dados, da mesma forma como já é efetuado pela tag. Quando a comunicação for interceptada e repetida pelo atacante a tag atualizará sua chave. No entanto, a chave antiga ainda estará armazenada. O leitor legítimo, ao tentar utilizar a chave nova sem obter sucesso, utilizará a chave antiga, que a tag também possui, e a comunicação ocorrerá satisfatoriamente.

Fu, Zhang e Wang (2010) efetuaram um estudo sobre ataques de negação de serviço em sistema RFID. O estudo explorou a geração da interferência eletromagnética como forma de ataque do tipo jamming ativo e analisou seus efeitos em sistemas RFID.

O estudo foi dividido em três etapas. Na primeira etapa foi realizada uma análise matemática sobre o efeito da interferência eletromagnética maliciosa durante a comunicação. Na segunda etapa, foi realizada uma simulação computacional. Na terceira e última etapa, foi efetuado um experimento prático para demonstrar o efeito do ataque jamming.

A **Figura 41** apresenta o resultado da simulação computacional. O gráfico **(a)** indica o sinal de dados enviado. O gráfico **(b)** indica a demodulação do sinal enviado adicionado de um sinal interferente em mesma frequência de operação. O gráfico **(c)** indica a demodulação do sinal enviado adicionado de um sinal interferente com frequência de operação ligeiramente diferente. O gráfico **(d)** indica a demodulação do sinal enviado adicionado de um sinal interferente em mesma frequência de operação com dados modulados. O gráfico **(e)** indica a demodulação do sinal enviado adicionado de um sinal interferente com frequência de operação ligeiramente diferente e com dados modulados. No gráfico **(b)**, o sinal recebido foi distorcido, no entanto, é possível identificar traços do sinal original. Nos gráficos **(c)** e **(e)**, o sinal recebido foi totalmente distorcido, não sendo possível recuperar os dados enviados.

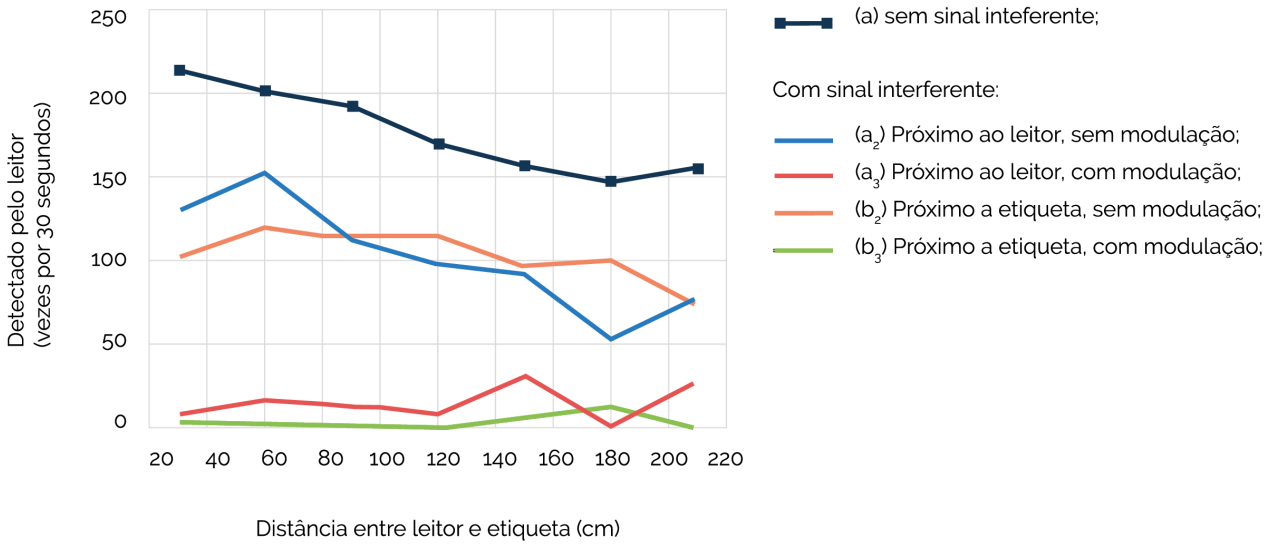


Fonte: Fu, Zhang e Wang (2010).

No primeiro experimento, a distância entre leitor e tag foi alterada gradativamente, e a potência do sinal interferente mantida inalterada. No segundo experimento, a distância entre leitor e tag foi mantida inalterada, sendo que a potência do sinal interferente foi elevada gradativamente. Para ambos os testes, o período de coleta utilizado foi de 30 segundos.

A **Figura 42** apresenta a quantidade de vezes que a tag foi detectada enquanto a distância entre leitor e tag é alterada. A linha **(a)** indica a quantidade de leitura sem sinal interferente. As linhas **(a_n)** referem-se ao sinal interferente próximo ao leitor. As linhas **(b_n)** referem-se ao sinal interferente próximo à tag. Nas linhas **a_2** e **b_2**, o sinal interferente não possui dados modulados e a interferência ocasiona uma queda na quantidade de leituras sem interromper o funcionamento. Nas linhas **a_3** e **b_3**, o sinal interferente possui dados modulados, sendo que a interferência praticamente interrompe o funcionamento.

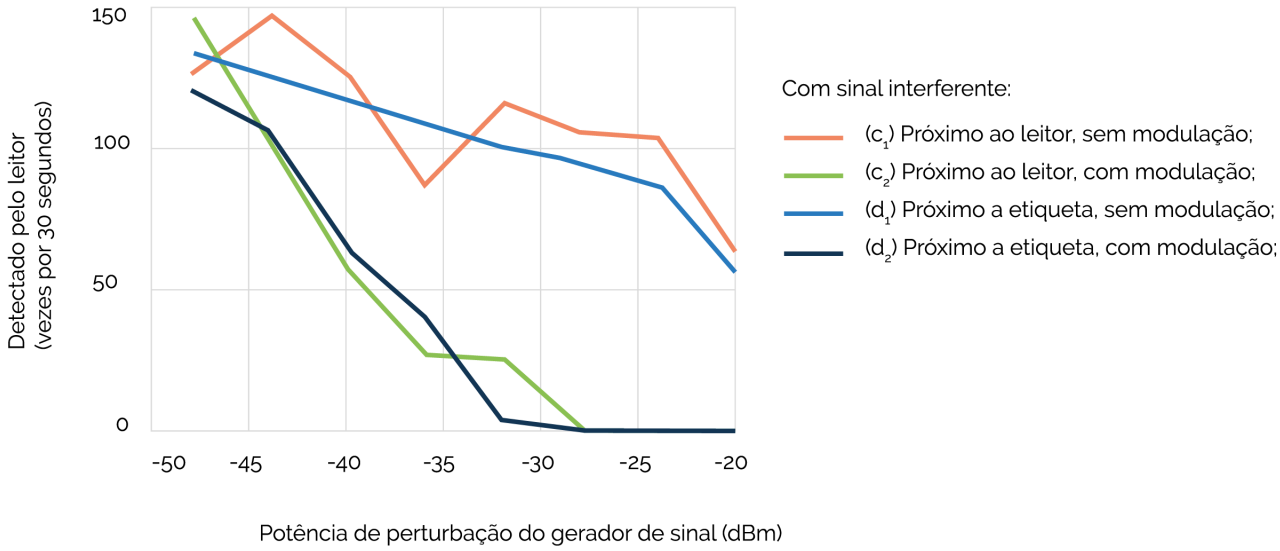
Figura 42. Ataque *jamming* variando a distância.



Fonte: Fu, Zhang e Wang (2010, tradução nossa).

A **Figura 43** apresenta a quantidade de vezes que a tag foi detectada enquanto a potência do sinal interferente é alterada. As linhas **(c_n)** referem-se ao sinal interferente próximo ao leitor. As linhas **(d_n)** referem-se ao sinal interferente próximo à tag. Nas linhas **(c_1)** e **(d_1)** o sinal interferente não possui dados modulados, e a interferência ocasiona uma pequena queda na quantidade de leituras à medida que a potência do sinal interferente aumenta. Nas linhas **(c_2)** e **(d_2)** o sinal interferente possui dados modulados, sendo que a interferência ocasiona uma acentuada queda na quantidade de leituras efetuadas.

Figura 43. Ataque *jamming* variando a potência.



Fonte: Fu, Zhang e Wang (2010, tradução nossa).

Fu, Zhang e Wang (2010) mostraram o funcionamento teórico do ataque de negação de serviço do tipo jamming.
Gao, Shu e Liu (2011) realizaram um trabalho abordando o ataque de dessincronização. O trabalho propôs um novo protocolo que introduz uma variável de ruído eteve como foco a característica de tempo intermitente de seção. Os resultados apresentados no artigo evidenciam a eficácia deste protocolo para evitar ataques de dessincronização.

O trabalho realizado por Yang, Guo e Deng (2011) apresenta um sistema colaborativo de detecção de intrusão em RFID baseado em sistema imunológico artificial. Este sistema analisa registros de logs gerados pelos sistemas RFID e utiliza o conceito de um sistema imunológico biológico para determinar se houve um ataque. Os ataques detectados pelo sistema são: adivinhação de senha, tentativas de leitura não autorizada e negação de serviço.

Os eventos gerados originalmente pelo leitor RFID não são suficientes para que o sistema identifique os ataques. Assim, por meio de um analisador de sinal por radiofrequência, é gerado um registro da comunicação denominado log de canal. O sistema trata os eventos de ataque de forma colaborativa, ou seja, para a identificação positiva de um ataque é necessário que ao menos dois eventos relacionados confirmem a existência do ataque. Além disso, trabalha com os eventos como antígenos, sempre comparando com padrões preexistentes para identificar possíveis ameaças.

O processo de colaboração, para o qual foi utilizado o algoritmo “aiNet”, é otimizado ao agrupar os eventos gerados. Este algoritmo simula o processo evolutivo dos sistemas imunológicos. Ocorre então a estimulação dos antígenos que geram redes de memória, posteriormente usadas para correlacionar os eventos.

A Tabela 3 apresenta os resultados da simulação de detecção de intrusão em laboratório utilizando o processo colaborativo.

Tabela 3. Resultado estatístico da detecção colaborativa.

	TAXA DE DETECÇÃO MÉDIA (%)	TAXA DE FALSA DETECÇÃO MÉDIA (%)	TAXA DE PERDA DE DETECÇÃO MÉDIA (%)
SISTEMA EM GERAL	99,39	1,50	0,61
ROUBO DE DADOS DE TAG	100,00	0,00	0,00
TESTES DE SENHA	100,00	0,00	0,00
NEGAÇÃO DE SERVIÇO	98,00	1,00	2,00
ATAQUE DESCONHECIDO	93,33	0,50	6,67

Fonte: Yang, Guo e Deng (2011, tradução nossa).

Yang, Guo e Deng (2011) apresentaram um sistema de detecção de intrusão para diversos ataques em RFID.

Oren, Schirman e Wool (2012) efetuaram um estudo sobre os ataques zapping e jamming e seus efeitos em sistemas RFID. O ataque zapping consiste em enviar um rápido pulso de alta potência para o cartão. Esse pulso sobrecarrega o circuito eletrônico do cartão, desabilitando-o permanentemente. Esse ataque é bastante eficiente em tags e cartões passivos, já que sua única fonte de energia é proveniente da onda eletromagnética enviada pelo leitor..

No primeiro teste experimental, o ataque zapping foi efetuado com uma simples câmera fotográfica. A lâmpada do flash da câmera foi substituída por uma antena caseira de circuito impresso. Ao acionar o disparador, um pulso de alta energia é enviado ao

cartão, que é desativado permanentemente. Para aumentar o alcance deste dispositivo, basta substituir os capacitores originais por componentes de maior capacidade.
O ataque jamming pode ser executado ao enviar um sinal de alta potência na frequência da portadora ou em suas subportadoras. Este sinal gera uma perturbação na comunicação entre leitor e cartão, o que pode afetar o desempenho do sistema de leitura e até interromper a comunicação.

No segundo teste experimental foram utilizados uma fonte de energia, um gerador de sinais, um amplificador e dois tipos de antenas, ambas utilizadas em aplicações militares.

A Tabela 4 apresenta o resultado do ataque com as antenas selecionadas. Para cada detecção do cartão o sistema emite um sinal sonoro. O jamming parcial foi considerado quando o sistema emitia no máximo dois sinais sonoros a cada 10 segundos.

Tabela 4. Distância do ataque *jamming* com antenas diferentes.

ANTENA	ALCANCE DO JAMMING TOTAL (M)	ALCANCE DO JAMMING PARCIAL (M)
HUSTLER	1,1	1,65
HELICOIDAL	2	2,3

Fonte: Oren, Schirman e Wool (2012, tradução nossa).

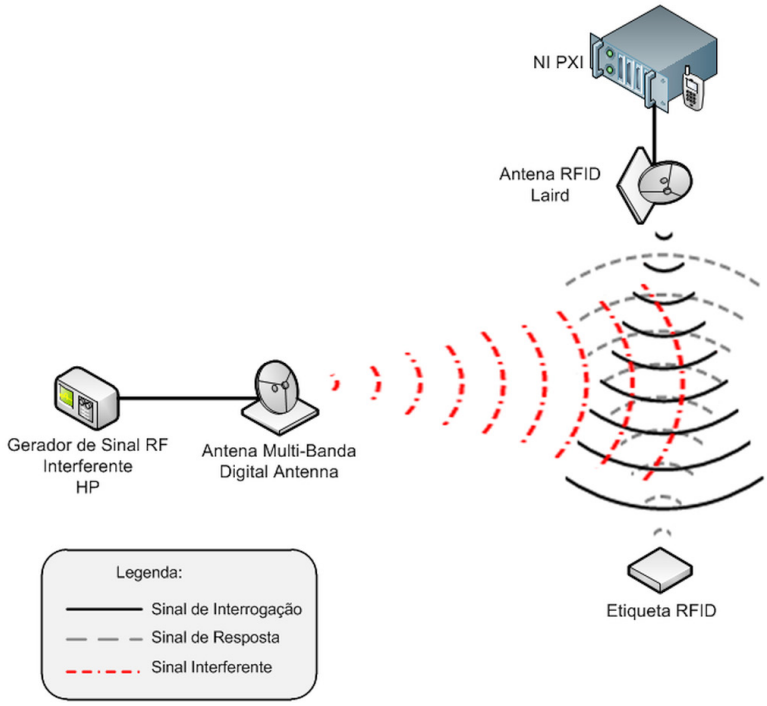
Oren, Schirman e Wool (2012) mostraram como gerar ataque de negação de serviço do tipo zapping e jamming em sistema RFID sem contato utilizando diferentes tipos de antenas.

O trabalho realizado por Avanço et al. (2015) desenvolve um sistema de detecção de intrusão (IDS) para identificar a ocorrência do comportamento malicioso e notificar o operador do sistema sobre um tipo específico de interferência eletromagnética em Sistemas RFID, ou seja, o ataque jamming.

O sistema foi testado em um ambiente laboratorial utilizando os equipamentos a seguir. A **Figura 44** mostra o esquema de montagem utilizado:

- National Instruments PXIe 1065;
- Tag Impinj E44 RFID;
- Tag Confidex Pino RFID;
- Antena RFID Laird S9028PC
- Gerador de Sinal HP ESG-D4000A;
- Antena Digital Antenna 489-DB com polarização linear e 10 dBi de ganho.

Figura 44. Configuração do ambiente de validação.

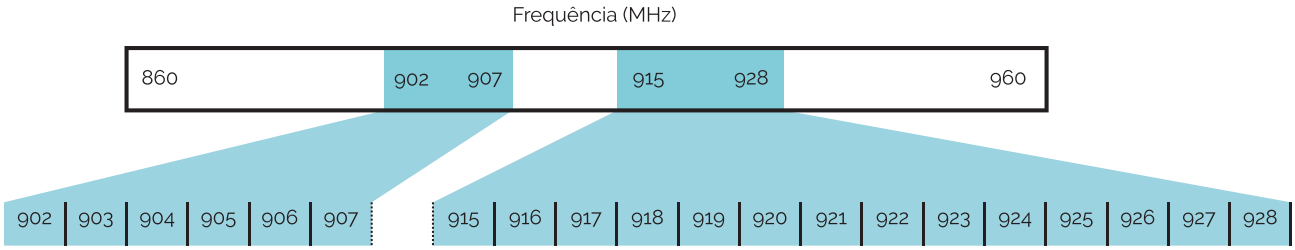


Fonte: Avanço et al. (2015).

Os testes foram realizados na faixa de frequência permitida para operação de RFID no Brasil, conforme ilustrado na **Figura 45**.

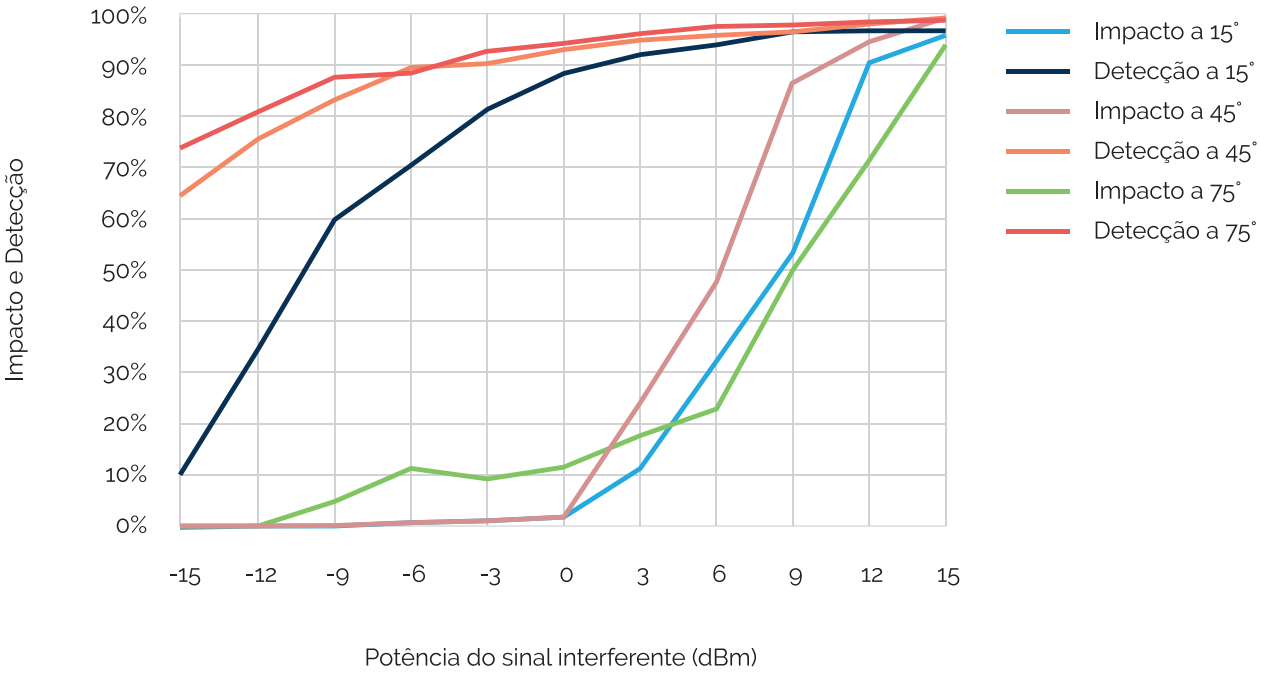
A **Figura 46** mostra os resultados do ensaio realizado comparando impacto do ataque e a detecção do sistema quando o sinal de interferência varia a potência no canal de operação.

Figura 45. Faixas de frequências para RFID no Brasil.



Fonte: Avanço et al. (2015).

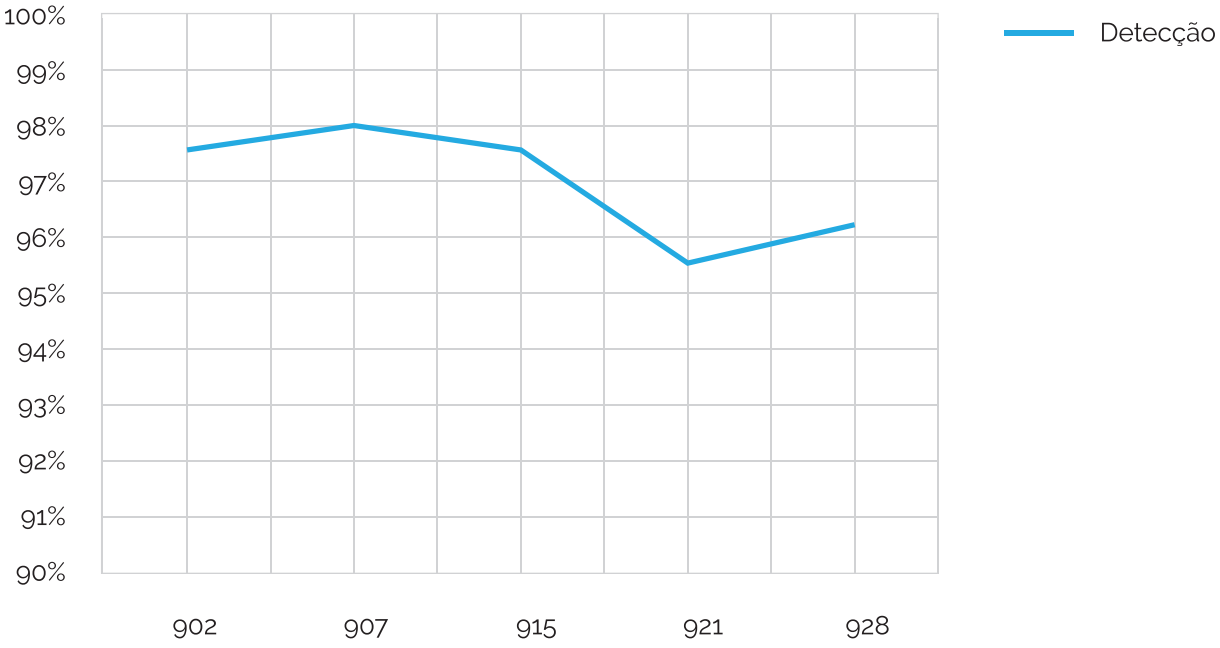
Figura 46 – Impacto e detecção versus potência.



Fonte: Avanço et al. (2015).

A **Figura 47** mostra os resultados da detecção com sinal de interferência variando a frequência do canal de funcionamento para algumas das frequências mostradas na **Figura 45**.

Figura 47. Detecção variando a frequência.

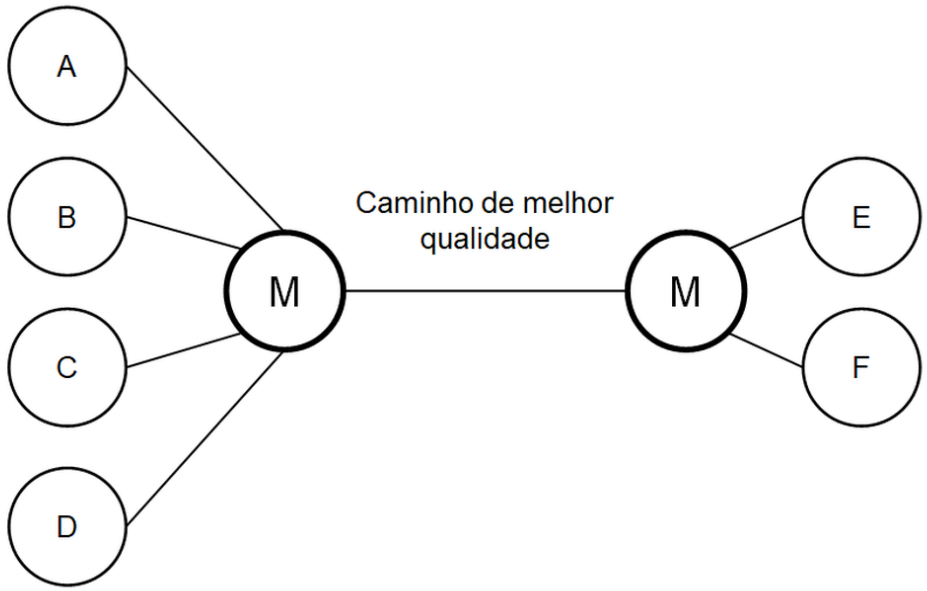


Fonte: Avanço et al. (2015).

Os resultados obtidos no trabalho de Avanco et al. (2015) mostraram que os ataques de interferência são detectados antes de ter um impacto significativo na comunicação entre o leitor de RFID e a tag, isto é, o ataque de interferência foi detectado mesmo com poder insuficiente para impactar na comunicação.

O trabalho proposto por Goyal (2015) realiza um revisão do ataque denominado Sybil em RSSF. Neste ataque um nó comprometido propaga múltiplos endereços, como se estivesse em locais distintos, prejudicando os mecanismos de tolerância a falhas existentes na rede. A **Figura 48** ilustra esse tipo de ataque, em que o nó M divulga dois endereços diferentes, fazendo com que os nós vizinhos se conectem como se fossem dois nós diferentes, e gerando um ponto único de falha.

Figura 48. Esquema de um ataque Sybil.



Fonte: Goyal (2015, tradução nossa).

Como contramedidas levantadas por Goyal (2015), destacam-se as seguintes estratégias:

- **Certificação confiável:** utilizar uma Autoridade Certificadora para garantir a unicidade de cada nó da rede, não permitindo a um mesmo nó realizar sua divulgação como sendo múltiplos nós;
- **Teste de recursos:** utilizar um esquema que calcula, armazena e compara níveis de energia, capacidade de armazenamento, entre outros parâmetros, a cada comunicação, assim um novo nó malicioso não conseguirá se comunicar se enviar parâmetros sem coerência com o histórico das comunicações anteriores;
- **RSSI:** utilizar um esquema que compara e armazena o histórico de nível de sinal de rádio recebido (RSSI, do inglês Radio Resource Strength Signaling). É considerado o mais robusto, pois em um ambiente real, um nó malicioso não consegue prever as variações no nível de sinal, e ao enviar um sinal constante revela um possível atacante.

O trabalho realizado por Patel e Soni (2015) apresentou uma proposta para defesa contra o ataque em RSSF, denominado ataque vampiro. O ataque vampiro consiste em manter o equipamento em constante operação, drenando a bateria de forma prematura. Pode ser realizado de duas formas: na primeira, o atacante envia um pacote cujo destino envolve sempre passar por um mesmo nó diversas vezes até atingir seu destino.

Na segunda forma, o pacote força um caminho mais longo, obrigando a participação de um maior número de nós na comunicação. Os nós excedentes são ligados por períodos desnecessários e acabam consumindo sua bateria indevidamente.

Para evitar este comportamento do ataque, Patel e Soni (2015) propuseram a adição de comandos adicionais ao protocolo de roteamento AODV (Ad-hoc on Demand Distance Vector Routing), que indicam quando uma rota falhar, evitando que os nós consumam energia tentando enviar um dado que não atingirá o nó de destino. Os comandos adicionais notificam quando a rota for corrigida, assim os nós envolvidos podem enviar os dados coletados pelos sensores conectados a uma RSSF.

Kaushal e Sahni (2016) propuseram um método de detecção contra ataques de negação de serviço distribuído em RSSF.

O método de detecção ocorre quando cada nó realiza a comparação da taxa de entrega de pacotes de cada nó em sua vizinhança. Quando um nó vizinho possui uma taxa relativamente alta, comparada aos demais nós, este nó poderá realizar um ataque. Assim, a comunicação deste nó será isolada até que sua taxa de entrega de pacotes seja reduzida para valores considerados aceitáveis pela RSSF.

Os resultados do trabalho de Kaushal e Sahni (2016) mostraram valores significativos para ataques distribuídos com um número crescente de atacantes. Em situações de ataque as taxas de entrega de pacotes e energia remanescente nos nós não se alteraram, indicando a eficácia do método proposto.

Já o trabalho realizado por Jangra e Choudhary (2017) apresenta um modelo para detecção do ataque buraco negro em RSSF.

O ataque buraco negro é caracterizado por um nó atacante da RSSF que anuncia a si próprio como uma rota de menor distância, fazendo com que nós vizinhos o utilizem como melhor rota. Quando o nó atacante recebe o tráfego passante, enviado pelos nós vizinhos, este tráfego é descartado, não atingindo o destino.

O modelo proposto realiza o envio de pacotes de teste para os nós da rede. O nó com comportamento de buraco negro será identificado, e sua identificação é compartilhada com os nós da rede, assim, todos os nós evitaram utilizar o nó comprometido como rota disponível para comunicação. As simulações realizadas mostraram a eficácia do método proposto.

4.1.2 CONFIDENCIALIDADE

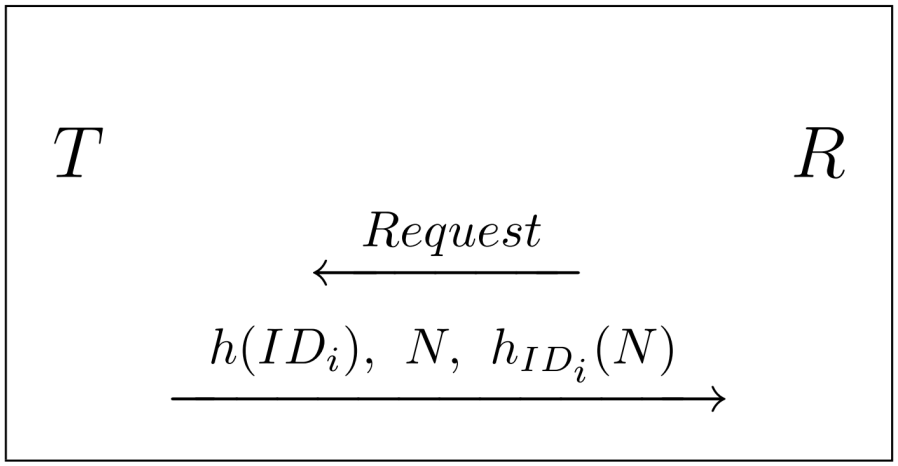
Em Segurança da Informação, o pilar Confidencialidade tem como objetivo garantir que a informação esteja disponível somente a entidades autorizadas, não permitindo acessos não autorizados.

Um dos principais problemas de segurança, relacionados aos sistemas RFID, é a violação da privacidade do usuário. Isso pode acontecer quando a tag expõe seu conteúdo ou transmite identificadores universais, infringindo as questões de confidencialidade durante o processo de comunicação.

Dimitriou (2005) realizou um estudo que propôs um protocolo de autenticação RFID que garante a confidencialidade das informações do usuário contidas nas tags RFID.
O protocolo foi projetado para garantir autenticação em ambos os sentidos, ou seja, da tag para o leitor e do leitor para a tag. Sem a utilização de autenticação em ambos os sentidos qualquer protocolo de autenticação está propenso a ataques de clonagem que, se bem sucedidos, podem comprometer a confidencialidade das informações.
O funcionamento do protocolo baseia-se no compartilhamento de uma chave entre a tag e um banco de dados que é mantido atualizado para evitar rastreamento da tag. Este processo de atualização é realizado de tal forma que a eficiência de identificação da tag não é sacrificada, ou seja, o processo de leitura não sofre influência por conta da atualização.

A **Figura 49** mostra um processo de leitura usual, em que o Leitor (R) realiza uma requisição para a tag (T). A tag responde com o identificador da comunicação (N), com o hash sobre o ID gerado pelo leitor na requisição (h(ID)) e com o hash sobre o identificador da comunicação (hID(N)). Nesse processo, um leitor ilegítimo pode realizar a interrogação, sendo que a tag responderá.

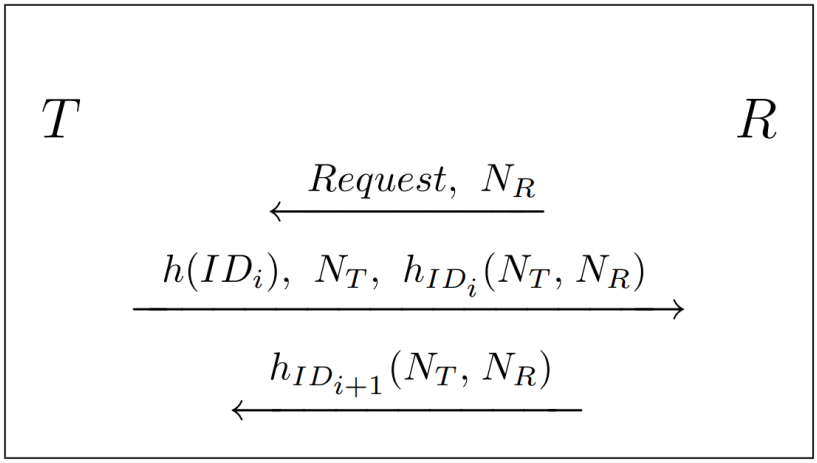
Figura 49. Processo de comunicação entre leitor e tag.



Fonte: Dimitriou (2005).

A **Figura 50** mostra o funcionamento do protocolo proposto por Dimitriou (2005). O Leitor (R) realiza uma requisição para a tag (T) encaminhando um identificador da comunicação do Leitor (NR). A tag responde com o identificador da comunicação gerado pelo Leitor (NT), o hash sobre o ID gerado pelo leitor na requisição (h(ID)) e o hash sobre o identificador da comunicação gerado pela tag e pelo leitor (hID(NR;NT)). Se os dados recebidos estiverem corretos, ao consultar um banco de dados de autenticação o leitor atualizará as informações na tag para a próxima comunicação futura (hIDi+1(NT, NR).

Figura 50. Funcionamento do protocolo proposto.



Fonte: Dimitriou (2005).

Thamilarasu e Sridhar (2008) apresentaram um modelo para detectar a existência de leitor e tag maliciosos que podem gerar um ataque *man-in-the-middle* em sistemas RFID. O modelo proposto é dividido em três módulos: Módulo de Auditoria, Módulo de Detecção e Módulo de Ação.

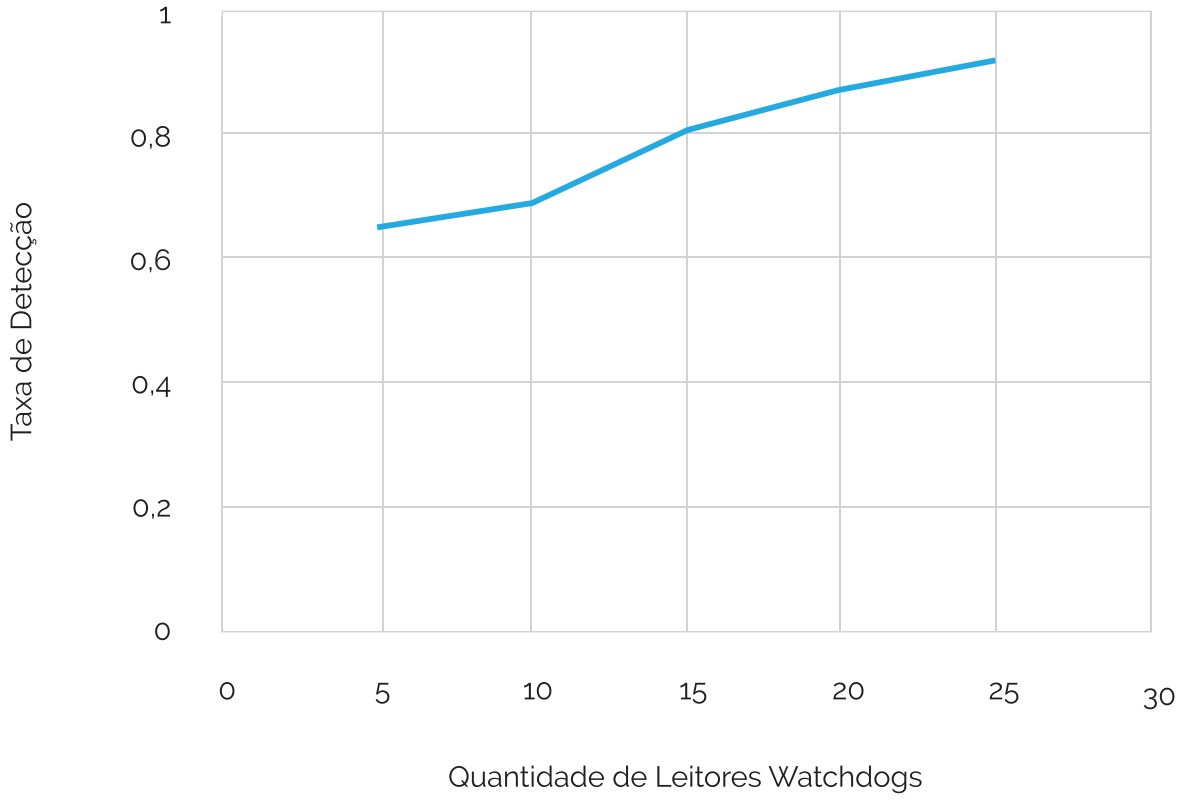
O Módulo de Auditoria é responsável por monitorar e coletar os dados dos equipamentos RFID envolvidos na comunicação, ou seja, leitor e tag. A monitoração é efetuada por leitores com mecanismos de *watchdog*, que observam de forma passiva o comportamento de outros leitores dentro do seu alcance de leitura. O Módulo de Detecção analisa os registros coletados pelo Módulo de Auditoria, e com base em um modelo estatístico para detecção de intrusão, identifica as anomalias na rede.

O ataque *man-in-the-middle* em RFID pode ocorrer de duas formas. A primeira forma consiste em um leitor atacante interceptar a comunicação entre leitor e tag e se passar pelo leitor legítimo. O leitor atacante recebe as informações da tag, simula uma tag atacante e responde para o leitor legítimo. Ao término desse processo, a comunicação entre leitor e tag legítimos foi comprometida e o acesso ao leitor foi adquirido pelo usuário atacante. A segunda forma consiste em um leitor atacante se comunicar com uma tag legítima, obter acesso de escrita e inserir informações maliciosas no campo de dados da tag.

O primeiro experimento foi executado com um número fixo de 10 leitores watchdogs. A quantidade de ataques foi aumentada gradativamente, com a variação de 50 ataques, até o máximo de 300 ataques. O segundo experimento foi executado variando o número de leitores watchdogs entre cinco e 30.

A **Figura 51** apresenta o resultado do primeiro experimento. Observa-se uma queda na taxa de detecção conforme a quantidade de ataques cresce.

Figura 51. Detecção versus quantidade de ataques.

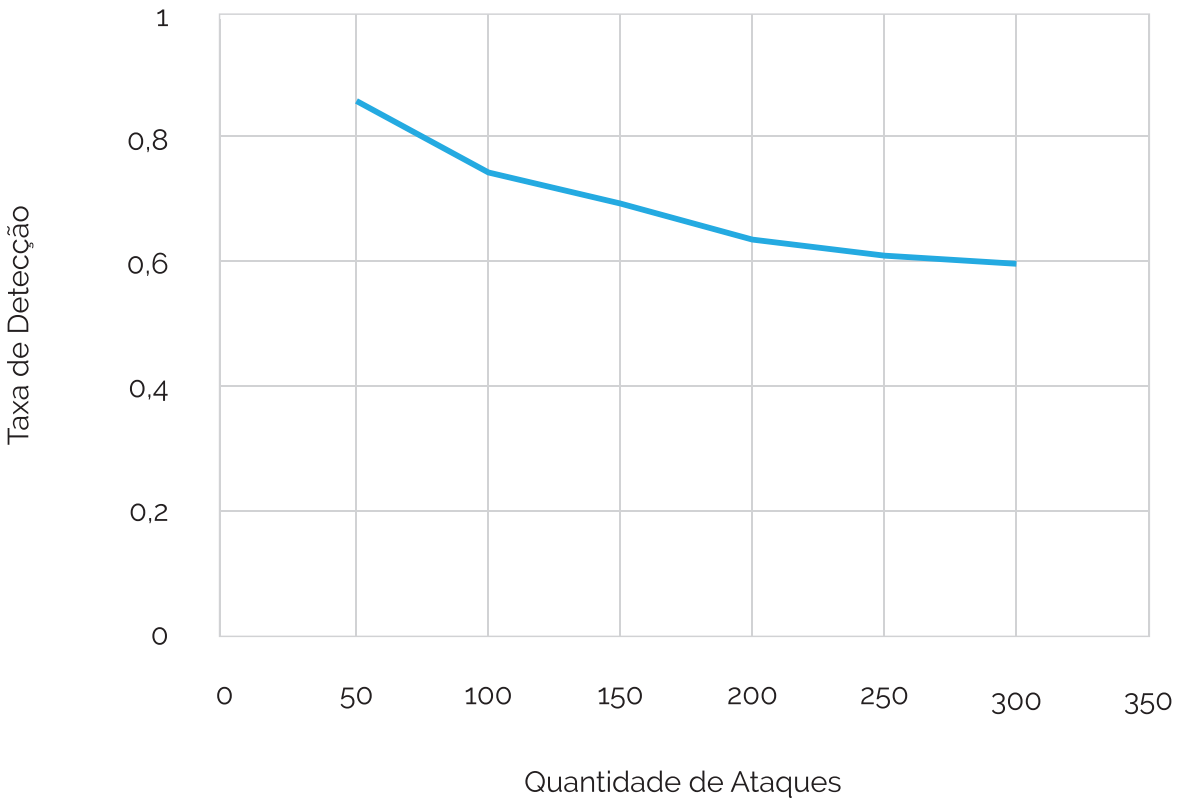


Fonte: Thamilarasu e Sridhar (2008, tradução nossa).

A **Figura 52** apresenta os resultados do segundo experimento. Observa-se uma melhora na taxa de detecção conforme a quantidade de watchdogs aumenta.

Já o trabalho realizado por Feldhofer, Aigner e Baier (2010), além do ataque abordado na seção Disponibilidade, propôs um cenário para utilização dos protótipos de tag RFID em que as tags são utilizadas em ataques do tipo homem no meio. Nesse cenário, a tag customizada opera como um proxy, que intercepta toda a comunicação entre leitor e tag legítima. A tag proxy faz um duplo papel, em que se comporta como um leitor legítimo para a tag e também como uma tag legítima para o leitor utilizado na comunicação.

Figura 52 – Detecção versus quantidade de watchdogs.



Fonte: Thamilarasu e Sridhar (2008, tradução nossa).

Essa operação ocorre de forma silenciosa, e todos os dados podem ser processados sem que leitor e tag legítima tenham conhecimento dela.

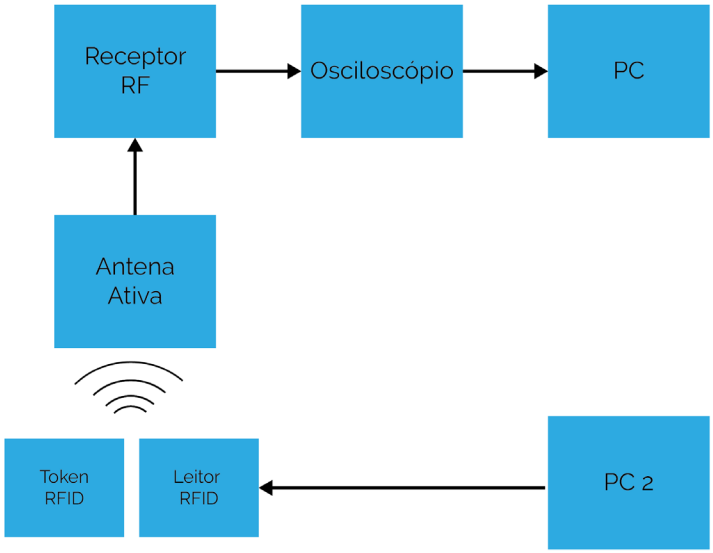
O trabalho de Hancke (2011) abordou os ataques de skimming em que os dados da tag são capturados para uso ilegítimo. O trabalho apresentou resultados da prova de conceito para ataques de espionagem e skimming executados contra dispositivos RFID operando na faixa de 13,56 MHz. Os ataques de espionagem foram executados com sucesso em dispositivos que operam com os protocolos bastante populares: ISO 14443A/b e ISO 15693.

Hancke (2011) mostrou a configuração experimental que fornece a outros pesquisadores um ataque de referência para estudo e melhorias. Os resultados apresentados confirmam que os dispositivos de campo próximo não são rigidamente limitados e que um invasor pode definitivamente recuperar dados além do intervalo de operação anunciado. O estudo também fornece um resultado prático para o debate, que é importante para a tecnologia RFID, em que as distâncias de ataque são tantas vezes vistas como uma medida de segurança. A **Figura 53** mostra a configuração utilizada para o ataque de espionagem.

Figura 53. Configuração para ataque de espionagem.

(a) capturando a comunicação

(b) configuração experimental

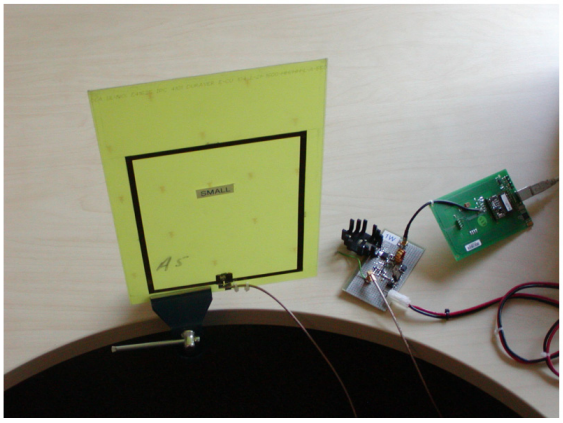


Fonte: Hancke (2011, tradução nossa).

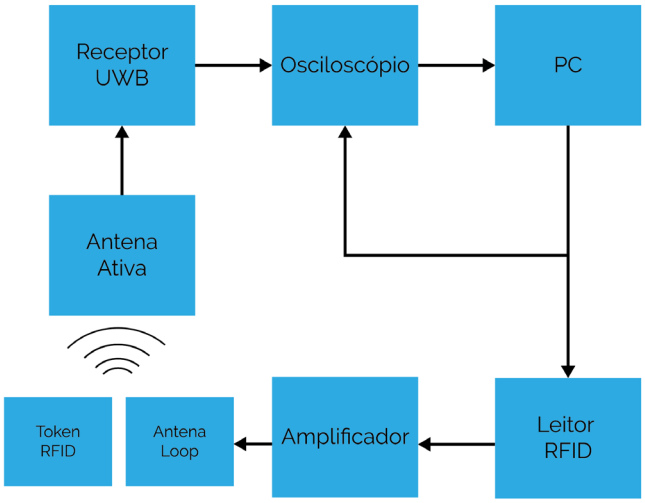
Hancke (2011) também apresentou resultados de ataque de skimming, em que os atacantes usam duas antenas separadas para energizar a tag e recuperar sua resposta, ao contrário da maioria dos ataques de skimming que usam uma única antena.
Os resultados mostraram que mesmo para um receptor de RF que não alcance os mesmos resultados que o equipamento comercial, a escuta não está além dos meios do atacante médio. A **Figura 54** mostra a configuração utilizada para o ataque de skimming.

Figura 54. Equipamentos para ataque de skimming.

(a) Leitor Skimming



(b) configuração experimental



Fonte: Hancke (2011, tradução nossa).

O trabalho de Noman, Rahman e Adams (2011) propõe uma solução de detecção de adulterações para tags RFID de baixo custo do padrão *EPC Class1 Generation 2* com base em uma função criptográfica de PRNG (um pseudogerador de números aleatórios para tags de RFID de baixo custos) chamada LAMED e o mapa caótico *Skew Tent*. Adicionalmente, este trabalho também inclui uma solução para a detecção de clonagem.

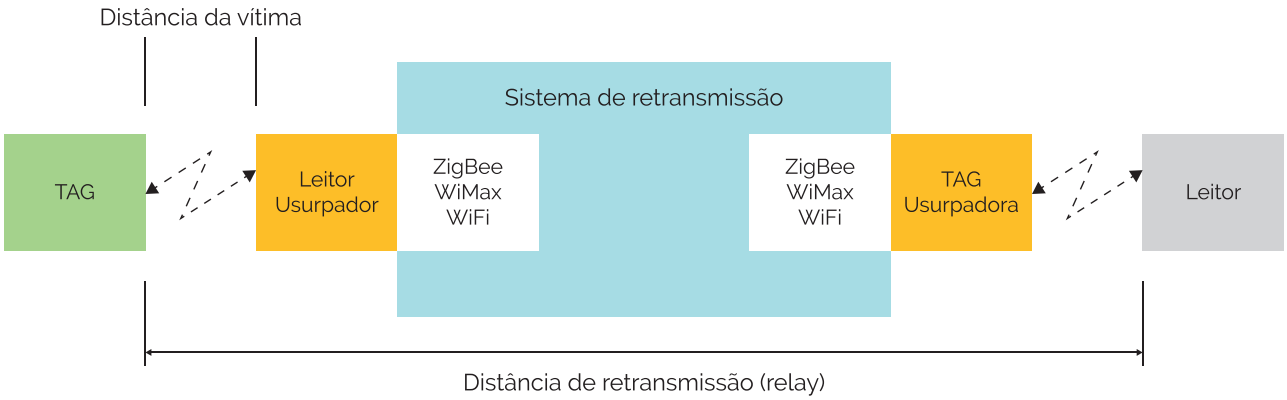
Para detecção de adulteração, é gerado para cada tag um código de verificação de 32 bits a partir dos campos EM, OC e SN de uma tag EPC. Este código é gerado usando uma função PRNG criptográfica chamada LAMED, que é especificamente proposta para a tag EPC-C1G2, sendo que a senha de acesso de 32 bits é usada como a chave para essa função. Como resultado, cada leitor pode ler a partir da memória do usuário, mas não pode

modificá-la sem saber a senha de acesso. Isso significa que mesmo que um leitor malicioso possa facilmente modificar as informações de tag EPC, como EM, OC e SN, não será possível alterar o código de verificação, por não possuir a senha de escrita na memória.

O trabalho de Lima, Miri e Nevins (2012) discutiu aspectos pertinentes à análise do ataque relay, sendo a principal a máxima distância (dmax) entre o usurpador (falso Leitor) e a vítima. A **Figura 55** apresenta um cenário típico para ataque desta natureza.
O trabalho apresenta uma análise e metodologia de cálculo da distância da vítima (dmax). O aumento da distância pode ser obtido pelo uso de algoritmos que reduzem interferência local gerada pela portadora pura que é transmitida pelo falso leitor.

Assim, Lima, Miri e Nevins (2012) proveem uma solução com forma fechada para estimar a distância da vítima (dmax). Também apresentam opções de aumento da distância da vítima pelo uso de canceladores de interferência. As soluções propostas são implementadas em hardware e são compatíveis com os sistemas comerciais existentes no mercado.

Figura 55. Cenário para ataque relay.



Fonte: Lima, Miri e Nevins (2012).

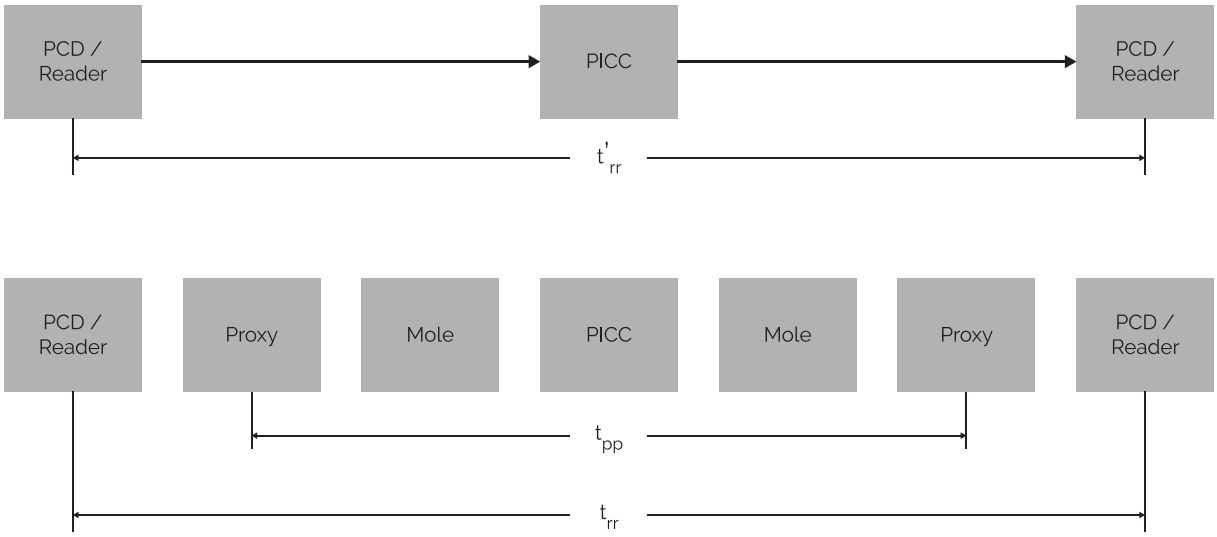
O trabalho realizado por Gong, Nikova e Law (2012) propôs uma nova família de protocolo de criptografia baseada em ciframento de blocos chamado KLEIN. Esse trabalho teve como objetivo fornecer uma cifra prática e segura para aplicações com recursos computacionais escassos, especialmente para RFIDs e redes de sensores sem fio.

Embora KLEIN esteja centrado principalmente em implementações em software, também apresenta eficiência de hardware. O protocolo de criptografia KLEIN utiliza diversos comprimentos de chave oferecendo uma flexibilidade e um nível de segurança moderado para aplicações ubíquas. O resultado apresentado no trabalho mostrou a eficiência do protocolo contra ataques lineares e diferenciais, escalonamento de chaves, ataques integrais e algébricos, assim como ataques de canal adjacente.

Os telefones que implementam NFC não permitem a manipulação de parâmetros como o da comunicação, a saber: UID não pode ser pré-definido como um valor fixo; não é possível alterar parâmetros de protocolo ISO/IEC de baixo nível; e não é permitido modificar comandos de protocolo RFID de baixo nível. Ainda assim, o trabalho realizado por Korak e Hutter (2014) mostrou como realizar um ataque man-in-the-middle em sistemas NFC utilizando telefones com interfaces NFC.

Além disso, Korak e Hutter (2014) mostraram como implementar uma estrutura de proxy utilizando dispositivos NFC customizáveis, que permite um ataque man-in-the-middle mais sofisticado. A **Figura 56** ilustra um processo de comunicação NFC tradicional e um processo utilizando proxy para realizar o ataque man-in-the-middle.

Figura 56. Processo de comunicação NFC utilizando proxy.



Fonte: Korak e Hutter (2014).

O ambiente de ataque proposto por Korak e Hutter (2014) atingiu a distância de 110 metros entre leitor e tag NFC, garantindo que os tempos de atraso não interrompam a comunicação. O resultado mostra a efetividade dos ataques realizados com dispositivos NFC customizáveis.

4.1.4 IRRETRATABILIDADE

Em Segurança da Informação o pilar Irretratabilidade tem como objetivo garantir que a informação foi gerada por fonte autêntica e não permitir repúdio quanto à origem e autoria.

Geta (2011) apresentou um mecanismo de detecção de ataque que identifica a existência de tags clonadas em um sistema de controle de acesso baseado em RFID.
O mecanismo utiliza um algoritmo de aprendizado baseado em uma máquina híbrida com lógicas genética e fuzzy. O algoritmo analisa os eventos gerados pelo sistema RFID e cria um modelo de detecção de ataque.

O algoritmo de aprendizado, baseado em uma máquina híbrida com lógicas genética e fuzzy, combina os algoritmos Pitsburg e Michigan para desenvolver um sistema de classificação que utiliza as bases de regras fuzzy. Pitsburg e Michigan são algoritmos de aprendizado genéticos. O primeiro é utilizado para gerar novas regras fuzzy. Já o segundo realiza a seleção das melhores regras dentre todas as regras criadas. Essa associação se beneficia das melhores características de ambos os algoritmos.

Os índices de desempenho foram definidos como: acurácia, quando a regra identifica o evento anômalo sem erros; sensibilidade, quando a regra consegue identificar a ocorrência de um evento anômalo; e especificidade, quando a regra identifica o evento anômalo dentre outros eventos anômalos.

Para validação do mecanismo foi utilizado o método de validação cruzada do tipo kfold. Uma parcela da massa de dados foi dividida em dez partes, tendo sido uma parte utilizada como teste e as nove restantes como aprendizado. O ciclo foi repetido até que todas as partes fossem utilizadas como teste e aprendizado. Nesta etapa, o algoritmo obteve assertividade acima de 99%.

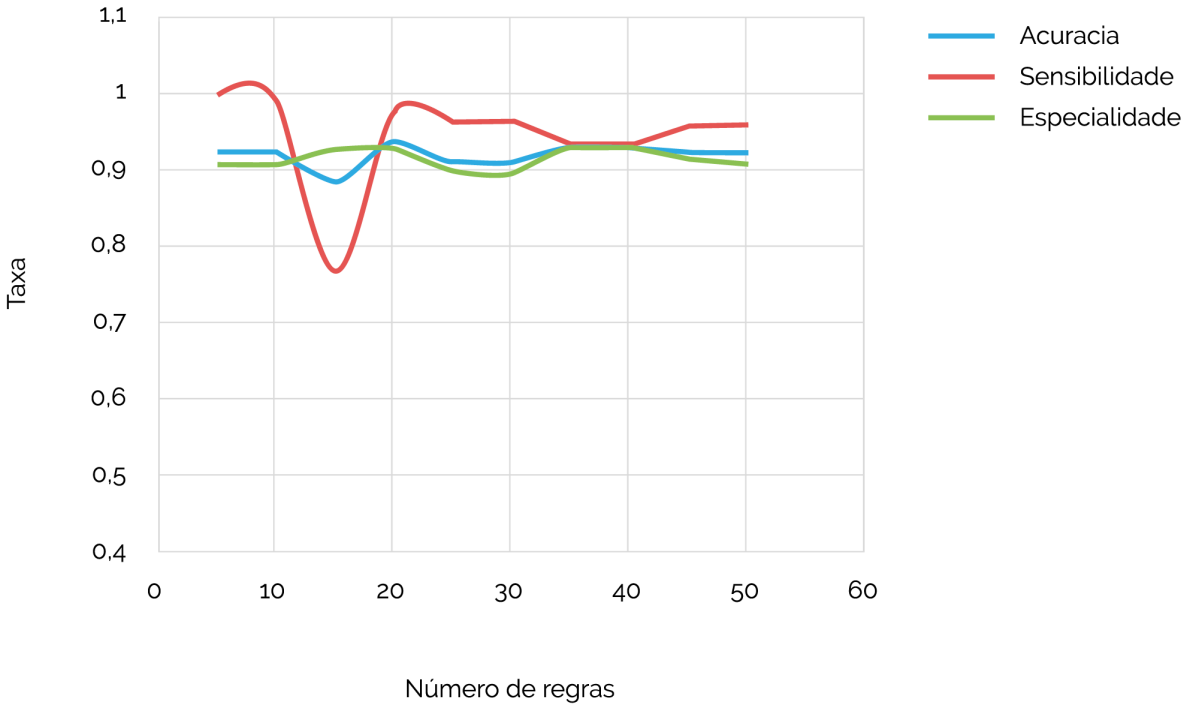
A Figura 57 apresenta o resultado dos testes variando o número de regras fuzzy. O modelo apresentou um melhor aproveitamento dos recursos em torno de 20 regras. Conforme o número de regras cresce a sensibilidade do sistema diminui. Abaixo de 20 regras, o comportamento do algoritmo não apresentou características estáveis.

O trabalho realizado por Ferreira, Azogu e Liu (2012) tem como foco o ataque de repetição. Uma das características desse tipo de ataque é interromper a comunicação das tags afetando a disponibilidade do sistema. O trabalho pospôs dois métodos para eliminar ou reduzir o impacto deste tipo de ataque, a saber, tempo de atraso e atualização aleatória de identificação. O ambiente proposto envolve um ambiente de coleta automática de pedágio .

A Figura 58 mostra o funcionamento do método de atraso realizando o bloqueio da autorização de pagamento, quando o tempo gerado pela tag legítima é reutilizado pela tag atacante, ocasionando a negação de sua autorização de passagem.

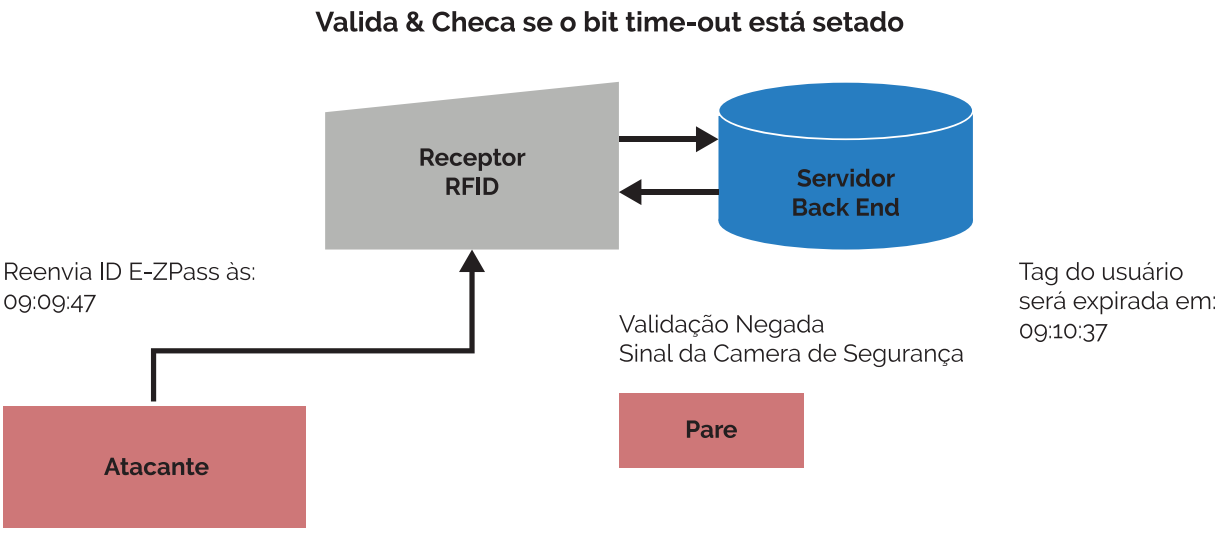
A **Figura 59** apresenta o funcionamento do método de atualização aleatória de identificação realizando o bloqueio da autorização de pagamento, quando um identificador de tag é reaproveitado. O temporizador gerado pela tag legítima é reutilizado pela tag atacante, ocasionando a negação de sua autorização de passagem.

Figura 57 – Acurácia, sensibilidade e especificidade versus número de regras.



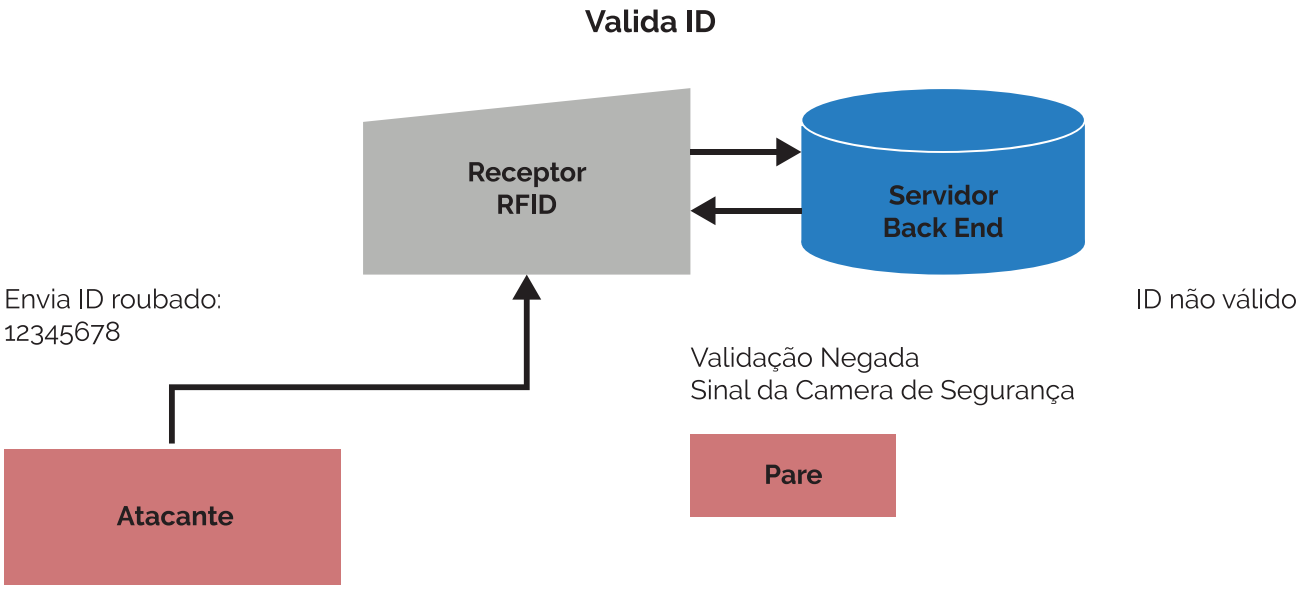
Fonte: Geta (2011, tradução nossa).

Figura 58 – Método de atraso proposto.



Fonte: Ferreira, Azogu e Liu (2012, tradução nossa).

Figura 59. Método de atualização aleatória proposto.



Fonte: Ferreira, Azogu e Liu (2012, tradução nossa).

O trabalho realizado por Ferreira, Azogu e Liu (2012) também abrange o quesito Confidencialidade, pois o ataque de repetição envolve obter informações confidenciais existentes na tag e repeti-las pelo dispositivo fraudador ao se passar pelo dispositivo legítimo.

O trabalho realizado por Kywe, Li e Shi (2013) tem como foco o Serviço Eletrônico de Descoberta de Código de Produto (EPCDS, do inglês Electronic Product Code Discovery Service). EPC Global propôs o EPCDS, que permite às empresas de cadeia de suprimentos encontrarem seus parceiros desconhecidos globalmente.

Nesse trabalho, Kywe, Li e Shi (2013) introduziram o ataque de injeção de eventos realizado por empresas maliciosas presentes na cadeia de suprimentos. Esse ataque não foi considerado anteriormente em sistemas de controle de acesso de EPCDS.

Kywe, Li e Shi (2013) descrevem o processo geral de prevenção e detecção de tais ataques e introduzem o conceito de "prova de propriedade" como um dos métodos de prevenção. Além disso, propõem o método de geração de números pseudoaleatórios do tags EPC, que garante a prova de titularidade da marca EPC e autenticação do evento EPC.

O trabalho realizado por Ling et al. (2017) apresenta um esquema de autenticação para RSSF. A maneira mais simples para autenticação envolve a utilização de senhas,

que são vulneráveis a diversos ataques. O esquema proposto utiliza para autenticação o ID do usuário, uma chave predefinida e o timestamp do momento da comunicação. A cada comunicação o usuário enviará estes parâmetros e receberá do gateway um número randômico, que será usado para calcular a senha. Desta forma a cada sessão o usuário utilizará uma nova senha para contato Ling et al. (2017).

Esse trabalho apresentou a discussão do comportamento do modelo proposto para diversos ataques de autenticação em RSSF.

Rao, Silky e Rana (2013) apresentaram uma proposta para ampliar a segurança de transações bancárias on-line utilizando um fator adicional de autenticação. A proposta inclui utilizar técnicas de RTLS para indicar onde o usuário está no momento da transação, adicionando assim um quarto fator ao processo, que consiste em senhas, smartcard e biometria.

4.1.5 PRIVACIDADE

Em Segurança da informação, o pilar Privacidade tem como objetivo garantir que o dono ou gerador da informação tenha sua identidade preservada.

O protocolo de autenticação proposto por Dimitriou (2005), além de garantir a confidencialidade das informações, também oferece proteção à privacidade das informações do usuário, não permitindo a identificação da tag por um Leitor RFID não autorizado..

O trabalho realizado por Sakai et al. (2013) propôs um esquema de codificação de dois bits para proteção de canal retrogrado. Nesse esquema de codificação, o comprimento da palavra de código é dinamicamente alterada para cada bit de origem, o que aumenta o nível de dificuldade para o atacante calcular e identificar o ID original da tag original com base em comunicação anterior.

Os resultados obtidos nas simulações realizadas mostram que o esquema proposto supera as soluções anteriores para ataques de adivinhação e correlação de ID originais. Além disso, fornecem uma melhor proteção de canal retrógrado em Sistemas RFID comparados às soluções existentes, ainda assim trazem uma sobre sobrecarga à comunicação.

O trabalho realizado por Gao, Shu e Liu (2011) abordou os ataques de rastreamento e dessincronização. O ataque de rastreamento está relacionando diretamente a questões de privacidade.

4.1.6 CONFORMIDADE

Em Segurança da informação, o pilar Conformidade tem como objetivo garantir que a informação gerada atenda aos requisitos regulatórios e legais.
O governo do estado de São Paulo instituiu, por exemplo, o Protocolo de Transação Dual para operação nos sistema de arrecadação de pedágio nas rodovias do estado de São Paulo (RIGO e MARTE, 2001).

Leal et al. (2011) apresentam uma metodologia para avaliação automatizada de conformidade de equipamentos de Sistema de Transporte Inteligentes (ITS, do inglês Intelligent Transport System), operando com o protocolo de Transação Dual. A metodologia proposta testa a conformidade de execução dos comandos utilizados para operação do sistema.

De forma a adequar as regras em operação ao avanço da tecnologia, o governo do estado de São Paulo definiu novas normas para seu sistema de arrecadação da Secretária de Logística e Transportes (2011). As novas normas definiram o uso de RFID com um protocolo seguro para comunicação entre as tags e antenas nas praças de pedágios, buscando a compatibilidade com demais sistema em desenvolvimento no Brasil.

Leal. et al. (2013) apresentaram a criação de um testbed para tecnologias de Internet das Coisas. Esse ambiente permite a realização de testes de conformidade para o novo padrão de comunicação adotado pelo governo do estado de São Paulo, sem perder a compatibilidade com ambiente teste utilizado para a tecnologia anterior usada nas rodovias. Além disso, permite a conexão com ambientes experimentais para Internet das Coisas.

4.2 PERSPECTIVAS DE SEGURANÇA DA INFORMAÇÃO PARA CIDADES INTELIGENTES E INDÚSTRIA 4.0

A história apresenta um cenário em que a Segurança da Informação não é considerada nas fases iniciais de pesquisa e implantação de projetos de sistemas computacionais. No entanto, as tecnologias de internet incorporaram mecanismos de segurança da informação ao longo do tempo. Com o uso dessas redes ultrapassando as barreiras das redes de pesquisas das universidades, a infraestrutura computacional tornou-se exposta, permitindo o acesso aos sistemas e informações. Esse acesso permitiu a exploração da vulnerabilidade inerente à tecnologia, que até aquele momento era improvável. Com a exploração foram iniciados processos para implantar contramedidas, tornando o sistema seguro, sem perder funcionalidades.

Os trabalhos estudados neste capítulo abordam a exploração de vulnerabilidades e algumas contramedidas para tornar os sistemas computacionais utilizados em soluções de Internet das Coisas mais seguros. Entre os ataques vale destacar:

- Jamming (RSSF e RFID);
- Zapping (RFID);
- Dessincronização (RFID);
- Vampiro (RSSF);
- Sybil (RSSF, RFID);
- Buraco Negro (RSSF);
- Man-in-the-Middle (RFID, NFC);
- Skimming (RFID);
- Falsificação (RFID);
- Rastreamento (RFID).

As contramedidas propostas envolvem:
- Sistema de detecção de intrusão;
- Protocolos de autenticação;
- Protocolos de criptografia.

As iniciativas existentes de projetos de soluções para Cidades Inteligentes levam em consideração as lições aprendidas com as tecnologias precursoras. Os projetos incorporam os requisitos de Segurança da Informação em suas fases iniciais. Os sensores e atuadores são concebidos para atender a necessidade da aplicação, sem negligenciar os requisitos para disponibilidade, integridade e confidencialidade dos sistemas e informações.

Ainda assim, os projetos de soluções para Indústria 4.0 mantêm a cultura do sistema de tecnologia de automação, em que a necessidade de interoperabilidade ocorre dentro da própria empresa e não entre diferentes empresas. Nesse ambiente, a influência de agentes externos ainda não é considerada, pois, em geral, não existe comunicação com ambientes em nuvem. A disponibilidade e integridade estão restritas a um ambiente controlado, com características funcionais exigidas para operação da indústria, sem a necessidade de garantir confidencialidade.

Os aspectos de Segurança da Informação para a Indústria 4.0 necessitam levar em consideração que a comunicação com o ambiente externo irá expor vulnerabilidades ainda não exploradas. O estágio dos requisitos de segurança da informação dos projetos compara-se aos que eram utilizados nos primórdios da internet, mas com um importante diferencial, que é usar o conhecimento adquirido com as decisões do passado para identificar as vulnerabilidades e mitigar a materialização das falhas.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2013.

ASHRAF, A. et al. A model for classifying threats and framework association in wireless sensor networks. In: INTERNATIONAL CONFERENCE ON ANTI-COUNTERFEITING, SECURITY, AND IDENTIFICATION IN COMMUNICATION, 3., 2009, Hong Kong. Proceedings... Piscataway: IEEE, 2009.

AVANÇO, L. et al. An effective intrusion detection approach for jamming attacks on RFID systems. In: INTERNATIONAL EURASIP WORKSHOP ON RFID TECHNOLOGY (EURFID), 2015, Rosenheim. Proceedings... Piscataway: IEEE, 2015. p. 73–80. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7332388>. Acesso em: 20 nov. 2018.

DIMITRIOU, T. A lightweight RFID protocol to protect against traceability and cloning attacks. In: INTERNATIONAL CONFERENCE ON SECURITY AND PRIVACY FOR EMERGING AREAS IN COMMUNICATIONS NETWORKS, 1., 2005, Athens, Greece. Proceedings... Piscataway: IEEE, 2005. p. 59–66. Disponível em: <http://ieeexplore.ieee.org/document/1607559/>. Acesso em: 3 mar. 2019.

FELDHOFER, M.; AIGNER, M.; BAIER, T. Semi-passive RFID development platform for implementing and attacking security tags. In: INTERNATIONAL CONFERENCE FOR INTERNET TECHNOLOGY AND SECURED TRANSACTIONS, 2010. London. Proceedings... Piscataway: IEEE, 2010. v. 1, p.16–24. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5678040>. Acesso em: 8 maio 2013.

FERREIRA, M.; AZOGU, I.; LIU, H. Simulation of anti-relay attack schemes for RFID ETC system. In: COMMUNICATIONS AND NETWORKING SIMULATION SYMPOSIUM, 2012, Orlando. Proceedings...San Diego: Society for Computer Simulation International, 2012. Disponível em: <http://dl.acm.org/citation.cfm?id=2331771>. Acesso em: 4 jul. 2013.

FU, Y.; ZHANG, C.; WANG, J. A research on denial of service attack in passive RFID system. In: INTERNATIONAL CONFERENCE ON ANTI-COUNTERFEITING, SECURITY AND IDENTIFICATION, 2010, Chengdu, China. Proceedings... Piscataway: IEEE, 2010. p. 24–28. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5551848>. Acesso em: 16 maio 2013.

GAO, L.; SHU, Y.; LIU, C. RFID security protocol trace attack and desynchronizing attack deep research. In: INTERNATIONAL CONFERENCE ON COMPUTER SCIENCE AND NETWORK TECHNOLOGY, 2011, Harbin, China. Proceedings... Piscataway: IEEE, 2011. p. 918–922. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6182111>. Acesso em: 15 dez. 2018.

GETA, G. S. A hybrid fuzzy/genetic algorith for intrusion detection in RFID systems. Halifax: Dalhousie University, 2011. Disponível em: <http://dalspace.library.dal.ca:8080/handle/10222/14416>. Acesso em: 7 jul. 2013.

GONG, Z.; NIKOVA, S.; LAW, Y. W. KLEIN: a new family of lightweight block ciphers. RFID. In: Security and Privacy. Berlin: Spring, 2012. p. 1–18. Disponível em: <http://link.springer.com/chapter/10.1007/978-3-642-25286-0_1>. Acesso em: 8 maio 2013.

GOYAL, S. Wormhole and Sybil Attack in WSN : A Review. In: INTERNATIONAL CONFERENCE ON COMPUTING FOR SUSTAINABLE GLOBAL DEVELOPMENT, 2., 2015, New Delhi. Proceedings... Piscataway: IEEE, 2015. p. 1463–146. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7100491/>. Acesso em: 13 dez. 2018.

HANCKE, G. Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens. Journal of Computer Security, v. 19, p. 259–288, 2011.

HONG, L.; YONG, H. C.; ZHANG, Q. H. The survey of RFID attacks and defenses. In: INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS, NETWORKING AND MOBILE COMPUTING, 2012, Shanghai. Proceedings... Piscataway: IEEE, 2012. p. 1–4. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6478720>. Acesso em: 4 set. 2013.

JANGRA, A.; CHOUDHARY, R. A Framework to Detect Black Hole Attack in WSN Using Multi Base Stations Based Mechanism. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, v. 2, n. 5, p. 716–720, 2017.

JUELS, A. RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications, v. 24, n. 2, p. 381–394, 2006. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1589116>. Acesso em: 30 mar. 2019.

KAUSHAL, K.; SAHNI, V. Early Detection of DDoS Attack in WSN. International Journal of Computer Applications, v. 134, n. 13, p. 14–18, 2016. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.741.6288&rep=rep1&type=pdf>. Acesso em: 3 abr. 2019.

KHATAWKAR, P. et al. Wireless sensor network security threats. In: INTERNATIONAL CONFERENCE ON ADVANCES IN RECENT TECHNOLOGIES IN COMMUNICATION AND COMPUTING, 5., 2013, Bangalore. Proceedings... London: Institution of Engineering and Technology, 2013. v. 35, p. 131–135. Disponível em: <http://dl.acm.org/citation.cfm?id=168607%5Cnhttp://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1039518%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0%5Cnhttp://books.google.com/books?hl=en&lr=&id=pA2XUtdwewAC&oi=fnd>. Acesso em: 20 dez. 2018.

KORAK, T.; HUTTER, M. On the power of active relay attacks using custom-made proxies. In: IEEE INTERNATIONAL CONFERENCE ON RFID, IEEE RFID 2014, Proceedings... Piscataway: IEEE, 2014. p. 126–133.

KYWE, S. M.; LI, Y.; SHI, J. Attack and defense mechanisms of malicious EPC event injection in EPC discovery service. In: IEEE INTERNATIONAL CONFERENCE ON RFID-TECHNOLOGIES AND APPLICATIONS, 2013, Johor Bahru, Malaysia. Proceedings... Piscataway: IEEE, 2013. p. 4–5, 2013.

LEAL, A. G.; et al. Avaliação automatizada da conformidade e interoperabilidade de equipamentos e sistemas de its ao padrão ntcip por meio da plataforma de testes ttcn-3. In: CONGRESSO BRASILEIRO DE RODOVIAS E CONCESSÕES, 7., 2011, Foz do Iguaçu. Anais... São Paulo: Associação Brasileira de Concessionária de Rodovias, 2011. p. 1–15. Disponível em: <http://cbrcbrasvias.com.br/palestras/arquivos/TC0026-3.PDF>. Acesso em: 20 set. 2017.

LEAL, A. G. et al. Criação de Ambiente de Testes para Exploração de Tecnologias da Internet da Coisas Voltado Para Soluções de Transporte. In: CONFERÊNCIA IBERO AMERICANA WWW/ INTERNET, 2013, Porto Alegre. Anais... [S.l.]: IADIS, 2013. Disponível em: <http://www.iadisportal.org/digital-library/criação-de-ambiente-de-testes-para-exploração-de-tecnologias-da-"internet-das-coisas"-voltado-para-soluções-de-transporte>. Acesso em: 20 dez. 2017.

LIMA, J.; MIRI, A.; NEVINS, M. Analysis of relay attacks on RFiD systems. IEEE Latin America Transactions, v. 10, n. 1, p. 1274–1282, Jan. 2012. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6142473>. Acesso em: 4 abr. 2018.

LING, C. H. et al. A secure and efficient one-time password authentication scheme for WSN. International Journal of Network Security, v. 19, n. 2, p. 177–181, 2017.

NOMAN, A. N. M.; RAHMAN, S. M. M.; ADAMS, C. Improving security and usability of low cost RFID tags. In: ANNUAL INTERNATIONAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, 9., 2011, Montreal. Proceedings... Piscataway: IEEE, 2011.p. 134–141. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5971975>. Acesso em: 2 fev. 2018.

OREN, Y.; SCHIRMAN, D.; WOOL, A. RFID Jamming and Attacks on Israeli e-Voting. In: EUROPEAN CONFERENCE ON SMART OBJECTS, SYSTEMS AND TECHNOLOGIES (SMART SYSTECH), 2012, Osnabrück, Deutschland. Proceedings... Frankfur: Verlag, 2012. p. 1-7. Disponível em: <http://www.vde-verlag.de/proceedings-en/453441004.html>. Acesso em: 7 jul. 2013.

PATEL, A. A.; SONI, S. J. A novel proposal for defending against vampire attack in WSN. In: INTERNATIONAL CONFERENCE ON COMMUNICATION SYSTEMS AND NETWORK TECHNOLOGIES, 5., 2015, Gwalior, India. Proceedings... Piscataway: IEEE, 2015. p. 624–627. Disponível em: <http://ieeexplore.ieee.org/document/7279993/>. Acesso em: 6 jun. 2019.

RAO, A. L. N.; SILKY, P.; RANA, S. Review : location based authentication to mitigate intruder attack. International Journal of Engineering and Innovative Technology, v. 2, n. 9, p. 336–339, 2013. Disponível em: <http://www.ijeit.com/archive/15/vol 2/Issue 9/IJEIT1412201303_63.pdf>. Acesso em: 30 maio 2019.

RIGO, A. L.; MARTE, C. L. Protocolo de Transação Dual (PTD-Brasil): utilizado na Comunicação Dedicada de Curta Distância (DSRC) para Coleta Eletrônica de Pagamentos (EFC). São Paulo: IPT, 2001.

SAKAI, K.; KU, W.; ZIMMERMANN, R.; SUN, M.-T. Dynamic Bit Encoding for Privacy Protection against Correlation Attacks in RFID. Backward Channel, v. 62, n. 1, p. 112–123, 2013.

SECRETÁRIA DE LOGÍSTICA E TRANSPORTES. Resolução Secretária de Logística e Transportes - SLT 13/2011. São Paulo: SLT, 2011.

TAGRA, D.; RAHMAN, M.; SAMPALLI, S. Technique for preventing DoS attacks on RFID systems. In: INTERNATIONAL CONFERENCE ON SOFTWARE, TELECOMMUNICATIONS AND COMPUTER NETWORKS, 2010, Split, Dubrovnik. Proceedings... Piscataway: IEEE, 2010. p. 6–10. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5623669>. .Acesso 11 dez. 2018.

THAMILARASU, G.; SRIDHAR, R. Intrusion detection in RFID systems. In: IEEE MILITARY COMMUNICATIONS CONFERENCE, 2008, San Diego. Proceedings... Piscataway: IEEE, 2008. p. 1–7. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4753218>. Acesso em: 9 jul. 2013.

XU, W. et al. Jamming sensor networks: attack and defense strategies. IEEE Network, v. 20, n. 3, p. 41–47, June, 2006. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1637931>. Acesso em: 1 jun. 2013.

YANG, H.; GUO, J.; DENG, F. Collaborative RFID intrusion detection with an artificial immune system. Journal of Intelligent Information Systems, v. 36, n. 1, p. 1–26, 2011. Disponível em: <http://link.springer.com/10.1007/s10844-010-0118-3>. Acesso em: 7 jul. 2013.

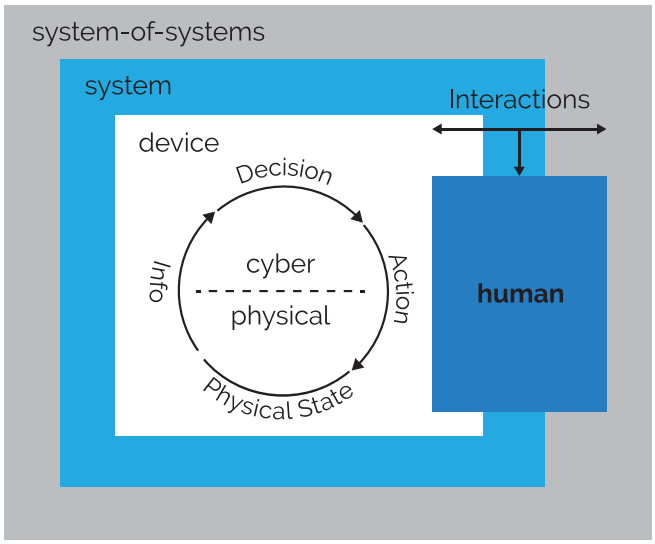
5 CONCLUSÃO

Este livro apresentou os conceitos básicos referentes às tecnologias chaves em IoT de forma a transpor a camada física diretamente associada a cada uma das tecnologias - RFID, RTLS e RSSF - para as aplicações em Cidades Inteligentes e Indústria 4.0, sem deixar de lado alguns aspectos importantes como disponibilidade dos serviços, confidencialidade e integridade das informações, sendo esses aspectos relacionados diretamente à Segurança da Informação.

Ao transpor a camada física para aplicações em Cidades Inteligentes e Indústria 4.0, o contexto é o de Sistemas Ciberfísicos. Segundo o documento "Framework for Cyber-Physical System: Overview", publicado pelo NIST em junho de 2017, um Sistema Ciberfísico deve prever a interação entre dispositivos, sistemas e pessoas (**Figura 60**):

> *Sistemas ciberfísicos (Cyber-physical systems – CPS) são sistemas inteligentes que incluem redes interativas projetadas de componentes físicos e computacionais. Esses sistemas altamente interconectados e integrados fornecem novas funcionalidades para melhorar a qualidade de vida e possibilitar avanços tecnológicos em áreas críticas, como assistência médica personalizada, resposta a emergências, gerenciamento de fluxo de tráfego, fabricação inteligente, defesa e segurança interna e fornecimento e uso de energia. (GRIFFOR et al., 2017)*

Figura 60. Modelo conceitual de referência para sistemas ciberfísicos, segundo NIST.



NIST CPS PWG Frameword Release 1.0

Fonte: Griffor et al.(2017)

Em Sistemas Ciberfísicos existe a necessidade de entrar em contato com o meio físico. Os conceitos e tecnologias apresentados neste livro concentram-se apenas nos desafios de transpor os fenômenos físicos, para que sejam integrados a meios digitais, a fim de que sejam aplicados recursos computacionais para criar o ecossistema ciberfísico.

Os Sistemas Ciberfísicos devem suportar provas de conceito em aplicações reais na quarta geração da indústria e em Cidades Inteligentes e sustentáveis. Vários desafios são enfrentados para superar os gargalos e obstáculos existentes, seja pela necessidade de incorporar novos conhecimentos na adequação de espaço físico, na infraestrutura laboratorial de software e hardware e no estabelecimento de parcerias com indústrias e gestores de cidades para desenvolvimento de protótipos realistas e de alto impacto.

Um ambiente ciberfísico integrado e organizado para suportar aplicações em Cidades Inteligentes e na manufatura avançada inclui uma atualização constante no estado da arte dos conceitos, aplicações e tecnologias, sendo uma arquitetura complexa, assim como a necessidade de profissionais com conhecimentos especializados. Esses dois pontos dificultam a expansão e disseminação desses cenários, algo que pode ser superado com o passar dos anos, com a evolução tecnológica e também com mecanismos mais transparentes para os usuários finais desses sistemas.

O uso das tecnologias RFID, RTLS e RSSF com aspectos de Segurança da Informação podem beneficiar e atingir a capilaridade necessária para que aplicações em Cidades Inteligentes exerçam sua principal função: aumentar a qualidade de vida e a satisfação das pessoas que vivem em cidades.

Ao longo deste livro, o uso das tecnologias chaves em IoT para Cidades Inteligentes foi amplamente discutido, destacando-se o uso de RFID no pagamento de transporte público e na coleta de tarifas de pedágio.

Como soluções futuras para Cidades Inteligentes, destacam-se:

- Ampliações de pesquisas em RTLS para diminuir as limitações atuais de exatidão dos sistemas de localização em ambiente indoor, de maneira que possam complementar as áreas de sombra existentes na cobertura atual de sistemas outdoor como o GPS das cidades;

- Uso de RSSF em soluções inteligentes nas áreas da saúde, construção, transporte, saneamento básido, distribuição de energia, meio ambiente (dos termos derivados em inglês: smart health, smart building, smart transportation; smart water, smart grid, smart environment), entre outras;

- Aumento dos requisitos de Segurança da Informação, que atualmente já são levados em consideração no desenvolvimento de sensores e atuadores, observando questões referentes à disponibilidade, integridade e confidencialidade dos sistemas e informações para atender as legislações referente a proteção de dados dos cidadãos.

A Indústria 4.0 também já faz o uso das Tecnologias chaves em IoT, destacando-se o uso de RFID no controle de estoque nos mais diversos segmentos, desde setores governamentais a indústrias siderúrgicas, passando pela indústria de eletrodomésticos.

Como soluções futuras para Indústria 4.0, destacam-se:

- Utilização de RTLS para controle de estoque, possibilitando a precisa localização física dos itens armazenados;

- Ampliação de pesquisas para aumentar a robustez física e lógica de RSSF, permitindo seu uso no ambiente industrial. Essas pesquisas podem proporcionar o uso na instrumentação das linhas de produção para obtenção, tratamento e processamento de dados com integração a mecanismos computacionais como Big Data e Inteligência Artificial. Essa integração também pode ser denominada como IIoT (Industrial Internet of Things);

- Inserção de requisitos de Segurança da Informação nos projetos, para garantir a integração de forma segura com os demais elementos computacionais neste contexto de Sistema Ciberfísico. Originalmente os aspectos de segurança não eram considerados devido à natureza de isolação do ambiente industrial em relação ao ambiente de tecnologia da informação.

Em 25 de junho de 2019, o governo federal publicou o Decreto nº 9.854, que institui o Plano Nacional de Internet das Coisas. Em seu Artº 1, afirma:

Fica instituído o Plano Nacional de Internet das Coisas com a finalidade de implementar e desenvolver a Internet das Coisas no País e, com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais. (BRASIL, 2019).

O Plano Nacional de Internet das Coisas tem como objetivo melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços prestados utilizando soluções de IoT; promover a capacitação profissional relacionada às aplicações de IoT; criar um ecossistema de inovação em IoT buscando aumentar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT.

Além disso, o Plano Nacional de Internet das Coisas busca promover a participação em fóruns, pesquisas, desenvolvimento e inovação internacionais para inserir o país nas discussões por padrões internacionais.

As áreas da saúde, cidades, indústria e rural são apontadas com prioritárias pelo Plano Nacional de Internet das Coisas. Os principais projetos integradores para atender essas áreas envolvem a criação de Plataforma de Inovação em Internet das Coisas e a implementação de Centros de Competência para Tecnologias Habilitadoras em Internet das Coisas.

REFERÊNCIAS

GRIFFOR, E. R. et al. Framework for Cyber-Physical System: Overview. Washington: NIST, 2017. 79 p. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf>. Acesso em: 3 mar. 2019.

BRASIL. Decreto nº 9.854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Diário Oficial da União, Brasília, 26 jun. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm>. Acesso em: 7 jul. 2019.

SIGLÁRIO

IOT
Internet of Things (Internet das Coisas)

BNDES
Banco Nacional de Desenvolvimento Econômico e Social

ITU-T
União Internacional de Telecomunicações

TICS
Tecnologias de Informação e Comunicação

CPS
Cyber-physical systems (Sistemas Ciberfísicos)

RSSF
Redes de Sensores Sem Fio

RFID
Identificação por Radiofrequência

RTLS
Real-Time Locating System (Sistemas de Localização em Tempo Real)

WSN
Wireless Sensor Networks (Redes de Sensores sem Fio)

MANET
Mobile Ad hoc NETworks

LPWAN
Low Power Wide Area Network

MIT
Massachusetts Institute of Technology

GPS
Global Positioning System (Sistema de Posicionamento Global)

IFF
Identification Friend or Foe (Identificação de Amigo ou Inimigo)

FHSS
Frequency Hopping Spread Spectrum (Espalhamento Espectral com Salto em Frequência)

ISO
International Organization for Standardization

IEC
International Electrotechnical Commission

PIE
Pulse Interval Encoding (Codificação por Intervalo de Pulso)

PPE
Pulse Position Encoding (Codificação por Posição de Pulso)

NFC
Near Field Communication (Comunicação por Campo Próximo)

GNSS
Global Navigation Satellite System (Sistema de Navegação Global por Satélite)

NAVSTAR-GPS
NAVigation Satellite with Time and Ranging

WI-FI
Wireless Fidelity

SSID
Service Set Identifier

PHY
Physical Layer

MAC
Medium Access Control (Controle de Acesso ao Meio)

SIG
Special Interest Group

RSSI
Received Signal Strength Indication (Variação da Intensidade do Sinal)

AOA
Angle of Arrival (ngulo de Chegada)

TOA
Time of Arrival (Tempo de Recebimento)

LO
Local Oscillator (Oscilador Local)

NLOS
Non-Line-Of-Sight

RMSE
Root Mean Square Error

IIOT
Industrial Internet of Things

RF
Radiofrequência

NIST
Instituto Nacional de Padrões e Tecnologia dos Estados Unidos

SS
Signal Strength

UMAP
Ultra Light Mutual Authentication Protocols (Protocolos Ultra Leves de Autenticação Mútua).

AODV
Ad-hoc on Demand Distance Vector Routing

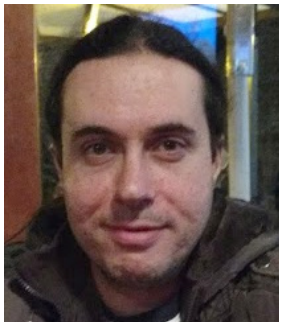
EPCDS
Serviço Eletrônico de Descoberta de Código de Produto (Electronic Product Code Discovery Service)

ITS
Intelligent Transport System (Sistema de Transporte Inteligentes)

SOBRE OS AUTORES

ALESSANDRO SANTIAGO DOS SANTOS

Nascido em 1974 na cidade de Goiânia-Goiás. Doutor em Engenharia de Transportes na Universidade de São Paulo desde 2018, onde também obteve o título de Mestre em Ciências da Computação em 2003. Bacharel em Ciência da Computação pela Universidade Federal de Mato Grosso (1997). Pesquisador do Instituto de Pesquisas Tecnológicas do Estado de São Paulo, atuando no Centro de Tecnologia da Informação, Automação e Mobilidade, por onde atuou como pesquisador chefe do laboratório de vírus digitais; gerente de seção de redes e segurança; atualmente chefia a seção de automação, governança e mobilidade digital. Têm atuado frequentemente em Comissões de Sistemas Inteligentes de Transporte (ITS) na Associação Brasileira de Normas Técnicas (ABNT), na Associação Nacional de Transporte Público (ANTP), etc.. Professor universitário. Dedica-se a pesquisas e projetos em linhas de trabalho como: Redes de Computadores, ITS, IoT, Sistemas Ciberfísicos, Cidades Inteligentes, Indústria 4.0 e Computação Aplicada. Além disso, atua em redes de cooperação da europa em pesquisa nas áreas de TIC e Transporte.



LEANDRO AVANÇO

Nascido em 1979 na cidade de Diadema/SP. Mestre em Engenharia de Computação - Redes de Computadores no IPT - Instituto de Pesquisas Tecnológicas do Estado de São Paulo desde 2015. Engenheiro Eletricista com Ênfase em Telecomunicações pela FEI (Fundação Educacional Inaciana Padre Sabóia de Medeiros) em 2007. Atuou na área de infraestrutura de TIC em empresas do setor financeiro. Tem atuado em comitês nas áreas de RFID da ARTESP. Pesquisador do Instituto de Pesquisas Tecnológicas do Estado de São Paulo na seção de Automação, Governança e Mobilidade Digital do Centro de Tecnologia da Informação, Automação e Mobilidade. Professor universitário. Dedica-se a projetos e pesquisas em linhas de trabalho como: Redes de Computadores, Infraestrutura de TIC, IoT, RFID, ITS, Cidades Inteligentes, Indústria 4.0, Governança de TI, Gestão da Segurança da Informação e Segurança Cibernética.

MATHEUS JACON PEREIRA

Nascido em 1986 na cidade de Araçatuba-SP. Possui graduação em Engenharia Elétrica pela Universidade Estadual Paulista Júlio de Mesquita Filho, UNESP (2010) e mestrado em Engenharia da Computação - Redes de Computadores pelo IPT - Instituto de Pesquisas Tecnológicas do Estado de São Paulo (2016). Atuou na área de P&D em empresas do setor de telecomunicações. Tem atuado em Comissões e Comitês nas áreas de IoT e RFID da ARTESP e ANATEL. Professor Universitário. Pesquisador do Instituto de Pesquisas Tecnológicas do Estado de São Paulo, atuando no Centro de Tecnologia da Informação, Automação e Mobilidade. Dedica-se a pesquisas e projetos em linhas de trabalho como: Redes de Computadores, Governança de TI, RFID, ITS, IoT, Sistemas Ciberfísicos, Cidades Inteligentes, Indústria 4.0 e Automação.

ISBN: 978-65-5702-000-5
CBL
9 786557 020005

FAPESP

Fundação de Apoio ao Instituto de Pesquisas Tecnológicas
fipt

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Desenvolvimento Econômico

ipt
INSTITUTO DE PESQUISAS TECNOLÓGICAS