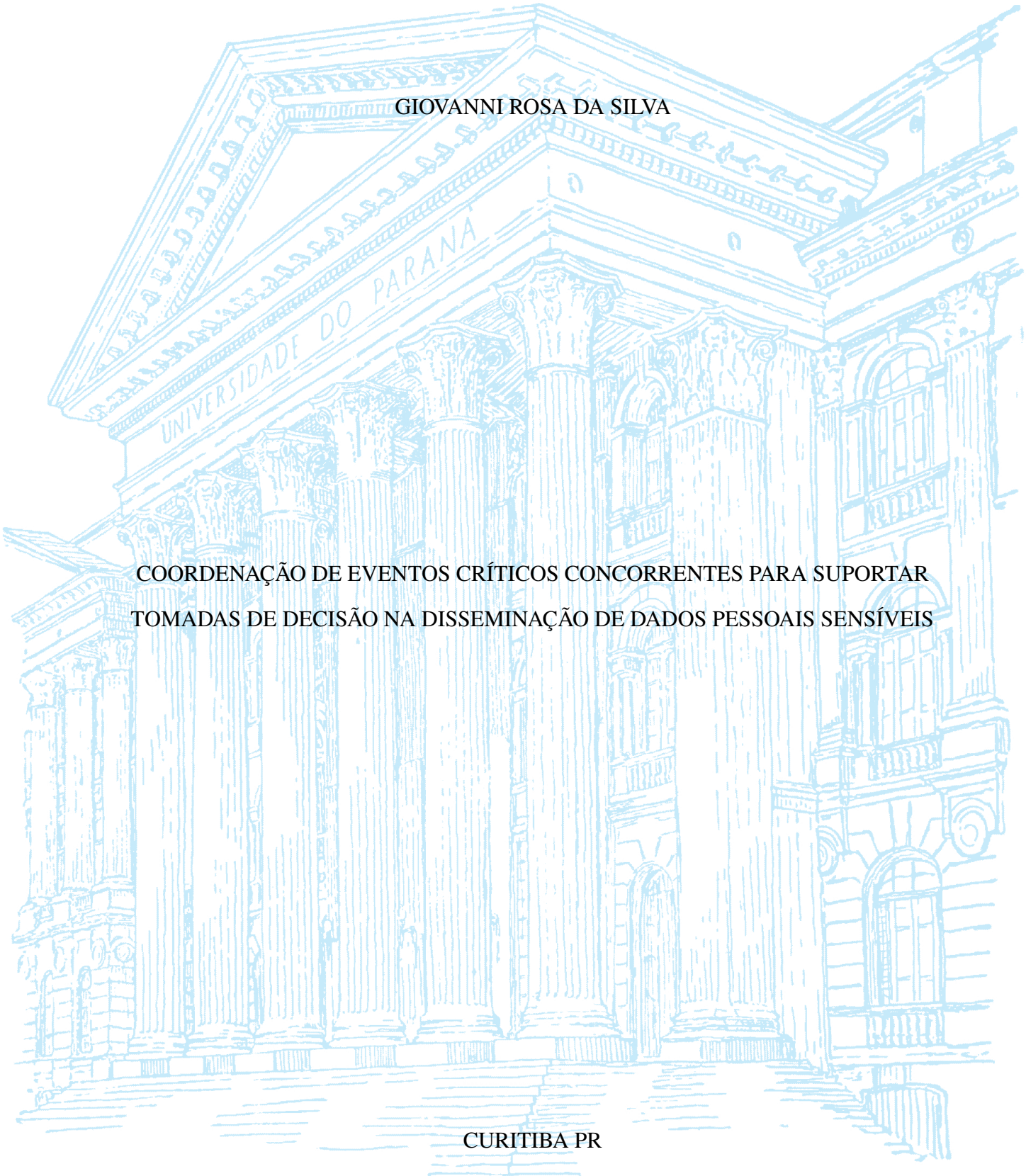
UNIVERSIDADE FEDERAL DO PARANÁ

GIOVANNI ROSA DA SILVA



COORDENAÇÃO DE EVENTOS CRÍTICOS CONCORRENTES PARA SUPORTAR TOMADAS DE DECISÃO NA DISSEMINAÇÃO DE DADOS PESSOAIS SENSÍVEIS

CURITIBA PR

2019

GIOVANNI ROSA DA SILVA

COORDENAÇÃO DE EVENTOS CRÍTICOS CONCORRENTES PARA SUPORTAR TOMADAS DE DECISÃO NA DISSEMINAÇÃO DE DADOS PESSOAIS SENSÍVEIS

Trabalho apresentado como requisito parcial à conclusão do Curso de Bacharelado em Ciência da Computação, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Aldri Luiz dos Santos.

Coorientador: Agnaldo de Souza Batista.

CURITIBA PR

2019

RESUMO

A expansão da Internet contribuiu para a popularização do uso de redes sem fio, com o padrão IEEE 802.11. Em especial, destaca-se o surgimento da IoT, um paradigma que estimula a criação de aplicações com objetos do mundo real conectados à Internet. A partir da união entre conceitos das SNs e da IoT surgiu um novo paradigma chamado de SIoT. Com a extração e processamento de aspectos sociais é possível criar modelos para representar comportamentos complexos do mundo real. No âmbito de redes complexas e oportunísticas, destaca-se a formação de comunidades para agrupamento de dispositivos, a fim de encontrar alguma similaridade entre seus donos. A avaliação de confiança também é uma técnica utilizada para tomadas de decisões em redes autônomas. Esse trabalho aproveita esses conhecimentos para propor um sistema de coordenação de eventos críticos concorrentes para disseminação de dados pessoais sensíveis. A proposta considera a interação oportunística entre os dispositivos para a formação de comunidades de interesse. Durante essa interação, um dispositivo avalia a confiança entre ele e outro dispositivo baseado na competência do outro dispositivo e a similaridade entre os seus conjuntos de interesse. Em um evento crítico, o sistema escolhe o dispositivo com quem apresenta o maior valor de confiança para disseminar seus dados pessoais sensíveis. A proposta ainda verifica um intervalo de tempo para garantir que o dispositivo receptor dos dados sensíveis tenha a oportunidade de agir. O sistema escolhe outro receptor até que garanta uma disseminação de sucesso. Isso assegura uma gestão ágil e assertiva na ocorrência de eventos críticos simultâneos e sequenciais. Os resultados demonstram que o sistema levou no máximo 8,1ms para disseminar os dados, chegando a atingir uma taxa de sucesso na disseminação dos dados de 100% em alguns casos.

Palavras-chave: Coordenação de Eventos Críticos Concorrentes, Disseminação de Dados Pessoais Sensíveis, SIoT, Comunidades de Interesse, Avaliação da Confiança, Redes Oportunísticas

ABSTRACT

The expansion of the Internet has also contributed to the popularization of wireless networks, using the IEEE 802.11 standard. In particular, IoT stands out as a paradigm that encourages the creation of applications with real-world objects connected to the Internet. From the union between concepts of SNs and IoT, a new paradigm called SIoT emerged. With the extraction and processing of social aspects, it is possible to create models to represent complex real-world behaviors. Within complex and opportunistic networks, the formation of communities for device clustering to find some similarity among their owners stands out. Trust evaluation is also a technique used to make decisions in autonomous networks. This work leverages this knowledge to propose a concurrent critical events coordination system for the dissemination of sensitive personal data. The proposal considers opportunistic interactions between devices in order to form communities of interest. During this interaction, a device evaluates trust between it and another device based on the other device's competence and similarity between its sets of interest. In a critical event, the system selects the device that has the highest trust value to disseminate its owner's personal data. The proposal also checks a time frame to ensure that the data receiving device can have the opportunity to act. The system selects another receiver until it vouches for successful dissemination. This assures agile and assertive management in the occurrence of simultaneous and sequential critical events. Results show that the system reached a maximum of 8.1ms to disseminate the data, reaching a success rate of 100% in some cases.

Keywords: Coordination of Concurrent Critical Events, Sensitive Personal Data Dissemination, SIoT, Communities of Interest, Trust Evaluation, Opportunistic Networks

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

4G	Cellular Network Fourth Generation Technology (Tecnologia de quarta geração de rede celular)
5G	Cellular Network Fifth Generation Technology (Tecnologia de quinta geração de rede celular)
AES	Advanced Encryption Standard (Padrão avançado de criptografia)
AP	Access Point (Ponto de acesso)
ARPA	Advanced Research Projects Agency (Agência de projetos de pesquisa avançada)
ARPANET	Advanced Research Projects Agency NETwork (Rede da agência de projetos de pesquisa avançada)
CCMP	Counter Cipher Mode Protocol (Protocolo do modo de contador de cifras)
CD	Community Discovery (Descoberta de comunidade)
CoI	Community of Interest (Comunidade de interesse)
CSMA	Carrier Sense Multiple Access (Acesso múltiplo com detecção de portadora)
DAG	Directed Acyclic Graph (Grafo acíclico dirigido)
DCD	Dynamic Community Discovery (Descoberta de comunidade dinâmica)
DInf	Departamento de Informática
DNS	Domain Name System (Sistema de nomes de domínio)
DSL	Digital Subscriber Line (Linha de assinante digital)
DTN	Delay-Tolerant Networking (Redes tolerantes a atraso)
FTP	File Transfer Protocol (Protocolo de transferência de arquivos)
Gbps	Gigabits per second (Gigabits por segundo)

GDPR	General Data Protection Regulation (Regulamento Geral de Proteção de Dados)
GHz	Gigahertz
GNU	GNU's Not Unix (GNU não é Unix)
GNU GLPv2	GNU General Public License version 2 (Licença Pública Geral GNU versão 2)
H2H	Human-to-Human (Humano para Humano)
HTTP	Hypertext Transfer Protocol (Protocolo de transferência de hipertexto)
ICM	Information City Model (Modelo de informação da cidade)
ICMP	Internet Control Message Protocol (Protocolo de mensagens de controle da Internet)
IDE	Integrated Development Environment (Ambiente de desenvolvimento integrado)
IEEE	Institute of Electrical and Electronics Engineers (Instituto de engenheiros elétricos e eletrônicos)
IoT	Internet of Things (Internet das Coisas)
IP	Internet Protocol (Protocolo da Internet)
IPv4	Internet Protocol version 4 (Protocolo da Internet versão 4)
LAN	Local Area Network (Redes locais)
LGPD	Lei Geral de Proteção de Dados
M2M	Machine-to-Machine (Máquina para máquina)
MAN	Metropolitan Area Network (Redes metropolitanas)
MANET	Mobile Ad Hoc Network (Redes ad hoc móveis)
Mbps	Megabits per second (Megabits por segundo)
NAP	Network Access Protection (Proteção de acesso à rede)

NFC	Near Field Communication (Comunicação por campo de proximidade)
NS-3	Network Simulator 3 (Simulador de rede 3)
NSF	National Science Foundation (Fundação nacional de ciências)
NSFNET	National Science Foundation NETwork (Rede da fundação nacional de ciências)
OFDM	Orthogonal Frequency Division Multiplexing (Multiplexação de divisão de frequência ortogonal)
OSI	Open System Interconnection (Interconexão de sistemas abertos)
OSN	Opportunistic Social Network (Rede social oportunística)
PAN	Personal Area Network (Redes pessoais)
RFID	Radio-Frequency IDentification (Identificação por rádio frequência)
RTP	Real-Time Transport Protocol (Protocolo de transporte em tempo real)
SIoT	Social Internet of Things (Internet das Coisas Social)
SMTP	Simple Mail Transfer Protocol (Protocolo simples de transferência de correio)
SN	Social Network (Rede social)
SONET	Synchronous Optical NETworking (Rede óptica síncrona)
SRI	Stanford Research Institute (Instituto de pesquisa de Stanford)
T2T	Thing-to-Thing (Coisa para coisa)
TCP	Transmission Control Protocol (Protocolo de controle de transmissão)
UCLA	University of California, Los Angeles (Universidade da Califórnia em Los Angeles)
UCSB	University of California, Santa Barbara (Universidade da Califórnia em Santa Bárbara)

UDP	User Datagram Protocol (Protocolo de datagrama do usuário)
UFPR	Universidade Federal do Paraná
UTAH	University of Utah (Universidade de Utah)
VANET	Vehicular Ad Hoc Network (Rede ad hoc veicular)
WAN	Wide Area Network (Redes abrangentes)
WEP	Wired Equivalent Privacy (Privacidade equivalente com fio)
Wi-Fi	Wireless Fidelity (Fidelidade sem fio)
WLAN	Wireless Local Area Network (Rede de alcance local sem fio)
WPA	Wi-Fi Protected Access (Acesso protegido por Wi-Fi)
WPA2	Wi-Fi Protected Access 2 (Acesso protegido por Wi-Fi 2)
WSN	Wireless Sensor Network (Rede de sensores sem fio)
WWW	World Wide Web (Rede mundial de computadores)

LISTA DE SÍMBOLOS

τ	tau, décima nona letra do alfabeto grego

SUMÁRIO

1 INTRODUÇÃO

Os dispositivos computacionais estão cada vez mais presentes no cotidiano das pessoas auxiliando em diversas tarefas com diferentes interesses e propósitos. Apesar deles funcionarem de forma isolada, é comum os dispositivos estarem conectados por uma rede que os permita trocar informações. As redes de computadores são utilizadas tanto por empresas quanto por indivíduos para fornecer um serviço realizado para pessoas em lugares específicos, como em casa ou no trabalho, ou em movimento, nas ruas, carros, barcos ou aviões. Elas são classificadas de acordo com seu alcance em redes pessoais (do inglês, *Personal Area Network* - PAN); locais (do inglês, *Local Area Network* - LAN); metropolitanas (do inglês, *Metropolitan Area Network* - MAN); a longas distâncias (do inglês, *Wide Area Network* - WAN); e interligadas (do inglês, *internets*). Desta última classificação, pode-se citar como exemplo a Internet, a qual é um vasto conjunto de redes diferentes que utilizam uma tecnologia comum, interligadas a nível mundial (Tanenbaum et al., 2011).

A Internet tem sido utilizada por mais da metade da população mundial, tendo mais de 4,5 bilhões de usuários. Essa rede mundial tem colaborado ao surgimento e a transformação de vários serviços, como comércio eletrônico, acesso à informação, redes sociais, cuidados de saúde, educação, entre outros. Inicialmente, apenas os cabos conectavam dispositivos computacionais fixos na Internet. Nesse período, ainda não se considerava a mobilidade desses dispositivos. O desenvolvimento das tecnologias de comunicação sem fio possibilitou que os dispositivos computacionais se conectassem em redes a partir de qualquer local e a qualquer momento. Logo, a conexão do dispositivo na medida em que ele se movimenta se tornou possível e se popularizou. Atualmente, há 5,11 bilhões de usuários de dispositivos móveis no mundo, sendo que 3,986 bilhões desses usuários usavam a internet móvel em 2018 (We Are Social Ltd, 2019).

O trabalho de (Weiser, 1991) em 1991 previa que dispositivos computacionais conectados por fios, ondas de rádio e infravermelho seriam tão onipresentes (ubíquos), que suas presenças não seriam notadas. Dessa visão surgiu a Intranet das Coisas (do inglês, *Intranet of Things*), onde dispositivos computacionais interagem localmente (Ortiz et al., 2014). A Internet das Coisas (do inglês, *Internet of Things* - IoT) foi uma evolução natural dessa rede após o surgimento da Internet. Na IoT, diversos tipos de dispositivos computacionais, denominados de objetos, utilizam a infraestrutura da rede mundial para comunicação. A IoT é um novo paradigma que tem ganho relevância nos últimos anos com a utilização de sensores, identificadores e dispositivos móveis (Atzori et al., 2010). Esse paradigma possibilita que num futuro próximo entidades digitais e físicas possam interagir com a finalidade de prover serviços (Miorandi et al., 2012).

Os dispositivos conectados em rede carregam diversas informações, inclusive algumas relativas aos seus proprietários e suas relações sociais, tais como interesses e competências. Nesse contexto, surge a Internet das Coisas Social (do inglês, *Social Internet of Things* - SIoT). Nela os objetos estabelecem relações sociais de maneira autônoma, utilizando as redes sociais dos proprietários dos dispositivos. Na medida em que esses dispositivos estabelecem relações de confiança utilizando características de seus donos, eles têm condições de prover serviços de forma oportunística (Chen et al., 2016). Apesar de serviços com foco em SIoT proverem conveniência e conforto para as pessoas, discussões sobre privacidade dos dados surgem nesse ínterim. Leis como a Lei Geral de Proteção de Dados (LGPD), que entra em vigor no Brasil em agosto de 2020, e a *General Data Protection Regulation* (GDPR), que entrou em vigor na União Europeia em maio de 2018, surgiram para regular a utilização de dados pessoais (Barsotti, 2019).

A privacidade tem sido uma preocupação constante na área de redes devido às informações sensíveis que nelas trafegam (Tanenbaum et al., 2011).

No contexto da SIoT, a confiança entre dois dispositivos é um fator determinante para disseminação de dados. Ela pode ser verificada a partir de características como honestidade, cooperatividade e interesses (Chen et al., 2016; Bao et al., 2013). Uma comunidade de interesse (do inglês, *Community of Interest* - CoI) pode ser formada quando dispositivos de uma rede compartilham um mesmo interesse, possibilitando formações de agrupamentos. Adicionalmente, é preciso definir o grau de confiança para que uma informação sensível não seja disseminada para um dispositivo que apresente um comportamento malicioso e venha a comprometer a privacidade do emissor.

Além disso, nesse ambiente de redes formadas dinamicamente, as decisões são tomadas apenas com dados do instante atual, dispensando a necessidade de armazenar maiores quantidades de informação. Essa característica é denominada *Zero-Knowledge* (Feige et al., 1988), que indica que as tomadas de decisão ocorrem a partir de informações atuais, ou seja, eventos passados são desconsiderados.

1.1 APLICAÇÕES

Os domínios de aplicação são diversos quando tratamos de IoT devido aos seus potenciais. Atualmente, as pessoas estão cercadas de objetos em todos os ambientes, mas apenas uma pequena parcela deles está conectada a alguma rede e transmite informações. A aplicação da IoT pode contribuir para a melhoria da qualidade de vida das pessoas, seja em casa, em viagem, em tratamento médico, no trabalho, na academia, entre outras situações. Segundo (Atzori et al., 2010), diversas áreas podem se beneficiar do emprego da IoT, tais como:

Transporte e logística: nos transportes destacam-se os avanços de tecnologia dos carros, trens, bicicletas bem como rodovias e trilhos, que vem sendo equipados com sensores, atuadores e processamento de energia. Identificadores e sensores tem ajudado a gerenciar o tráfego nas cidades, e também a rastrear produtos em transporte. A utilização de tecnologias como RFID (do inglês, *Radio-Frequency IDentification*) e NFC (do inglês, *Near Field Communication*) permite o processamento de informações em tempo real, possibilitando uma melhor rastreabilidade dos bens de consumo nas cadeias de produção e distribuição. Carros autônomos e mapas com realidade aumentada para auxiliar turistas também são possíveis aplicações nessa área.

Cuidados com a saúde: na área da saúde vários benefícios surgiram com o uso da IoT. Entre eles, o rastreamento em tempo real de pessoas e objetos em movimento para, por exemplo, monitorar o fluxo dentro de um hospital a fim de otimizar processos e controlar inventários. Ela permite a identificação e autenticação de pessoas para registros em hospitais com a finalidade de manter um histórico de atendimentos e evitar uso de medicamentos indevidos. Ela possibilita a coleta automática e análise de dados com aprendizado de máquina (do inglês, *Machine Learning*) para atendimentos automatizados, procedimentos de auditoria e gestão de inventário médico. A utilização da IoT por meio de sensores auxilia no monitoramento de pacientes em tempo real para ajudar em diagnósticos e indicadores de saúde. Por fim, a integração de diferentes tecnologias de rede sem fio ajuda na resiliência de monitoramentos de sinais biológicos em situações de mobilidade dos pacientes.

Ambientes inteligentes (do inglês, *smart homes, smart cities*): nesse contexto, sensores e atuadores distribuídos em casa ou escritórios ajudam a prover maior conforto para as pessoas. Eles possibilitam a regulação da temperatura ambiente, luzes, energia e o controle de equipamentos

eletrônicos à distância. A indústria 4.0 também depende dessas tecnologias para assegurar um controle de qualidade rigoroso e um planejamento de produção baseado em dados estatísticos coletados de sensores nas fábricas. No lazer, museus e academias inteligentes são exemplos existentes. Além disso, cidades inteligentes ganham cada vez mais incentivo, como por exemplo Curitiba, que por meio do Vale do Pinhão e outras iniciativas fomenta um ecossistema de inovação (Gazeta do Povo, 2019).

Domínio pessoal e social: aplicações desse domínio são aquelas que possibilitam a interação entre pessoas para manter ou construir relações sociais. Entre exemplos práticos destacam-se a utilização do RFID e Wi-Fi (do inglês, *Wireless Fidelity*) para geração de eventos que podem ser compartilhados em redes sociais como Facebook ou Twitter. Além disso, a análise de dados históricos para identificar tendências em atividades ao longo do tempo surge como outra aplicação. Ademais, mecanismos de busca por objetos perdidos por meio de RFID, disponibilizando as últimas posições ou a localidade atual é outro exemplo nessa área. Por fim, alertas de roubos ao detectar se um objeto saiu de uma determinada área restrita com o uso de sensores é mais uma possibilidade.

Aplicações futurísticas: se encaixam nesse domínio aplicações que ainda não dispõem de tecnologias necessárias a sua implementação ou que a sociedade ainda não está preparada para utilizar (Atzori et al., 2010). Pode-se citar táxis autônomos, os quais otimizariam o tempo de espera e trajeto dos usuários ao utilizar dados do trânsito em tempo real, e comunicariam-se entre si de modo a ficarem bem distribuídos nas regiões. Outra aplicação seria um Modelo de Informação da Cidade (do inglês, *Information City Model* - ICM), que disponibilizaria informações sobre construções e infraestruturas da cidade, como esgoto, rede de energia, linhas de trem, corredores de ônibus, etc. Desse modo, prédios poderiam compartilhar energia e outros recursos a fim de otimizar o custo benefício e a oferta e demanda. Planejamentos e projetos seriam realizados de maneira inteligente com base em estatísticas. Por fim, mas não menos interessante, uma sala de jogos aprimorada equipada com sensores de localização, movimento, aceleração, umidade, temperatura, barulho, voz, informação visual, batimentos cardíacos e pressão sanguínea surge com a utilização de dados coletados desses sensores para fornecer uma experiência imersiva em jogos computacionais. Cenários interativos com sensores de toque também são uma possibilidade de aplicação com uso de IoT.

1.2 CARACTERÍSTICAS

Esse trabalho explora as redes sem fio locais (do inglês, *Wireless Local Area Network* - WLAN), por meio da tecnologia Wi-Fi. Além disso, a proposta deste trabalho considera uma situação de mobilidade dos dispositivos na rede, que é um fator importante para demonstrar a formação das redes de maneira oportunística. Na medida em que os dispositivos entram no raio de alcance um do outro, suas respectivas vizinhanças são atualizadas. O cálculo da confiança em tempo real também é um dos principais mecanismos que influenciam na seleção do dispositivo para o qual os dados são disseminados. Este trabalho utiliza comunidades de interesse para formar grupos dentro das vizinhanças e classifica os dispositivos nessa comunidade de acordo com a similaridade de interesses entre o emissor e o receptor, e do grau de competência do dispositivo receptor da disseminação do evento crítico. Um evento crítico caracteriza-se como uma situação emergencial, onde uma pessoa está sob um risco iminente, como por exemplo no caso de uma queda de alta gravidade, um infarto, um atropelamento, entre outros tipos de urgências. Ademais, entende-se que uma pessoa está em estado crítico após a ocorrência do evento crítico. Por fim, o trabalho explora um ambiente *Zero-Knowledge*, onde a disseminação

dos dados não é realizada com base em informações coletadas ao longo do tempo, mas apenas com conhecimentos do instante atual.

1.3 OBJETIVOS

O domínio de aplicação tratado neste trabalho é a saúde, área na qual a utilização de sensores e redes sem fio mostram-se úteis para diversas finalidades, como as que foram citadas anteriormente. De acordo com (Thibaud et al., 2018), alguns fatores e necessidades incentivam pesquisas nesse domínio, tais como o aumento da expectativa de vida das pessoas, associado ao aumento de doenças crônicas; a falta de informações de saúde disponíveis sobre os pacientes e de uma gestão sistemática; o avanço de tecnologias de redes sem fio, tecnologias vestíveis (do inglês, *wearables*) e sensores, como RFID; a tendência de tratamentos de saúde feitos em casa ao invés de hospitais; a falta de treinamento das pessoas envolvidas com atendimento médico; e a falta de cuidados com a segurança e privacidade dos dados.

Com base nessas necessidades e nos potenciais da utilização da IoT nessa área vital, este trabalho apresenta um sistema para coordenação de eventos críticos concorrentes para disseminação de dados pessoais sensíveis. A aplicação construída simula pessoas com diferentes competências e um conjunto de interesses andando pelas ruas de uma cidade. Os dispositivos dessas pessoas interagem de maneira autônoma, formando comunidades de interesse com outros dispositivos no raio de alcance das ondas de rádio do sinal Wi-Fi. Dentro das comunidades, é calculada a similaridade entre o conjunto de interesses do dispositivo emissor e do receptor, assim como o grau de competência do dispositivo receptor da mensagem. Com isso, é possível chegar a um ranqueamento, onde o melhor dispositivo é escolhido para receber a disseminação de dados sensíveis sobre o dono do dispositivo emissor. Dessa maneira, pode-se reagir a um evento crítico com agilidade e com a segurança de que os dados serão compartilhados com uma pessoa de confiabilidade compatível com o recebimento daquele dado sensível.

Portanto, os principais objetivos desse trabalho são propor um algoritmo capaz de gerenciar a ocorrência de eventos críticos concorrentes que podem interferir em um atendimento e assegurar um tempo de resposta suficiente para o receptor do evento crítico. Como objetivos secundários estão a garantia de privacidade dos dados pessoais sensíveis por meio do mecanismo de avaliação da confiança, a capacidade de agrupar dispositivos pela similaridade de interesses e o estabelecimento de relações oportunísticas em uma rede dinâmica.

1.4 ESTRUTURA DA MONOGRAFIA

Esta monografia está estruturada em 6 capítulos. O Capítulo 2 apresenta os conceitos necessários para a compreensão do desenvolvimento da pesquisa. O Capítulo 3 discorre sobre os trabalhos relacionados. O Capítulo 4 descreve como foi projetado e implementado o mecanismo proposto. O Capítulo 5 apresenta a avaliação da implementação proposta com relação ao mecanismo. Finalmente, o Capítulo 6 apresenta as considerações finais sobre o estudo realizado.

2 FUNDAMENTOS

Este capítulo apresenta os fundamentos necessários ao entendimento desse trabalho de pesquisa. A Seção 2.1 apresenta questões relacionadas à privacidade dos dados na IoT. A Seção 2.2 discorre sobre as redes de computadores, seus tipos e classificações. A Seção 2.3 apresenta a evolução da computação ubíqua e descreve alguns conceitos que servem de ferramenta para o funcionamento de aplicações no contexto da SIoT.

2.1 PRIVACIDADE DOS DADOS NA IOT

Privacidade consiste no direito de indivíduos manterem sigilo e controle sobre suas informações (Porambage et al., 2016). A utilização de uma enorme quantidade de sensores e dispositivos gera grandes massas de dados no contexto da IoT. Esses dados contém informações que podem comprometer a privacidade das pessoas. Um atacante pode se apropriar desses dados para rastrear, localizar, traçar perfis e até chantagear seus proprietários. Além disso, a aplicação de técnicas em grandes quantidades de informação revela tendências e comportamentos que podem ser explorados (Porambage et al., 2016). Esse problema torna-se ainda mais voltado às pessoas em SIoT, onde dados pessoais são gerados, transportados, processados e possivelmente armazenados. Regulações e conceitos estão sendo definidos para abordar essas questões.

2.1.1 Dados pessoais e dados sensíveis

De acordo com (Intersoft Consulting, 2019) baseada na GDPR, os dados pessoais carregam informações sobre uma pessoa, tais como de identificação direta, como nome, sobrenome e número de telefone. Além disso, essa categoria inclui dados com a utilização de pseudônimos ou informações de identificação não direta que não permitem a identificação direta de usuários, mas permitem a individualização de comportamentos. A GDPR incentiva o uso de dados de identificação não direta para minimizar os riscos com um eventual vazamento. A GDPR se refere a dados sensíveis como aqueles que necessitam de proteção especial por sua natureza ou pela relação que possuem com os direitos e liberdades fundamentais dos indivíduos. A regulamentação europeia, que serviu de base para a brasileira LGPD, considera dados sensíveis aqueles referentes à origem étnica ou racial, opinião política, credos filosóficos ou religiosos, filiações a grupos, dados genéticos, dados biométricos com a finalidade de identificar indivíduos e dados relativos à saúde, vida sexual ou orientação sexual. Em especial, este trabalho explora dados relativos à saúde.

Essa regulamentação proíbe o processamento de dados sensíveis, exceto se a parte envolvida tenha dado o seu consentimento explícito, no âmbito de atividades legítimas desempenhadas por associações ou fundações cujo objetivo é permitir o exercício de liberdades fundamentais, houver interesse público com base na legislação atual de todos os países da União Europeia, por exemplo, no ambiente de trabalho, proteção social, pensões, saúde e outras ameaças graves à saúde. Este trabalho considera o compartilhamento de dados com o consentimento explícito de seus donos.

2.1.2 Lei Geral de Proteção de Dados

A Lei 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), é a versão brasileira da GDPR. A LGPD foi sancionada por Michel Temer em agosto de 2018 e entrará

em vigor em agosto de 2020. Ela se aplica a qualquer atividade que envolva utilização de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Seus principais objetivos estão expostos na Figura 2.1. A Lei também se aplica extraterritorialmente se: a operação de tratamento dos dados seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional (LBCA, 2020).

Figura 2.1: Principais objetivos da LGPD (LBCA, 2020)

Os titulares dos dados tem por direito, assegurados pelo artigo 18, em relação aos seus dados pessoais: confirmação da existência de tratamento; acesso; correção; anonimização, bloqueio ou eliminação; portabilidade; obtenção de informações sobre o compartilhamento; a revogação do consentimento (LBCA, 2020). Essa lei deve afetar o desenvolvimento de novas pesquisas e aplicações na IoT, uma vez que elas geram uma grande quantidade de dados coletados a partir de sensores, que podem estar relacionados à atividades ou comportamentos humanos. A aplicabilidade dessas restrições da nova lei dependerá da fiscalização e dos entendimentos posteriores definidos pelos tribunais.

2.2 REDES DE COMPUTADORES

As redes de computadores surgiram da necessidade de conexão entre múltiplas máquinas computacionais. Os primeiros computadores caracterizavam-se por serem máquinas isoladas que resolviam determinados problemas por completo. A longo do tempo, com a necessidade de resolver problemas cada vez mais complexos e a implantação de diversos computadores, as redes foram criadas para viabilizar a comunicação entre esses dispositivos. Primeiramente, por meio de cabos ligando locais espacialmente longínquos, e depois com o desenvolvimento de redes sem fio para comunicação de computadores em redes locais. Atualmente, existem tecnologias de redes sem fio capazes de cobrir grandes áreas, como o 4G e o 5G. Esta subseção descreve as principais classificações para redes sem fio na Subseção 2.2.1 e um breve histórico da rede que interliga os computadores ao redor do planeta, a Internet, na Subseção 2.2.2.

2.2.1 Redes sem fio

Esta subseção apresenta os conceitos associados com a construção de redes sem fio estruturadas e não estruturadas. Em seguida, apresenta os enlaces de difusão e ponto-a-ponto. Além disso, descreve serviços orientados à conexões e não orientado à conexões. Após isso, exibe de maneira breve o modelo de referência TCP/IP, para então discorrer sobre o protocolo utilizado nesse trabalho, o 802.11.

2.2.1.1 Redes sem fio estruturadas e ocasionais

As redes sem fio estruturadas, dependem de uma estação-base ou roteador sem fio, também conhecida como ponto de acesso (do inglês, *Access Point* - AP), representadas na Figura 2.2. Os APs se conectam à rede com fios, e por sua vez então distribuem as mensagens para os receptores. A comunicação entre dois dispositivos é sempre por meio do AP, mesmo que estejam próximos o suficiente para estabelecer uma conexão direta (Tanenbaum et al., 2011). A telefonia móvel utiliza esse modelo estruturado, com tecnologias como 4G e o 5G. Segundo o trabalho (Schulz et al., 2017), as redes 5G diminuirão a latência na conexão, além de aumentar a conectividade entre os dispositivos. Com isso, essa nova tecnologia criará um ambiente favorável ao desenvolvimento de mais aplicações da IoT.

Figura 2.2: Rede sem fio estruturada

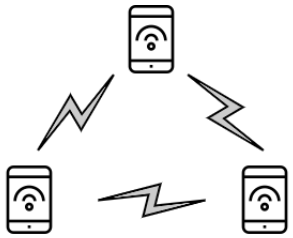


Figura 2.3: Rede sem fio ad hoc

As redes ocasionais ou ad hoc permitem que os dispositivos troquem informações diretamente entre si, conforme representado na Figura 2.3. Nessa classificação destacam-se algumas redes específicas como as redes ad hoc móveis (do inglês, *Mobile Ad hoc NETworks* - MANETs), redes ad hoc veiculares (do inglês, *Vehicular Ad hoc NETworks* - VANETS), entre outras. Esse modelo não depende de uma infraestrutura fixa, mas dos próprios dispositivos computacionais que formam a rede. Topologia se refere à maneira como os dispositivos estão associados em uma rede. A topologia das redes ad hoc muda com frequência e de forma imprevisível, consequência da sua característica de mobilidade dos dispositivos (Tanenbaum et al., 2011). Tecnologias de comunicação como *Bluetooth*, *Zigbee* e *Wi-Fi* são utilizadas para estabelecer redes ad hoc. Entre as vantagens das redes ad hoc sobre as redes estruturadas destacam-se a rápida instalação, pois não dependem de infraestrutura fixa, podendo ser estabelecidas dinamicamente; a tolerância a falhas, visto que sua característica adaptativa permite reestabelecer conexões utilizando uma nova rota; a conectividade, sendo que dois nós móveis podem se comunicar diretamente se estiverem dentro da área de alcance um do outro; a capacidade de movimentação dos dispositivos na rede. Contudo, é possível ressaltar algumas desvantagens do modelo ad hoc em relação ao modelo estruturado, tais como o desafio de criar bons algoritmos de roteamento devido às características de mobilidade dos dispositivos e dinamismo da topologia; a falta de informações acerca da localização geográfica de um dispositivo, sendo possível apenas utilizar o endereço da máquina; uma taxa de erros mais elevada em comparação com as redes

estruturadas; um tráfego de dados menor, uma vez que os cabos permitem um tráfego de dados por segundo maior do que as redes sem fio.

2.2.1.2 Enlaces de difusão e ponto a ponto

Segundo (Tanenbaum et al., 2011), os dispositivos computacionais em uma rede podem transmitir e disseminar dados com enlaces de difusão e ponto-a-ponto. As redes de difusão (do inglês, *broadcast*) têm apenas um canal de comunicação, que é compartilhado por todas as máquinas, conforme representado na Figura 2.4. Todos os dispositivos no alcance do meio físico de difusão podem recuperar um pacote enviado por qualquer máquina da rede. Porém, o pacote pode estar destinado a alguma máquina específica e, nesse caso, contém o endereço do destinatário e é ignorado por outras máquinas. Outro tipo de transmissão, chamada de *multicasting*, acontece quando um pacote é enviado a um subconjunto de dispositivos na rede. Por fim, a transmissão dirigida a todas as máquinas da rede é denominada *broadcasting*. A transmissão de estações de rádio é um exemplo comum de enlace de difusão.

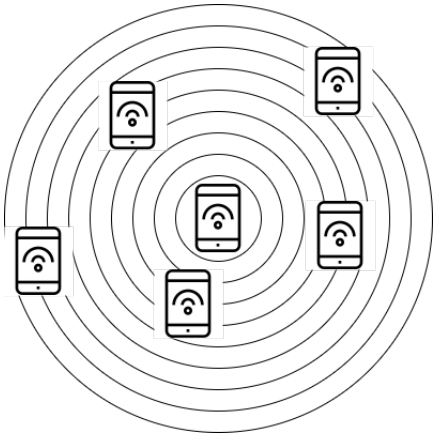


Figura 2.4: Enlace de difusão

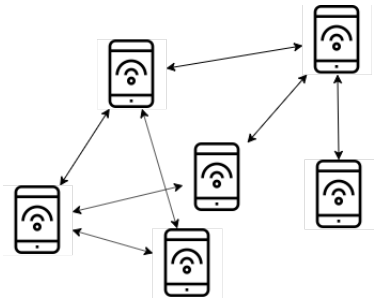


Figura 2.5: Enlace ponto-a-ponto

De acordo com (Tanenbaum et al., 2011), os enlaces ponto-a-ponto (do inglês, *unicast*) conectam pares de dispositivos individuais. Os pacotes são enviados de uma máquina para outra e podem passar por máquinas intermediárias, como representado na Figura 2.5. Encontrar boas rotas de tráfego na rede entre dois dispositivos é importante para enlaces ponto-a-ponto, uma vez que pode existir mais de uma rota disponível. Um exemplo dessa categoria de enlace é o *torrent*, que é uma maneira de pessoas compartilharem arquivos sem a necessidade de um servidor central. Os arquivos são transmitidos diretamente entre as máquinas por partes, até que esteja completo (Choffnes e Bustamante, 2008).

2.2.1.3 Serviços orientados e não orientados a conexões

Segundo (Tanenbaum et al., 2011), os dispositivos podem se comunicar por meio de serviço orientado e não orientado a conexões. A primeira classificação se refere a uma conexão constante entre dois dispositivos, em que os dados trafegam de forma sequencial entre um dispositivo e outro. Na maioria dos casos, a ordem de envio é preservada com a ordem de chegada dos dados. Uma chamada telefônica é um exemplo de serviço orientado a conexões. Ao contrário, o serviço não orientado a conexões se baseia no envio de uma mensagem por pacotes independentes que podem ser transmitidos por mais de uma rota. Os pacotes podem chegar ao destino fora de ordem e devem ser reordenados de maneira correta para formar a mensagem

original. O serviço orientado a conexões tem a vantagem de garantir que a mensagem chegue ao destinatário. Por sua vez, o serviço não orientado a conexões não introduz atrasos com o processo de confirmação do recebimento das mensagens. Este trabalho utiliza serviço não orientado a conexões, devido ao contexto de mobilidade dos dispositivos e sua maior responsividade. O estabelecimento de uma conexão entre cada par de dispositivos poderia sobrecarregar o processo de troca de mensagens.

2.2.1.4 Modelo de referência TCP/IP

As redes são organizadas em camadas ou níveis para reduzir sua complexidade (Tanenbaum et al., 2011). As camadas estão dispostas de maneira hierárquica, de modo que cada camada é responsável por uma função específica. Uma camada se comunica com outra camada de nível superior ou inferior por meio de interfaces. A comunicação entre camadas de mesmo nível ocorre por meio de protocolos. A Internet utiliza o modelo de referência TCP/IP para descrever suas camadas e protocolos, e por esse motivo esse modelo se tornou popular e bem aceito na prática, apesar do modelo de referência OSI ser mais detalhado.

O TCP/IP apresenta cinco camadas, como ilustrado na Figura 2.6, sendo a primeira delas a camada Física, que trata da transmissão de dados por um canal de comunicação. Logo acima, a camada de Enlace cumpre os requisitos de interconexão de uma rede de comutação de pacotes com serviço não orientado a conexões. A camada de rede, também chamada de camada internet, permite que dispositivos computacionais injetem pacotes em qualquer rede e garante que eles trafeguem independentemente até o destino. Essa camada define um formato de pacote oficial e um protocolo chamado IP (do inglês, *Internet Protocol*), mais um protocolo acompanhante chamado ICMP (do inglês, *Internet Control Message Protocol*). O roteamento de pacotes e a gestão de congestionamento são questões de grande importância para essa camada (Tanenbaum et al., 2011). A seguir, a camada de transporte tem a finalidade de permitir que entidades pares dos dispositivos de origem e de destino mantenham uma conversação. Dois protocolos se destacam nessa camada, com o primeiro deles sendo o protocolo de controle de transmissão (do inglês, *Transmission Control Protocol* - TCP), que é um protocolo orientado a conexões confiável que garante uma entrega sem erros de uma mensagem. O segundo é o protocolo de datagrama do usuário (do inglês, *User Datagram Protocol* - UDP), que é um protocolo não orientado a conexões, não confiável, que não tem a garantia do TCP, mas pode oferecer um controle próprio e customizado. Por último, a camada de aplicação contém os protocolos de mais alto nível, tais como protocolo de terminal virtual (TELNET), protocolo de transferência de arquivos (do inglês, *File Transfer Protocol* - FTP), protocolo de correio eletrônico (do inglês, *Simple Mail Transfer Protocol* - SMTP), o protocolo que mapeia os nomes dos dispositivos aos seus respectivos endereços da camada de rede (do inglês, *Domain Name Service* - DNS), o protocolo usado para buscar páginas na World Wide Web (do inglês, *HyperText Transfer Protocol* - HTTP) e o protocolo para entrega de mídia em tempo real (do inglês, *Real-time Transport Protocol* - RTP). Em especial este trabalho utiliza o UDP para customizar o controle do envio de pacotes entre os dispositivos.

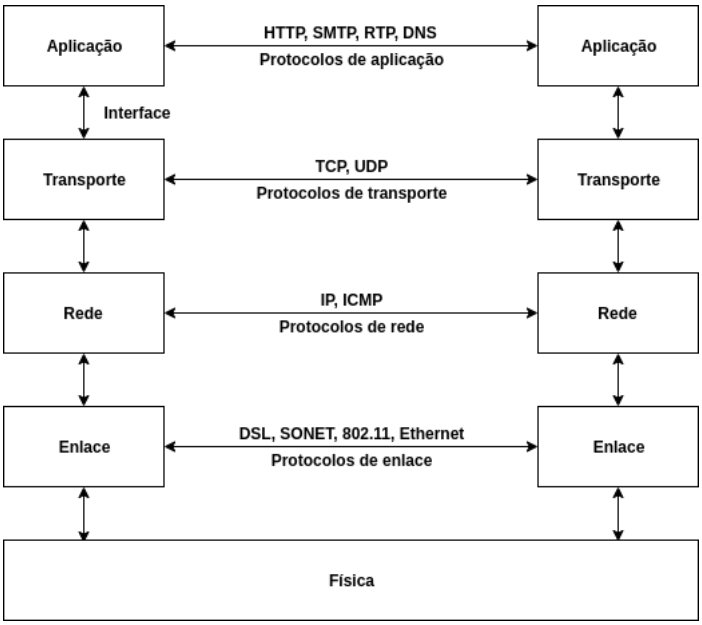


Figura 2.6: Modelo de referência TCP/IP

2.2.1.5 Redes locais sem fio

Com base em (Tanenbaum et al., 2011), as redes locais sem fio são muito populares atualmente pelo motivo de simplificar a conexão de dispositivos, que é mais trabalhosa com a utilização de cabos. Quando essas redes surgiram, cada empresa implementou a comunicação de uma maneira, o que levou a falta de compatibilidade entre dispositivos e APs. Por esse motivo surgiu o padrão IEEE 802.11, popularmente conhecido como Wi-Fi. De acordo com (Perahia e Stacey, 2013), esse padrão trabalha com velocidades entre 1,2 Mbps (megabits por segundo, onde 1 Mbps é 10^6 bits/s) no início até a 1 Gbps (gigabits por segundo, que é igual a 10^9 bits/s) com a versão mais recente, denominada de 802.11ac. As faixas de frequência em que atua são 2,4 GHz (gigahertz, que equivale a 10^9 hertz) e 5 GHz. A relação de cada versão do padrão 802.11 com sua taxa de dados e faixa de frequência está na Tabela 2.1 com informações extraídas do trabalho (Perahia e Stacey, 2013).

	802.11	**802.11b**	**802.11a**	**802.11g**	**802.11n**	**802.11ac**
Taxa de Dados	1 e 2 Mbps	5,5 e 11 Mbps	6-54 Mbps	1-54 Mbps	6,5-600 Mbps	6,5-6933,3 Mbps
Faixa de Frequência	2,4 GHz	2,4 GHz	5 GHz	2,4GHz	2,4 GHz e 5 GHz	5 GHz

Tabela 2.1: Informações técnicas sobre as versões do 802.11

Esse padrão é utilizado na maioria das vezes em conjunto com um AP, isto é, no contexto de redes estruturadas. Porém, ele também pode ser utilizado para redes ad hoc, conectando diretamente um dispositivo ao outro. É neste último contexto que a proposta deste trabalho utiliza o padrão 802.11n, que é uma versão otimizada em relação às anteriores e bastante comum aos *smartphones*. A proposta utilizou essa versão com a faixa de frequência de 2.4 GHz, por ser mais popular e compatível com dispositivos mais antigos. Essa versão também utiliza um esquema de modulação chamado multiplexação ortogonal por divisão de frequência (do inglês *Orthogonal Frequency Division Multiplexing* - OFDM), que divide uma banda larga do espectro em várias fatias estreitas, sobre as quais diferentes dados são enviados em paralelo.

Visto que o 802.11 utiliza ondas de rádio, é necessário lidar com problemas de interferência durante múltiplas transmissões. Esse padrão utiliza um esquema de acesso múltiplo

com detecção de portador (do inglês *Carrier Sense Multiple Access* - CSMA), onde os dispositivos computacionais esperam por um intervalo aleatório antes de transmitir, e adiam suas transmissões caso detectem outro dispositivo transmitindo dados. Esse esquema diminui a probabilidade de dispositivos transmitirem ao mesmo tempo, reduzindo a interferência entre eles. Contudo, quando um dispositivo não está no raio de alcance do outro, a detecção entre eles torna-se impossível. Apesar disso, o CSMA funciona muito bem na prática (Tanenbaum et al., 2011).

Finalmente, o problema de segurança aparece, uma vez que por meio da radiodifusão outros dispositivos além do destinatário podem interceptar os pacotes enviados. Para evitar isso, o padrão 802.11 incluiu um esquema de encriptação conhecido como WEP (do inglês, *Wired Equivalent Privacy*). Entretanto, esse esquema de segurança tinha falhas e logo foi quebrado (Borisov et al., 2001). Após isso, ele foi substituído pelo WPA (do inglês, *Wi-Fi Protected Access*) e em seguida reforçado com a próxima geração WPA2, que incluiu o uso do AES (do inglês, *Advanced Encryption Standard*), um novo padrão para a segurança das informações, e o CCMP (do inglês, *Counter Cipher Mode Protocol*), um mecanismo de encriptação que protege os dados que passam pela rede.

2.2.2 A Internet

A Internet é formada por um grande conjunto de redes que utilizam protocolos comuns e fornecem serviços comuns. Ela foi planejada e controlada por uma entidade central no início, mas sua expansão ocorreu de forma descentralizada (Tanenbaum et al., 2011). A origem dessa rede ocorreu no contexto da Guerra Fria no final de 1969 com a ARPANET, devido à sua ligação com o ARPA (do inglês, *Advanced Research Projects Agency*), uma organização centralizada para pesquisa de defesa. O ARPANET surgiu para corrigir a falha do sistema de telefonia da época que dependia de centrais para comunicação entre as cidades, vulnerabilidade que poderia ser explorada em um eventual ataque. Com isso, a ideia era criar um sistema distribuído de comutação. As primeiras conexões foram entre quatro centros de pesquisa com grande atuação na ARPA nos Estados Unidos: a Universidade da Califórnia em Los Angeles (UCLA), a Universidade da Califórnia em Santa Bárbara (UCSB), Instituto de Pesquisa de Stanford (do inglês, *Stanford Research Institute* - SRI) e a Universidade de Utah (UTAH).

A expansão da ARPANET foi rápida, visto que em setembro de 1972 a rede já tinha 34 nós. Essa conexão possibilitou o compartilhamento de informações entre os pesquisadores, o que ajudou muito no desenvolvimento de pesquisas. Logo as empresas e outras instituições que não eram ligadas à ARPA se interessaram nessa tecnologia de comunicação e a NSFNET foi criada pela NSF (do inglês, *National Science Foundation*). Com seu sucesso e enorme expansão a NSF estimulou a criação da ANS (do inglês, *Advanced Networks and Services*), empresa sem fins lucrativos formada pelas empresas MERIT, MCI e IBM. Após isso, o governo deixou o negócio de redes ao contratar quatro operadoras para estabelecer pontos de acesso de rede, ou NAPs (do inglês, *Network Access Points*), garantindo com isso que todas as redes regionais pudessem se comunicar. As tecnologias relacionadas a redes se desenvolveram rapidamente, e logo a Europa e outros lugares do mundo criaram infraestruturas semelhantes. O uso da Internet explodiu com a ascensão dos computadores pessoais e o surgimento da *World Wide Web* (WWW), no início da década de 1990.

A Internet chegou às pessoas primeiramente com a DSL (do inglês, *Digital Subscriber Line*) que reutiliza a infraestrutura das linhas telefônicas. A velocidade e capacidade de transmissão de dados aumentou com a banda larga (do inglês, *broadband*), e com o uso de fibra óptica. Atualmente, existem equipamentos e infraestrutura necessária para suportar tráfegos gigabit para uma pequena parcela de usuários comerciais no mundo (Wakka, 2019).

2.3 COMPUTAÇÃO UBÍQUA

A computação ubíqua é a ideia de dispositivos computacionais tão pervasivos no cotidiano das pessoas que suas presenças deixam de ser notadas (Weiser, 1991). Nesta seção são apresentados paradigmas que evoluíram baseados nesse conceito de computação ubíqua, conforme representado na Figura 2.7.

Inicialmente temos a Intranet das Coisas, que são redes com troca de informações locais onde os objetos fornecem dados para serem consumidos pelos humanos, apresentada na Subseção 2.3.1. Em seguida, surgiu a Internet das Coisas, onde os objetos passam a ter um papel mais proativo, consumindo dados, tratada na Subseção 2.3.2. Por fim, com o surgimento da Internet das Coisas Social, consideram-se informações geradas com base em relações sociais, tema que é abordado na Subseção 2.3.3.

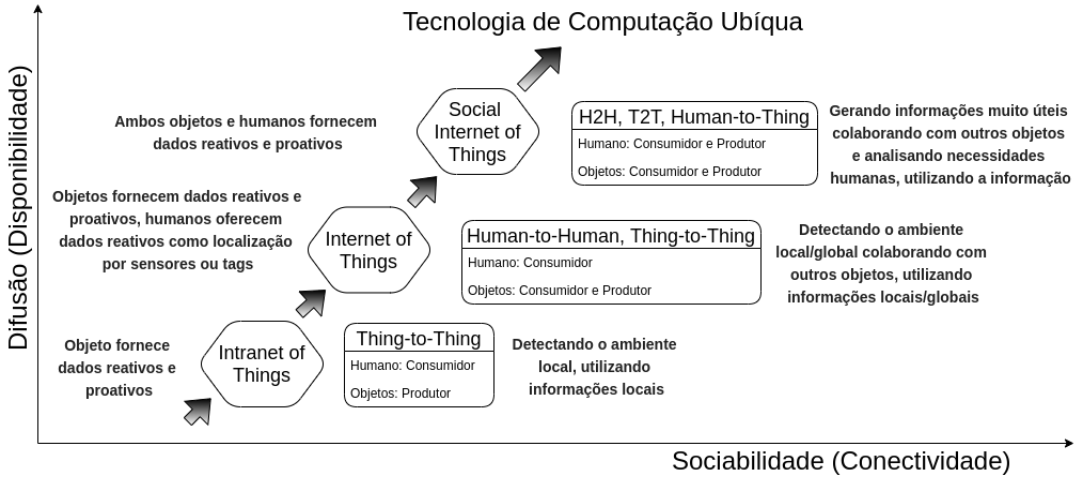


Figura 2.7: Evolução da computação ubíqua (Ortiz et al., 2014)

2.3.1 Intranet das Coisas

O termo *Intranet* das Coisas (do inglês, *Intranet of Things*) foi utilizado por (Zorzi et al., 2010) e (Ortiz et al., 2014) para definir uma rede local com um conjunto de objetos, tais como redes de sensores sem fio (do inglês, *Wireless Sensor Networks* - WSNs), comunicação de máquina para máquina (do inglês *machine-to-machine* - M2M), e casas inteligentes (do inglês *smart homes*). Nesse contexto, essas redes funcionam de maneira isolada e extraem apenas informações locais com conteúdos específicos acerca dos objetos.

2.3.2 Internet das Coisas (IoT)

Com o surgimento da Internet, as redes que antes eram isoladas encontram um meio para interagir. A IoT pode fornecer informações históricas, abrangentes e em larga escala por meio dessa colaboração entre as *Intranets* das Coisas, superando a heterogeneidade dos dispositivos, tecnologias de comunicação e objetivos de implantação. Além da possibilidade de integrar sistemas já existentes, a IoT favorece o surgimento de novas aplicações e serviços dedicados a diferentes propósitos, conforme abordado na Seção 1.1.

2.3.3 Internet das Coisas Social (SIoT)

A associação entre redes sociais (do inglês *Social Networks* - SNs) e IoT colaborou para o surgimento da SIoT, que tem o foco na relação entre humanos e objetos. A extração e análise de

aspectos sociais permite que objetos atuem de maneira autônoma para satisfazer as necessidades das pessoas. A combinação de relações sociais de indivíduos permite o estabelecimento de comunidades e avaliação de confiança entre dispositivos. Esses mecanismos ajudam tecnologias a alcançarem maior disponibilidade e conectividade, tornando os dispositivos computacionais mais pervasivos. Alguns conceitos utilizados no contexto da SIoT são explicados a seguir na Subseção 2.3.5, Subseção 2.3.4 e Subseção 2.3.6.

2.3.4 Redes oportunísticas

As redes oportunísticas são foco de estudo há algum tempo e são consideradas uma das evoluções das MANETs (Pelusi et al., 2006). Descobrir rotas entre o transmissor e o receptor de uma mensagem em ambientes com dispositivos esparsos e desconectados sempre foi um desafio. No contexto de redes oportunísticas, os dispositivos da rede não precisam estar conectados diretamente para trocarem informações. As mensagens podem trafegar por dispositivos intermediários a medida em que interagem entre si até chegarem ao destinatário. Além disso, os dispositivos não precisam conhecer a topologia da rede. Isso é importante pelo fato das rotas serem construídas dinamicamente de acordo com estabelecimento de interações oportunísticas entre os dispositivos. Vários conceitos de redes oportunísticas são originários de pesquisas em redes tolerantes a atrasos (do inglês *Delay-Tolerant Networks* - DTNs). As DTNs consideram situações com oportunidades ocasionais de comunicação entre os dispositivos, que podem ser regulares ou completamente randômicas. Os dispositivos recebem as mensagens e, se não houver conexão no momento, as guardam para disseminar a informação em um momento oportuno onde tenham conexão com outros dispositivos. As redes oportunísticas apresentam uma visão mais geral que inclui as DTNs.

No contexto de SIoT, o trabalho (Guo et al., 2012) definiu IoT oportunística como aquela que permite o compartilhamento e disseminação de informação em comunidades oportunísticas que são formadas com a mobilidade e contatos oportunísticos naturais das relações humanas. As redes oportunísticas de IoT podem ser formadas por diversos dispositivos equipados com transmissão a rádio e sensores, tais como *smartphones*, *wearables* e veículos. A Figura 2.8 apresenta a relação bi-direcional entre humanos, sociedades e a IoT oportunística. Por um lado, a IoT oportunística se torna o principal meio para detecção e monitoramento de comportamentos humanos. Por outro lado, a atuação e desempenho da IoT também são afetados pelos comportamentos humanos.

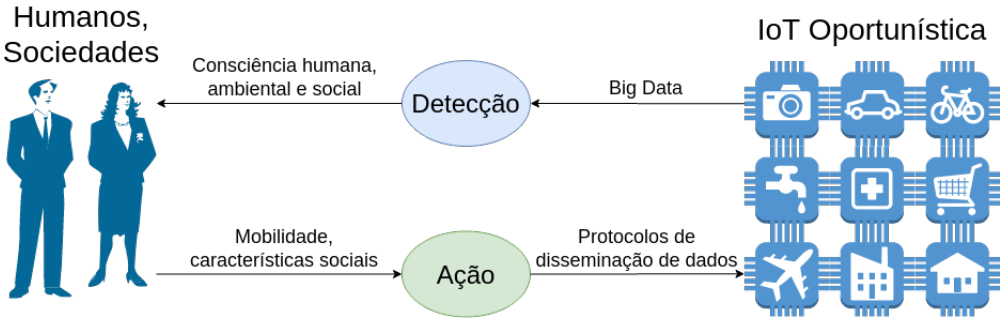


Figura 2.8: Efeitos da relação bi-direcional entre humanos, sociedades e IoT

2.3.5 Agrupamento de dispositivos

O agrupamento de dispositivos no contexto de redes dinâmicas é uma estratégia utilizada para capturar comportamentos complexos do mundo real (Rossetti e Cazabet, 2018). Vários

estudos sobre esse assunto mostraram que modelos de redes complexas de fenômenos reais têm duas características marcantes: são organizados em comunidades e sua estruturação envolve o tempo decorrido. Pesquisas para revelar as bases de redes complexas deram espaço para o surgimento do campo de descobrimento de comunidades (do inglês, *Community Discovery* - CD). Redes dinâmicas podem ser utilizadas para modelar a evolução de um sistema com a interação de seus dispositivos e estabelecimento de comunicações oportunísticas que impactam na formação das comunidades. Nesse contexto, surgiu a área de descobrimento de comunidades dinâmicas (do inglês, *Dynamic Community Discovery* - DCD). No qual, dispositivos podem estabelecer ou romper conexões com o passar do tempo, produzindo perturbações relevantes nas topologias de redes dinâmicas. Logo, esse comportamento também afeta a formação de comunidades, pois elas são altamente impactadas por mudanças locais. Diversos trabalhos abordaram redes que evoluem com o tempo: redes temporais (Holme e Saramäki, 2012), grafos com variação do tempo (Casteigts et al., 2012), redes interativas (Rossetti et al., 2015), conexões e grafos de fluxo contínuo (*stream*) (Latapy et al., 2018). O trabalho (Rossetti e Cazabet, 2018) faz algumas definições importantes para compreensão da formação de comunidades em redes complexas:

- **Redes temporais**: Uma rede temporal é um grafo $G = (V, E, T)$, em que V é um conjunto de tuplas da forma (v, t_s, t_e), onde v é um vértice do grafo e $t_s, t_e \in T$ respectivamente sendo os registros de nascimento e morte do vértice correspondente (com $t_s \leq t_e$); E é um conjunto de tuplas (u, v, t_s, t_e), com $u, v \in V$ sendo vértices do grafo e $t_s, t_e \in T$, respectivamente, o nascimento e morte da aresta correspondente (com $t_s \leq t_e$).

- **Captura instantânea da rede:** Uma captura instantânea G_τ é definida por um conjunto ordenado $G_1, G_2 ... G_t$, onde cada instantâneo $G_i = (V_i, E_i)$ é identificado univocamente pelos conjuntos de nós V_i e arestas E_i.

- **Ciclo de vida de uma comunidade:** Dada uma comunidade C, seu ciclo de vida (que identifica univocamente a história evolutiva completa de C) é composta pelo grafo acíclico direcionado (do inglês, *Directed Acyclic Graph* - DAG) de modo que (i) as raízes sejam eventos de nascimento de C e de seus possíveis predecessores se C tiver sido implicado em eventos de fusão; (ii) as folhas correspondem a eventos de morte de C e de seus sucessores, se C tiver sido implicado em eventos de divisão; e (iii) os nós centrais são as ações restantes de C, seus sucessores e predecessores. As arestas da árvore representam transições entre ações subsequentes na vida de C.

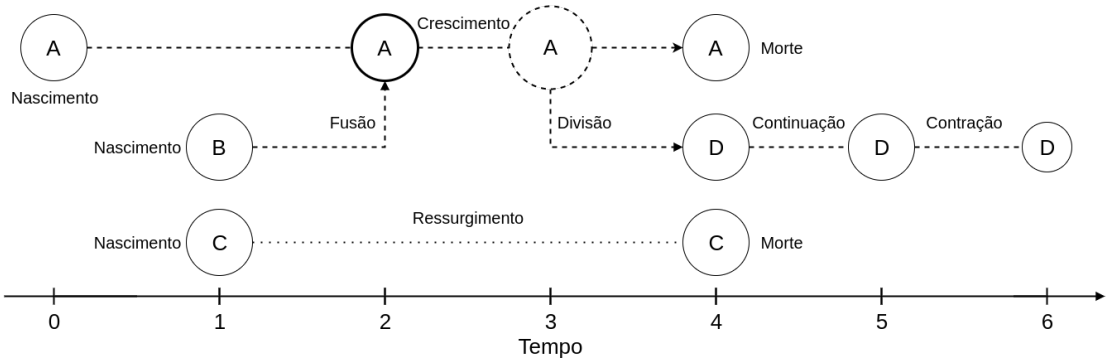


Figura 2.9: Ciclo de vida de uma comunidade (Rossetti e Cazabet, 2018)

A Figura 2.9 representa as operações possíveis em um ciclo de vida de uma comunidade e explicadas a seguir:

- **Nascimento**: primeira aparição de uma nova comunidade composta por um número qualquer de nós.
- **Morte**: desaparecimento de uma comunidade, onde todos os nós pertencentes a ela desaparecem.
- **Crescimento**: a entrada de novos nós aumenta o tamanho de uma comunidade.
- **Contração**: um ou mais nós deixam uma comunidade, reduzindo seu tamanho.
- **Fusão**: duas comunidades ou mais se fundem em uma única.
- **Divisão**: uma comunidade, como consequência do desaparecimento de um nó ou aresta, se divide em dois ou mais componentes.
- **Continuação**: uma comunidade permanece inalterada.
- **Ressurgimento**: uma comunidade desaparece por um período e depois volta sem perturbações, como se nunca tivesse deixado de existir. Esta situação pode ser vista como um falso evento de morte-nascimento envolvendo o mesmo nó durante um período de tempo defasado (por exemplo, comportamentos sazonais).

2.3.6 Gestão adaptativa de confiança

A confiança aparece como um fator importante para tomada de decisão e para manutenção de um relacionamento de longa duração baseado em cooperação e colaboração em vários trabalhos relacionados a IoT. A quantificação da confiança tornou-se mais complicada uma vez que é necessário derivá-la de redes complexas e compostas de várias camadas, tais como protocolos de comunicação, troca de informações, interações sociais e motivações cognitivas (Cho et al., 2015).

Além disso, diferentes domínios de aplicação requerem diferentes aspectos de confiança para tomada de decisão, tais como emocionais, lógicos e relacionais. Em geral, aplicações no contexto de IoT não trabalham com conhecimento total da situação da qual estão inseridas, mas sim com informações incertas, incompletas e conflitantes. Isso expõe o tomador de decisão a riscos de perdas por uma decisão equivocada baseada em uma confiança depositada de maneira incorreta em um indivíduo. O significado de confiança varia de acordo com o campo de estudo em questão. Por exemplo, a área da economia tem a visão de confiança como a expectativa de uma ação arriscada sob incerteza e ignorância com base nos incentivos calculados para a ação (Jr., 2002). Na área da sociologia, a confiança significa a probabilidade subjetiva de que a outra parte realizará uma ação que não prejudicará o interesse de quem está confiando, sob incerteza e ignorância (Gambetta, 1988). Ao condensar o significado de confiança para diversas áreas do conhecimento, (Cho et al., 2015) definiu:

Confiança é a disposição do avaliador de assumir riscos com base em uma avaliação subjetiva de que um avaliado exibirá um comportamento confiável para maximizar o interesse sob incerteza (por exemplo, ambiguidade devido a evidências conflitantes ou ignorância causada por completa falta de evidência) de uma dada situação com base nas avaliações cognitivas de experiências anteriores com o avaliado.

Os aspectos que afetam a definição da confiança, assim como suas classificações em atributos individuais e relacionais são mostrados na Figura 2.10. Os atributos individuais de confiança envolvem qualquer fator que pode ser derivado principalmente de características individuais. Eles ainda podem ser divididos em dois subgrupos: os lógicos, que indicam a confiança baseada em um raciocínio lógico sustentado por evidências e observações; e os emocionais, que tem base nos sentimentos e propensões de cada indivíduo. Os atributos relacionais emergem de relações com outros indivíduos. Esses tipos de atributos podem ser utilizados para compor um cálculo para quantificar a confiança entre duas pessoas.

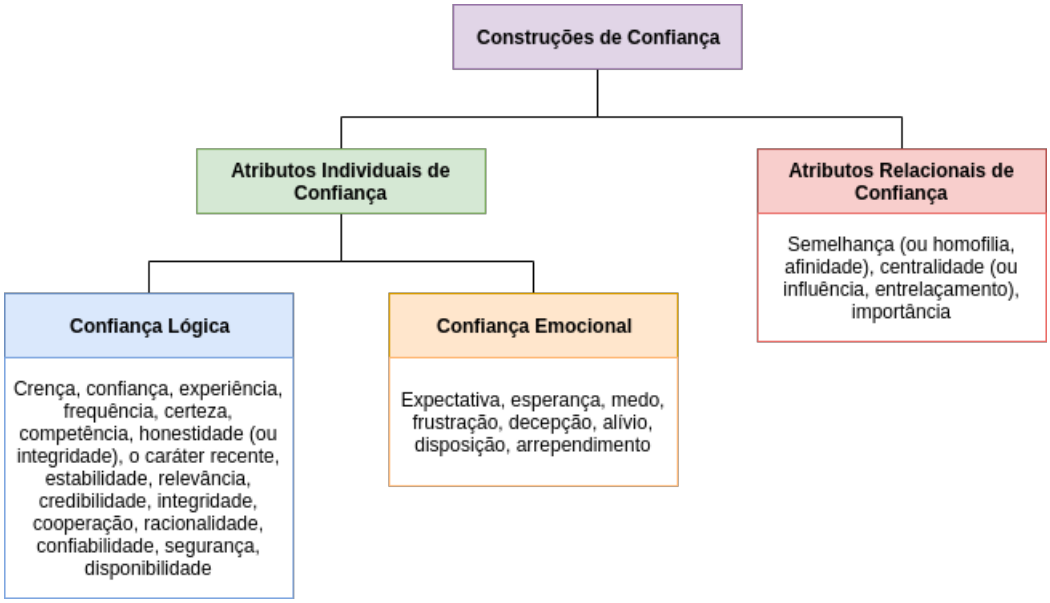


Figura 2.10: Classificação de fatores que afetam a confiança (Cho et al., 2015)

A confiança pode ser representada de maneira contínua, conforme mostra a Figura 2.11. Com isso, é possível estabelecer limites para decidir cooperar ou perdoar algum indivíduo, com base no valor da confiança. Desse modo, a confiança varia em um intervalo de [-1,+1], onde +1 representa o máximo de confiança e o -1 o máximo de desconfiança. O ponto 0 significa ignorância sobre a situação devido a falta de informações.

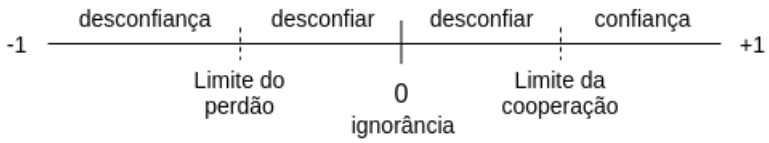


Figura 2.11: Confiança contínua

2.4 RESUMO

Este capítulo apresentou os conceitos teóricos que fundamentam este trabalho. Os dados pessoais sensíveis são informações que identificam características íntimas das pessoas. A Internet é uma rede mundial que surgiu nos Estados Unidos mas que se espalhou pelo mundo de maneira descentralizada. Na atualidade a Internet dispõe de tecnologias capazes de suportar as demandas do consumo moderno. As redes sem fio locais são a base para este trabalho, sendo classificadas em relação a sua infraestrutura em redes sem fio estruturadas ou ad hoc. Além disso, elas são classificadas em relação à sua transmissão em redes de difusão e ponto a ponto.

As redes sem fio provém serviços que são diferenciados pelo modo de conexão em serviços orientados e não orientados a conexões. Esta seção também apresentou o modelo de referência mais utilizado atualmente pela sua praticidade, o TCP/IP. Ademais, descreveu o padrão IEEE 802.11, popularmente conhecido como Wi-Fi. A evolução da computação ubíqua foi discutida com o início na Intranet das Coisas, ampliando-se para IoT após o surgimento e popularização da Internet, e chegando ao estágio atual da SIoT com a integração de redes sociais. As redes oportunísticas foram abordadas como aquelas que se formam com o contato oportunístico de dispositivos em uma rede. Além disso, o agrupamento de dispositivos foi apresentado como uma técnica utilizada para tentar capturar comportamentos complexos do mundo real. Por fim, a seção apresentou o cálculo da confiança como um importante fator para tomada de decisões em contextos com de aspectos sociais.

3 TRABALHOS RELACIONADOS

Este capítulo aborda os trabalhos relacionados considerados para a pesquisa e o desenvolvimento da solução proposta. A metodologia de pesquisa consistiu em reunir estudos no contexto da SIoT que abordassem questões de comunicação associadas a estrutura de redes, topologia, e gestão de confiança. A Seção 3.1 discute os trabalhos que consideram redes oportunísticas como uma característica para a definição da proposta. A Seção 3.2 detalha os trabalhos que utilizam técnicas de agrupamento de dispositivos para isolá-los e definir algum grau de similaridade entre eles. A Seção 3.6 descreve os trabalhos que empregam técnicas de gestão adaptativa de confiança para disseminar dados respeitando a privacidade dos indivíduos.

3.1 REDES OPORTUNÍSTICAS

O conceito de redes oportunísticas é uma ferramenta utilizada para lidar com o fator de mobilidade dos dispositivos. Entre os trabalhos estudados, destacam-se alguns com maior foco nas redes oportunísticas (Guo et al., 2012; Nuevo et al., 2015; Batista, 2019). Em especial, essa característica é comum na SIoT, uma vez que os nós representam as pessoas que podem se movimentar livremente. As redes oportunísticas tendem a utilizar sistemas distribuídos em virtude dessa característica de mobilidade e topologia dinâmica.

A pesquisa de (Guo et al., 2012) apontou para a evolução da IoT como uma rede dinâmica de interações oportunísticas centradas nos humanos e suas relações. Esse estudo propôs a IoT Oportunística (do inglês, *Opportunistic IoT*). A IoT centrada nos objetos foi um campo de vasto estudo nos últimos anos. Todavia, ao perceber o potencial da coleta e analise de dados de humanos, o lado social da IoT mostra-se uma área promissora. O trabalho estabelece definições importantes como consciência do usuário, do ambiente e social. Por meio disso, enfatiza a troca que ocorre entre as atividades humanas e os sensores. Entre os desafios, estão protocolos de disseminação de dados; redes sociais heterogêneas; segurança, privacidade e confiança; mecanismos de incentivo; e infraestrutura genérica. As informações expostas por esse trabalho sobre a interação entre a IoT e as pessoas de maneira oportunística inspirou este trabalho. Apesar de não implementar uma solução específica, essa visão e suas definições foram consideradas. Este estudo extrai elementos dessa visão e busca propor soluções para alguns desafios descrito pelos autores, entre eles: a implementação de uma rede oportunística, soluções para preservar a privacidade das pessoas utilizando confiança e a proposta de uma arquitetura genérica.

O trabalho ainda discute três aplicações para o contexto das redes oportunísticas. A primeira são redes sociais oportunísticas (do inglês *Opportunistic Social Networks* - OSNs). *Social Serendipity* é um dos primeiros estudos com OSNs, onde os interesses de indivíduos próximos que não se conhecem são comparados com a finalidade de sugerir contatos informais cara a cara (Eagle e Pentland, 2005). No *WhozThat* usuários em um espaço público podem trocar identificações de suas redes sociais para checar informações de perfil um do outro para encontrar alguém interessante (Beach et al., 2008). O ADESSO estabelece comunidades ad hoc para facilitar a comunicação e fornecimento de serviços de indivíduos próximos (Mokhtar et al., 2010). A segunda aplicação discutida são análises de comportamento em grupo. O projeto *SixthSense* da Microsoft utiliza RFID para inferir uma gama de inteligência empresarial, tais como a interação e associação entre pessoas e locais de trabalho (Ravindranath et al., 2008). Os dados coletados podem servir para, por exemplo, reservar uma sala de conferência automaticamente. A terceira aplicação explorada foi a publicidade oportunística. (Bottazzi et al., 2007) propôs uma solução

de publicidade viral entre clientes e seus parceiros em shoppings. Por fim, o FleaNet apresenta um serviço de mercado virtual que atua em veículos urbanos para facilitar a comunicação entre compradores e vendedores de produtos e encontrar interessados em produtos de maneira eficiente.

O trabalho (Nuevo et al., 2015) apresentou uma plataforma de IoT oportunística (OIoT), que ajuda desenvolvedores a criar e gerenciar comunidades de IoT oportunística entre dispositivos inteligentes. Essa proposta incluiu gerenciamento de perfis de usuário e dispositivos, gestão de redes oportunísticas IoT, publicação e subscrição de serviços e disseminação de dados oportunísticos. Esse trabalho apresentou uma aplicação chamada de *OpportunisticMeeting*, que foi projetada para ajudar estudantes e professores a estabelecer contatos oportunísticos com outros estudantes, baseado na comparação de *hobbies*, assuntos e preferências. Essa aplicação também permite a disseminação de perguntas, requisições e avisos, assim como respostas entre conhecidos ou outros alunos que nunca tenham estabelecido contato prévio.

A pesquisa de (Batista, 2019) atua sobre uma rede com alta mobilidade dos nós, onde pessoas portadoras dos seus dispositivos se movimentam pelas ruas de uma cidade. O protocolo de transmissão 802.11 também suporta a comunicação entre os nós, que acontece de maneira oportunística ao longo do tempo. Em virtude dessa característica de mobilidade, a topologia é dinâmica e distribuída, onde cada nó guarda sua própria informação sobre a sua vizinhança. Esse mecanismo descentralizado garante escalabilidade e robustez ao mecanismo, uma vez que uma arquitetura centralizada teria dificuldade em manter essas informações, causando uma sobrecarga de comunicações na rede, localizada em um ponto central.

3.2 AGRUPAMENTO DE DISPOSITIVOS

Os trabalhos relacionados (Bao et al., 2013; Chen et al., 2016; Batista, 2019) empregaram a técnica de agrupamento de dispositivos. Em geral, as propostas utilizaram esse método para isolar indivíduos com um certo grau de similaridade para produzir algum efeito nas interações dos dispositivos ou para reduzir a sobrecarga de comunicação. Nos três trabalhos analisados utilizou-se CoIs para agrupar os nós. As CoIs são opções viáveis para o contexto da SIoT, uma vez que os dispositivos representam características dos seus donos, e portanto seus interesses podem ser extraídos.

O trabalho (Bao et al., 2013) propõe um projeto e avaliação de um protocolo de gestão de confiança escalável, adaptativo e passível de sobrevivência. Utilizou-se o agrupamento de dispositivos em CoIs com as informações sociais dos donos dos dispositivos. Por meio desse agrupamento, a proposta considerou manifestações substancialmente distintas entre nós de um mesmo agrupamento em comparação com as interações entre nós de agrupamentos diferentes. Essas características foram determinantes para definição de uma configuração que maximizasse o desempenho do protocolo de comunicação. Dadas as relações dentro das CoIs e entre as CoIs, (Bao et al., 2013) identifica a melhor configuração para o protocolo de confiança a fim de atingir convergência, precisão, adaptabilidade e propriedades de resiliência na presença de condições adversas. Além disso, os agrupamentos são dinâmicos, onde nós podem participar ou deixar determinada CoI. Os resultados demonstraram que a confiança entre nós de um mesmo agrupamento converge mais rapidamente, o que já era esperado uma vez que suas interações ocorrem com maior frequência.

A pesquisa (Chen et al., 2016) também agrupa os nós em CoIs por meio das características sociais de seus proprietários. Essa abordagem possibilita a extração de um grau de interesses em comum ou de similaridade de capacidades entre dois dispositivos. Esses valores são computados pela razão entre as comunidades ou grupos de interesse em comum desses nós. Ademais, durante

a interação de nós de um mesmo agrupamento, os mesmos trocam informações sobre suas comunidades de interesse em comum, validando um ao outro.

O trabalho (Batista, 2019) também faz uso de CoIs para a formação de grupos de nós a fim de estabelecer uma relação de similaridade. Essa relação é utilizada para calcular a confiança entre dois dispositivos. No caso dessa proposta, a CoI tem um papel mais restritivo, uma vez que apenas aqueles nós que compartilham do interesse em saúde ão considerados para efetuar a disseminação dos dados.

3.3 GESTÃO ADAPTATIVA DE CONFIANÇA

No contexto da SIoT, vários trabalhos apresentaram propostas para uma gestão adaptativa da confiança (Guo et al., 2012; Bao et al., 2013; Chen et al., 2016; Truong et al., 2017; Al-Hamadi e Chen, 2017; Batista, 2019). O foco desses trabalhos é avaliação da confiança entre dois indivíduos utilizando aspectos sociais para uma tomada de decisão mais assertiva. A confiança pode ser computada a partir de diversos aspectos sociais e evolui ao longo do tempo, se adaptando às interações entre os dispositivos.

A pesquisa de (Guo et al., 2012) cita de maneira breve a confiança como um desafio chave para a realização das redes oportunísticas. Esse fator é considerado principalmente para uma disseminação de dados que respeite a privacidade das pessoas. A união entre as redes oportunísticas e as redes sociais humanas, segundo o trabalho, torna promissora a utilização de estruturas de redes sociais em modelos para representar a confiança entre dispositivos.

O trabalho (Bao et al., 2013) apresentou um protocolo de gestão de confiança para IoT de maneira distribuída. Cada nó armazena as informações de confiança em relação aos outros. Entretanto, as avaliações de confiança acontecem apenas após uma interação e se restringem a dispositivos de um mesmo agrupamento, de modo a evitar sobrecargas de armazenamento e comunicação. Além disso, ao trocarem informações, os dois nós em questão recomendam outros nós por meio de suas avaliações previamente coletadas de interações anteriores. As propriedades de confiança consideradas são honestidade, cooperatividade e CoIs. A computação do valor da confiança apresenta parâmetros configuráveis para definir o grau de importância de recomendações diretas e indiretas. A ideia central do protocolo proposto é que cada dispositivo calcule a confiança utilizando estimativa Bayesiana sobre as observações ao longo do tempo. O armazenamento dos valores de confiança em cada dispositivo considera a dinamicidade da rede. Como o número de nós é desconhecido, para evitar uma sobrecarga de armazenamento cada nó guarda um número limitado de valores de confiança. Após atingir um determinado limite, na ocorrência de uma nova interação o sistema remove valores de confiança abaixo da média para dar lugar à nova informação. Os resultados demonstraram que o mecanismo oferece uma boa performance no tempo de convergência da confiança e desempenho comparável a uma solução com armazenamento ilimitado.

A pesquisa (Chen et al., 2016) foi outra que propôs uma gestão adaptativa de confiança. Essa gestão se baseia em três componentes principais. O primeiro deles é a composição da confiança, responsável por selecionar as propriedades de confiança de acordo com os requisitos da aplicação IoT. Em seguida, destaca-se o componente de propagação e agregação de confiança, que foca em como disseminar e combinar as informações de confiança de modo a obter convergência e precisão. O último componente é o de formação, encarregado de gerar uma confiança geral e consolidada a fim de maximizar o desempenho da aplicação. Além disso, salienta-se a necessidade de uma gestão distribuída para um gerenciamento de entidades com livre arbítrio. O mecanismo considera as propriedades de honestidade, cooperatividade e CoI para compor o valor da confiança. O trabalho discute a aplicação do sistema para detecção de poluição do

ar em uma cidade inteligente, assim como um programa de assistência a viajantes por meio de um mapa aumentado. Os resultados obtidos de simulações nessas aplicações revelaram que é possível balancear entre velocidade de convergência e flutuação do valor da confiança. Além disso, outra conclusão foi de que o valor da confiança sempre convergirá ao máximo ao utilizar esse método adaptativo.

O trabalho de (Truong et al., 2017) parte da premissa de que um nó, ao avaliar outro por meio da confiança, é capaz de parcialmente reconhecer suas vulnerabilidades e riscos em potencial para executar uma determinada tarefa. Após uma ampla definição de conceitos sobre confiança, aplicações de trabalhos relacionados a avaliação de confiança são discutidos. Entre eles, destaca-se a construção de reputações voltadas ao comércio eletrônico, assim como focadas em sistemas distribuídos como WSNs, MANETs e redes ponto-a-ponto. Em resumo, (Truong et al., 2017) pontua que essas pesquisas consideram informações insuficientes, baseadas apenas em observações diretas e de terceiros. O trabalho propõem um modelo mais holístico da confiança, definida por dados sobre reputação, experiência e conhecimento (do inglês, *Reputation, Experience, Knowledge* - REK). A reputação representa a opinião pública acerca de determinado dispositivo e a experiência é um valor atribuído com base nas interações anteriores. Ambos os atributos são considerados traços sociais obtidos da acumulação de interações passadas entre as entidades ao longo do tempo. Por sua vez, o conhecimento mede os aprendizados daquele nó, e é uma confiança direta que reflete a perspectiva de um nó sobre outro em um determinado ambiente.

A pesquisa (Al-Hamadi e Chen, 2017) propõem um sistema para tomada de decisão baseada em confiança para o domínio de aplicação de cuidados de saúde. Os autores destacam que além do mecanismo considerar os valores de confiança dos provedores de serviço, ele também utiliza uma classificação de risco e probabilidade de perda de saúde dos pacientes. Como a aplicação envolve a saúde das pessoas, o sistema deve levar em conta o estado de saúde e a tolerância de perda de saúde de uma pessoa para tomada de decisão, uma vez que uma decisão incorreta pode gerar consequências trágicas. A proposta utiliza fatores de ambiente, como qualidade do ar, radiação magnética, barulho, entre outros. Ademais, estatísticas de saúde pessoal também são utilizadas, como temperatura corporal, pressão sanguínea, ritmo de respiração, entre outros. A arquitetura conta com três módulos. O primeiro deles é o especialista em saúde, responsável por manter os dados de limite e ser o ponto de interação com um profissional de saúde. O segundo é o gerenciamento de confiança, encarregado pelas avaliações de confiança e risco. O último deles é o da comunicação, que lida com as consultas e recebimento de dados.

O trabalho de (Batista, 2019) contribuiu com definições importantes de cálculo e gestão da confiança no contexto da SIoT voltada para cuidados de saúde. Entre elas, destaca-se uma equação para o cálculo de similaridade entre competências dos indivíduos. O cálculo da confiança entre dois dispositivos depende da competência, que é um aspecto social individual, e da similaridade, que é um atributo relacional. A similaridade entre dois nós é obtida por meio da razão entre os seus interesses em comum. Apenas indivíduos com interesse em saúde são considerados para o cálculo da confiança. Por sua vez, a competência é avaliada com relação a distância em uma taxonomia, onde o médico apresenta o maior valor. Além disso, cada nó armazena o valor da confiança em relação ao outro assim que a interação ocorre. Os valores são removidos com o passar do tempo para aqueles dispositivos que não interrompem sua interação. Dessa forma, não há sobrecarga de armazenamento, tornando o sistema escalável.

3.4 EVENTOS CONCORRENTES

blount2007, souil2011, geographic-information-science-2012, dar2015, wu2015

3.5 DISCUSSÃO

Os trabalhos que serviram de base para esta pesquisa estão na Tabela 3.1, ordenados por data e correlacionados a suas abrangências em relação aos assuntos de agrupamento de dispositivos (AD), redes oportunísticas (RO), avaliação de confiança (C) e eventos concorrentes (EC). Nenhum deles incluiu a incidência de eventos críticos concorrentes em suas construções. Com base nisso, a principal contribuição desta pesquisa reside na capacidade de gerenciamento de eventos críticos concorrentes.

Tabela 3.1: Trabalhos sobre agrupamento de dispositivos, redes oportunísticas, avaliação de confiança e eventos concorrentes.

TRABALHOS	**OBJETIVO**	**ABORDAGENS**			
		AD	**RO**	**C**	**EC**
Opportunistic IoT: Exploring the Social Side of the Internet of Things (Guo et al., 2012)	Explorar os aspectos sociais da IoT	–	social	desafio	–
Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems (Bao et al., 2013)	Considerar um ambiente social com CoIs para gestão dinâmica da confiança	CoIs	–	adaptativo	-
OIoT: A Platform to Manage Opportunistic IoT Communities (Nuevo et al., 2015)	Fornecer uma plataforma de disseminação de dados por meio de encontros oportunísticos	–	social	–	–
Trust-based Service Management for Social Internet of Things Systems (Chen et al., 2016)	Propor um protocolo de gestão de confiança adaptativa	CoIs	–	adaptativo	–
Toward a Trust Evaluation Mechanism in the Social Internet of Things (Truong et al., 2017)	Propor um mecanismo de avaliação holística da confiança	–	–	holístico	–
Trust-Based Decision Making for Health IoT Systems (Al-Hamadi e Chen, 2017)	Projetar e analisar um protocolo para tomada de decisão baseada em confiança para sistemas de saúde da IoT	–	–	avaliação de risco	–
Disseminação Robusta de Dados Pessoais Sensíveis Baseada em Comunidade de Interesse e Confiança Social para Suportar Situações Emergenciais de Saúde (Batista, 2019)	Propor um protocolo para disseminação de dados em emergências de saúde	CoIs	social	distribuído	–

3.6 RESUMO

Este capítulo discutiu os trabalhos existentes na literatura relacionados aos seus respectivos temas. A Seção 3.1 descreveu os trabalhos que abordaram uma rede oportunística para lidar com a mobilidade dos nós e a dinamicidade da topologia. A Seção 3.2 apresentou os trabalhos que empregaram técnicas de agrupamento de dispositivos. Todos os trabalhos discutidos empregaram CoIs para agrupar os dispositivos com base nos interesses de seus donos. A Seção 3.6 discutiu os trabalhos que utilizaram métodos de gestão adaptativa de confiança. Eles aproveitaram as características sociais disponíveis para construir valores de confiança ao longo do tempo.

4 COORDENAÇÃO DE EVENTOS CRÍTICOS CONCORRENTES

A proposta desse trabalho consiste em um sistema para coordenação de eventos críticos concorrentes para disseminação de dados pessoais sensíveis em redes dinâmicas. A visão geral do sistema, sua arquitetura e as tecnologias adotadas são apresentadas na Seção 4.1. A gestão de comunidades como meio para agrupar dispositivos é descrita na Subseção 4.1.1. Além disso, como esses dados não podem ser disseminados para qualquer pessoa, o sistema inclui um cálculo de confiança para determinar a melhor escolha baseada em alguns aspectos sociais, apresentada na Seção 4.2. Ademais, na ocorrência de um evento crítico é necessário que o sistema reaja de maneira ágil, correta e resiliente. Caso um indivíduo entre em uma situação emergencial, o mesmo deve ter a garantia de que encontrará o dispositivo mais confiável dentre aqueles de sua vizinhança para disseminar seus dados sensíveis ou de que não os disseminará para qualquer pessoa, conforme descrito na Seção 4.3. A Seção 4.4 discorre sobre o funcionamento do sistema deste trabalho. Por fim, a Seção 4.5 apresenta detalhes de implementação do sistema.

4.1 VISÃO GERAL

As redes sem fio ad hoc são utilizadas como ferramenta para estabelecer e manter a conexão entre os dispositivos. Para isso, na camada física o contato entre dispositivos ocorre por meio de ondas de radio e a tecnologia Wi-Fi. Além disso, na camada de enlace o sistema utiliza o padrão IEEE 802.11a, descrito na Subsubseção 2.2.1.5. O protocolo de rede utilizado foi o IPv4 devido à sua popularidade (Tanenbaum et al., 2011). O protocolo de transporte adotado foi o UDP por não introduzir uma sobrecarga nas comunicações entre os dispositivos que ocorreriam com o uso do TCP, e pela movimentação dos nós que provoca uma alteração frequente de suas vizinhanças. Por fim, o raio de alcance de cada dispositivo é de 100 metros para que ao mesmo tempo possibilitasse a interação entre eles, mas também mantivesse uma distância razoável para que uma pessoa consiga agir dentro de um intervalo de 24s.

O sistema considera um conjunto de dispositivos móveis (nós), interligados pela estrutura mencionada anteriormente. Esses nós são denotados por $D = \{d_1,\ d_2,\ d_3,\ ...,\ d_m\}$, onde $m \in \mathbb{N}$. Cada nó possui um identificador único (IP) e uma competência $S_n \in S$, em que $S = \{S_1,\ S_2,\ S_3,\ ...,\ S_p\}$, onde $p \in \mathbb{N}$ e S é o conjunto de todas as competências. Uma competência representa uma habilidade, perícia ou conhecimento para cumprir uma determinada tarefa, tal como médico, policial, músico, cozinheiro, engenheiro de *software*, entre outros. Ademais, um nó também possui um conjunto de interesses de tamanho variável, denotado por $I_n = \{i_1,\ i_2,\ i_3,\ ...,\ i_z\}$, tal que $z \in \mathbb{N}$, $|I_n| \neq 0$, $I_n \subset I$, onde I é o conjunto de todos os interesses. Os interesses são aspectos sociais referentes às atividades que são dignas da atenção de determinado indivíduo.

Cada nó forma uma rede ad hoc baseada nos seus vizinhos e os interesses são utilizados para formação de CoIs, conforme demonstrado na Figura 4.1. A união entre a base física, de rede e lógica do sistema está representada na Figura 4.2.

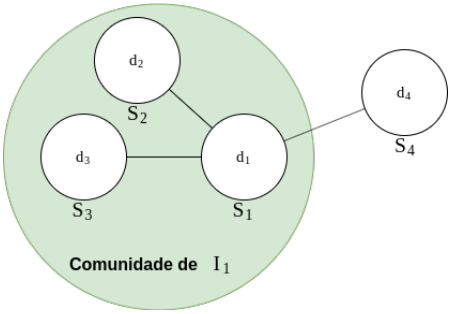


Figura 4.1: Exemplo de modelo da rede ad hoc estabelecida

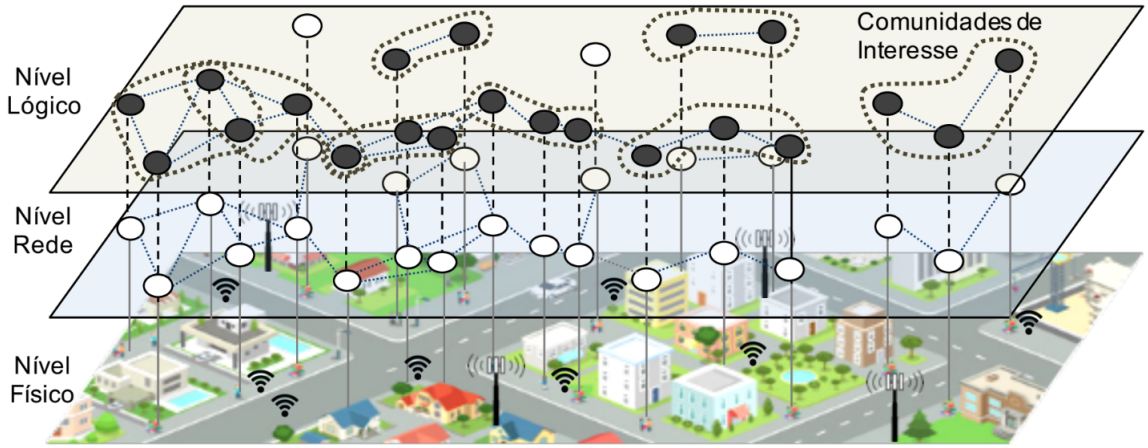


Figura 4.2: Camadas envolvidas no funcionamento do sistema (Batista, 2019)

A arquitetura do sistema envolve três componentes principais: Gestão de Recebimento de Mensagens, Gestão de Vizinhança e Gestão de Eventos Críticos. O módulo de Gestão da Vizinhança é responsável pelo envio da mensagem de anúncio a cada 4s para atualização da vizinhança do dispositivo. Todos os tipos de mensagens são recebidos e processados pelo módulo de Gestão de Recebimento de Mensagens. A mensagem de anúncio contém apenas o IP do emissor e é respondida por este módulo com uma mensagem de identificação, contendo sua competência e seu conjunto de interesses. Por sua vez, a mensagem de identificação é recebida e seu conteúdo é desmembrado para realização do cálculo da confiança. Com isso a vizinhança do dispositivo é atualizada com um novo vizinho ou, no caso de ser um vizinho já presente, continua como integrante ativo. Um dispositivo é removido da vizinhança se não responder o anúncio por mais de um ciclo, que ocorre a cada 4s. Na detecção de um evento critico, o módulo Gestão de Eventos Criticos envia uma mensagem de estado crítico sinalizando para ser removido da vizinhança de seus vizinhos. Se o dispositivo que entrou em estado crítico confirmou qualquer disseminação dentro dos últimos 24s, este módulo também é responsável pelo envio da interrupção de atendimento. Ademais, a disseminação de dados sensíveis para o nó melhor avaliado pelo cálculo da confiança também é tarefa deste módulo. Além disso, a mensagem contendo dados pessoais sensíveis de um nó em estado crítico é respondida com a mensagem de confirmação caso o nó receptor não esteja em estado crítico no instante do recebimento, ou ignorada caso o receptor já tenha sofrido um evento crítico. A partir da confirmação é iniciada a contagem de um intervalo de garantia de 24s. Se chegar ao final desse intervalo sem interrupções, a disseminação é considerada bem sucedida. Caso contrário, uma mensagem de interrupção é recebida e uma nova disseminação é realizada. Essa arquitetura está representada na Figura 4.3.

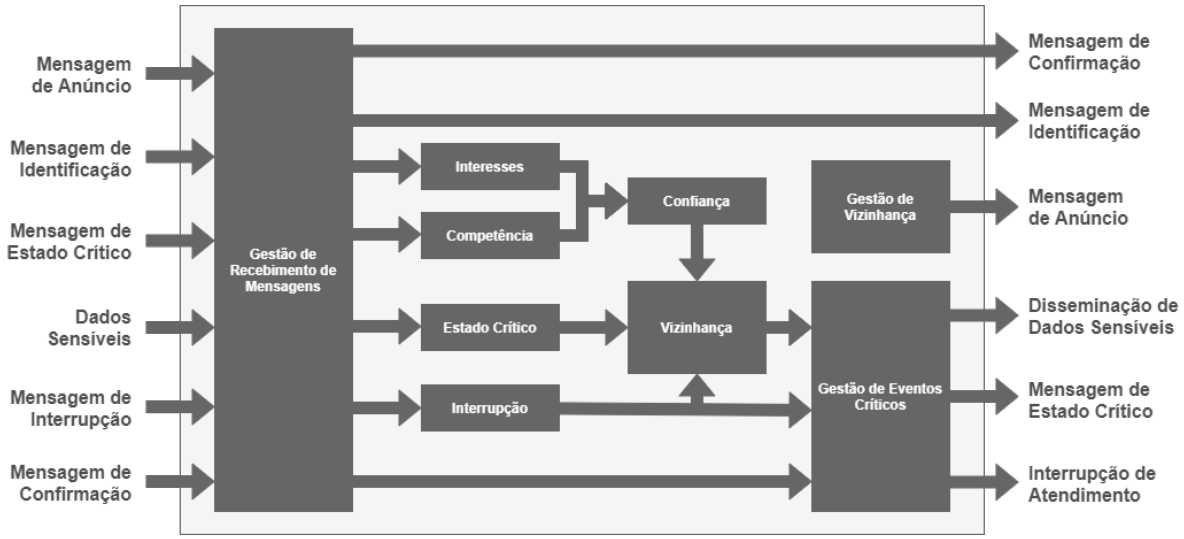


Figura 4.3: Arquitetura do sistema proposto

O impacto dos eventos críticos concorrentes na arquitetura reside no processo de interrupção de um atendimento. Esse processo ajuda a garantir que o procedimento seja concluído em face de eventos críticos que interfiram em um atendimento. Além disso, as constantes atualizações da vizinhança mantém os dispositivos conscientes sobre o estado de seus vizinhos.

4.1.1 Gestão de Comunidades

Toda pessoa possui alguns interesses em determinados assuntos, como por exemplo saúde, livros, música, filmes e viagens. Nesse contexto, é possível agrupar os dispositivos com as comunidades de interesse. Quando um indivíduo tem algum interesse em comum com outro é possível definir uma comunidade entre eles em torno deste interesse. Caso contrário, na ausência de interesses em comum não é possível agrupar os indivíduos, conforme representado na Figura 4.4. Esse agrupamento indica o nível de similaridade dos interesses entre duas entidades, baseadas na proposição de que quanto maior essa similaridade de uma entidade com outra, mais digna de confiança ela é (Truong et al., 2017).

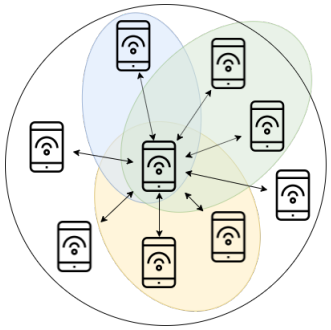


Figura 4.4: Comunidades de interesse entre dispositivos

4.2 CÁLCULO DA CONFIANÇA

O cálculo da confiança entre dois indivíduos define um valor para quantificar essa relação social. Os atributos, baseados em (Cho et al., 2015), considerados nesse cálculo são:

atributo relacional de confiança: o nível de similaridade entre o conjunto de interesses do receptor e do transmissor; e **atributo individual lógico de confiança:** a competência da pessoa que receberá os dados. Esses dois atributos são quantificados por meio de fórmulas que são explicadas a seguir. Com isso, chega-se a um valor de confiança entre um dispositivo i e outro dispositivo j, denotado por T_{ij}, onde i é um emissor da disseminação de seus dados sensíveis e j é um potencial receptor. Esse valor é uma média entre a relação entre os interesses dos dispositivos i e j, denotado por T_{ij}^{I}, e o peso da competência de j, denotado por T_{ij}^{Skill}. A fórmula, baseada em (Batista, 2019), está representada na Equação 4.1.

$$T_{ij} = \frac{T_{ij}^{I} + T_{ij}^{Skill}}{2} \tag{4.1}$$

O primeiro aspecto social abordado no cálculo é a similaridade entre os interesses de dois indivíduos. O nível de similaridade de interesses entre dois indivíduos é calculado pela intersecção dos seus dois conjuntos, conforme representado na Figura 4.5. Com isso, quanto mais interesses em comum, maior é o nível de similaridade. O cálculo, baseado em (Chen et al., 2016) e (Batista, 2019), utiliza como base o conjunto de interesses do avaliador i, onde I_i é o conjunto de interesses do indivíduo i e I_j é o conjunto de interesses do indivíduo j, e descrito na Equação 4.2.

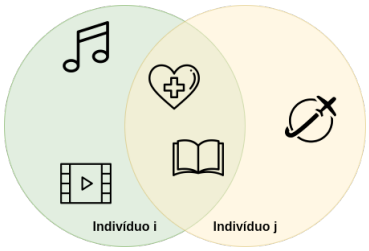


Figura 4.5: Relação de interesses sociais entre dois indivíduos

Os valores possíveis de serem assumidos por T_{ij}^{I} são $[0, 1]$. Considerando que o sistema atua em um domínio de aplicação específico, um interesse I_{ref} é direcionado para ser o interesse de referência. Com base na dissertação (Batista, 2019), este trabalho considera a Equação 4.3 para definir um valor da similaridade entre interesses de dois indivíduos. Com isso, quando o interesse I_{ref} não é um interesse em comum entre os dois indivíduos, o sistema atribui o valor 0. No caso de I_{ref} ser um interesse em comum, o valor é definido pela Equação 4.2. Se os conjuntos forem iguais, o sistema atribui o valor 1.

$$T_{ij}^{I} = \frac{|I_i \cap I_j|}{|I_i|} \tag{4.2}$$

$$T_{ij}^{I} = \begin{cases} 0, & \text{se} \quad I_{ref} \notin I_i \cap I_j \\ T_{ij}^{I} =]0,1[, & \text{se} \quad I_i \cap I_j \neq 0 \quad \text{e} \quad I_{ref} \in I_i \cap I_j \\ 1, & \text{se} \quad I_i = I_j \quad \text{e} \quad I_{ref} \in I_i \cap I_j \end{cases} \tag{4.3}$$

A competência da pessoa que receberá os dados é outro aspecto social utilizado para a quantificação da confiança. Trabalhos como (Truong et al., 2017) também se referem à competência como habilidade, expertise e credibilidade. Uma pessoa pode ser benevolente e íntegra, porém seus resultados podem ser insatisfatórios se ela não apresentar capacidade suficiente.

O sistema considera que cada indivíduo tem apenas uma competência, denotada por S_j, dentre um conjunto de competências, onde cada uma possui um peso diferente. Uma

competência de referência S_{ref}, mais adequada ao interesse I_{ref}, tem o maior peso, isto é, 1. Além disso, uma função, denotada por D_{Skill}, calcula a distância de uma competência qualquer S_j para a competência de referência S_{ref}. Essa função usa um cálculo sobre uma taxonomia de competências, explicado posteriormente, baseado nos trabalhos (Carminati et al., 2016) e (Mohammad e Hirst, 2012). Um conjunto de competências O contém aquelas que não têm nenhuma adequação ao interesse I_{ref}, e assim recebem o peso 0. O peso da competência de um indivíduo j, denotada como T_j^{Skill}, pode assumir valores entre $[0, 1]$, representada pela seguinte equação baseada na dissertação (Batista, 2019):

$$T_j^{Skill} = \begin{cases} 0, & \text{se} \quad S_j \in O \\ D_{Skill} =]0, 1[, & \text{se} \quad S_j \notin O \cup \{S_{ref}\} \\ 1, & \text{se} \quad S_j = S_{ref} \end{cases} \tag{4.4}$$

Uma taxonomia genérica é definida na Figura 4.6 no âmbito do cálculo da distância entre duas competências. Ela foi derivada de uma taxonomia dedicada a área da saúde do trabalho (Batista, 2019). Ela parte de uma raiz comum, nesse caso Pessoas, uma vez que estamos no contexto de SIoT. A raiz se estende para Áreas de Interesse e se aprofunda em Especialidades e Competências, que por sua vez podem ser estendidas àquelas cada vez mais específicas. A Competência S_{ref} é a referência para os cálculos de similaridade.

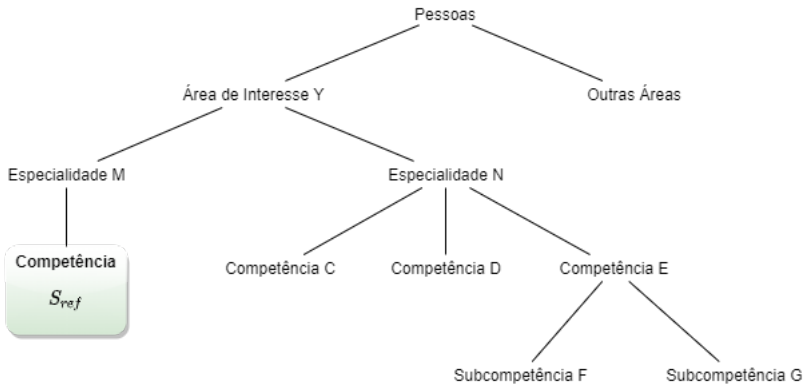


Figura 4.6: Taxonomia genérica de competências

O cálculo da distância entre uma competência qualquer S_j e uma competência de referência S_{ref} depende de três medidas, representadas na Figura 4.7 (Batista, 2019). A primeira delas, c_1, é o número de saltos partindo da $Raiz$ até S_{ref}. A segunda, c_2, é o número de saltos entre a $Raiz$ e o último nível em comum entre S_{ref} e S_j, denotado por L_{comum}. Finalmente, a terceira, c_3, quantifica o número de saltos da $Raiz$ até S_j. Com essas medidas é possível definir D_{Skill} com a Equação 4.5:

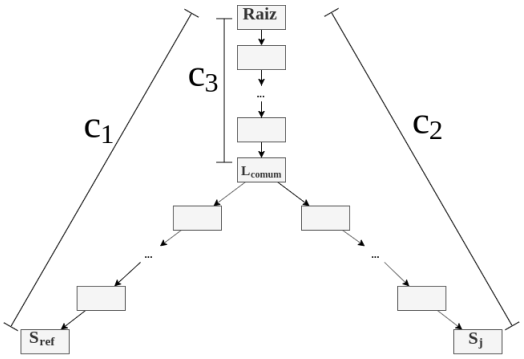


Figura 4.7: Propriedades do cálculo da similaridade entre competências

$$D_{Skill} = \frac{2 \times c_3}{c_1 + c_2} \tag{4.5}$$

Para avaliar a distância entre duas competências, supõe-se um cenário onde a competência de referência S_{ref} está a 3 saltos distante da $Raiz$, uma competência qualquer S_j a uma distância de 4 saltos da $Raiz$ e o L_{comum} distante da $Raiz$ por 1 salto. O valor encontrado é de 0,28 ao aplicar a Equação 4.5.

4.3 GESTÃO DE EVENTOS CRÍTICOS

O sistema proposto segue o ranqueamento previamente calculado para escolher o melhor destino para disseminação de seus dados sensíveis na ocorrência de um evento crítico. Essa resposta é ágil considerando a criticidade do evento e resiliente, pois caso ocorra algum problema com o atendimento daquela situação, o sistema busca outras alternativas de forma autônoma. Caso o dispositivo não encontre nenhum outro indivíduo que forme uma comunidade de interesse com base em I_{ref}, o sistema não dissemina os dados pessoais sensíveis da pessoa, visto que nenhuma relação de confiança pôde ser estabelecida.

A Gestão de Eventos Críticos só é acionada na ocorrência de um evento crítico relacionado ao dono do dispositivo. O evento crítico pode ser detectado por meio de sensores ou outros dispositivos. Quando isso acontece, o sistema dissemina os dados pessoais sensíveis e inicia a contagem de intervalo e tempo para que considere essa disseminação bem sucedida. O intervalo definido foi de 24s ou 6 ciclos do sistema, visto que cada ciclo corresponde a 4s. Esse tempo foi considerado suficiente para que outro indivíduo possa reagir ao receber os dados sensíveis de outro que se encontra em estado crítico. O sistema remove o receptor da disseminação da vizinhança caso ele ignore ou não tenha recebido a mensagem, escolhendo o próximo indivíduo no ranqueamento baseado no cálculo da confiança. Esse mecanismo pode se repetir até que o dispositivo não tenha mais vizinhos ou até que uma disseminação tenha sido bem sucedida. Nesses casos o sistema encerra suas atividades e desliga todos os módulos. Além disso, o dono de um dispositivo que já tenha confirmado uma disseminação pode entrar em estado crítico dentro do intervalo de garantia de 24s. Nesse caso, o sistema verifica que estava em atendimento e envia uma mensagem de interrupção, forçando o outro dispositivo a procurar um novo indivíduo para garantir uma disseminação de sucesso.

4.4 FUNCIONAMENTO

A proposta deste trabalho funciona com os três componentes, Gestão de Eventos Críticos, Gestão de Vizinhança e Gestão de Recebimento de Mensagens, que interagem entre si por meio da troca de mensagens por *broadcast* ou *unicast*. São 6 possíveis mensagens que distinguem-se pelo número da *Tag*, conforme apresentado na Tabela 4.1. O sistema de interação entre os componentes do dispositivo receptor com os do dispositivo transmissor está representado na Figura 4.8. Além disso, o sistema funciona com ciclos de 4s, onde a cada ciclo envia mensagens de anúncio e verifica o andamento de uma disseminação de dados sensíveis.

Número da *Tag*	Significado
0	Anúncio de busca por vizinhos
1	Mensagem de resposta com informações de competência e interesses
2	Mensagem de disseminação de dados pessoais relativos ao evento crítico
3	Mensagem de confirmação da disseminação
4	Anúncio de parada devido a um evento crítico
5	Mensagem de interrupção de atendimento

Tabela 4.1: Significado das mensagens trocadas entre dispositivos

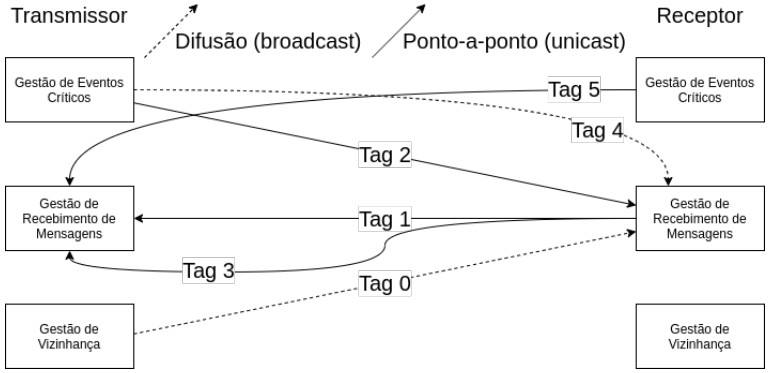


Figura 4.8: Interação entre os componentes

O sistema proposto neste trabalho apresenta quatro fluxos principais em relação ao seu funcionamento. O primeiro deles trata da exploração da vizinhança, representada na Figura 4.9, onde um dispositivo transmite um sinal *broadcast* a procura de vizinhos. Os receptores dessa mensagem enviam como resposta direta suas informações de interesses e competência. Com isso, o dispositivo transmissor pode atualizar sua vizinhança ao avaliar a relação de confiança com o receptor.

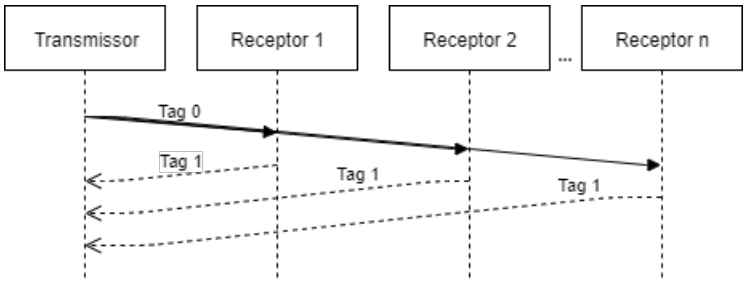


Figura 4.9: Fluxo da exploração da vizinhança

O segundo fluxo corresponde à confirmação de um evento crítico com sucesso na primeira tentativa, representado na Figura 4.10. Ao entrar em estado crítico, um dispositivo transmissor envia um sinal *broadcast* anunciando sua parada para que os vizinhos o removam de suas vizinhanças. Logo após, o transmissor escolhe o melhor dispositivo para disseminar seus dados, recebendo uma mensagem de confirmação em seguida.

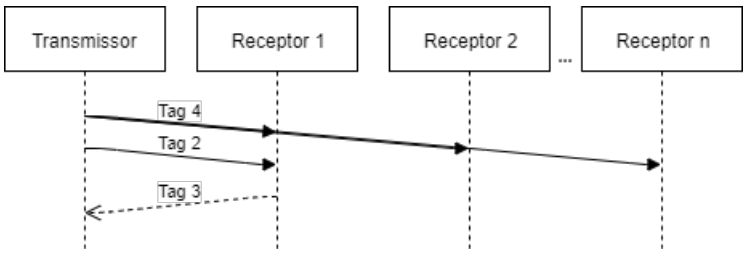


Figura 4.10: Fluxo de resposta ao evento crítico

O terceiro fluxo concerne a um evento crítico em que não obteve resposta na primeira disseminação de dados, mas que encontra um segundo receptor a partir de uma segunda disseminação, representado na Figura 4.11. O processo de evento crítico se repete ao do fluxo anterior, porém nessa situação o transmissor aguarda uma rodada, correspondente a 4 segundos, e verifica que não obteve resposta. Com isso, o receptor inicial é removido da vizinhança e o

próximo indivíduo do ranqueamento é escolhido para a nova disseminação de dados. Nesse caso o segundo receptor confirma o atendimento, mas o processo de busca por outro receptor pode se repetir em caso de não recebimento de resposta até que não haja mais vizinhos disponíveis ou até que receba uma confirmação.

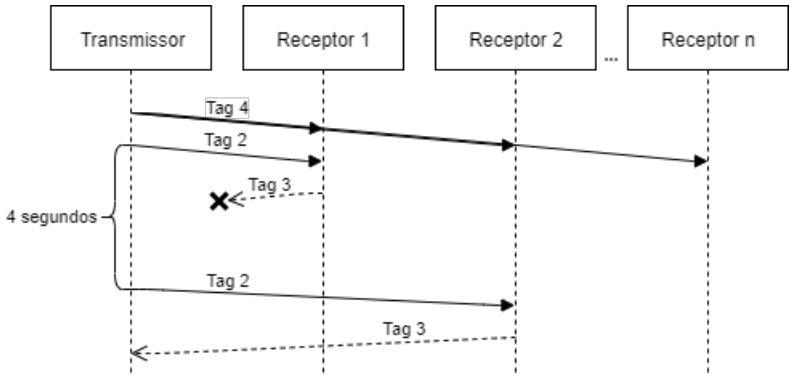


Figura 4.11: Fluxo de resposta ao evento crítico sem sucesso na primeira tentativa

Finalmente, o quarto fluxo refere-se a um atendimento que foi interrompido em virtude de um evento crítico sofrido pelo receptor no intervalo de 24 segundos, ou 6 rodadas. O processo de evento crítico se repete com uma confirmação do primeiro receptor para atendimento do transmissor da disseminação. Contudo, esse receptor entra em estado crítico após a confirmação do atendimento e precisa notificar o transmissor de que não pode completá-lo. A partir dessa interrupção, o transmissor retorna ao processo de busca por um novo receptor para disseminação de seus dados sensíveis, conforme representado na Figura 4.12.

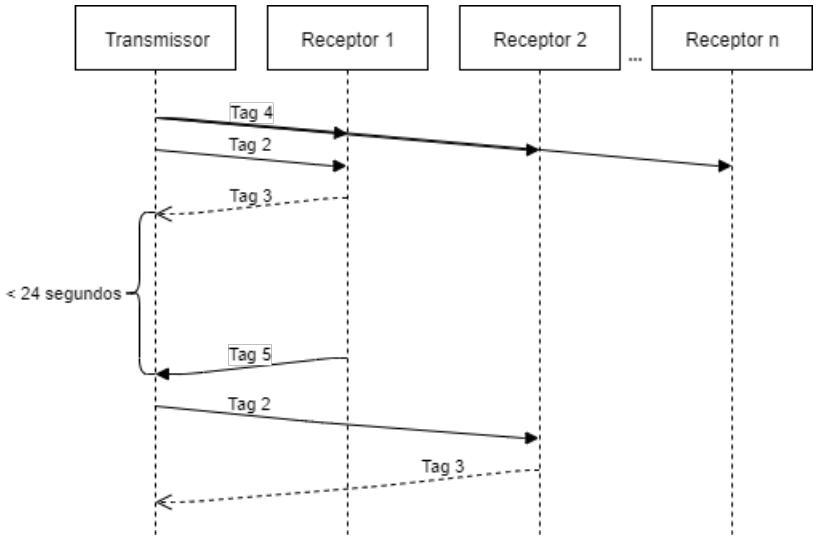


Figura 4.12: Fluxo de resposta ao evento crítico com interrupção de atendimento

4.5 IMPLEMENTAÇÃO

O sistema deste trabalho foi implementado com o simulador de redes *ns-3*, mais especificamente com sua versão 3.29. Essa ferramenta simula redes de eventos discretos para sistemas da Internet, direcionado para pesquisas e desenvolvimento acadêmico, além de ser um *software* livre, com a licença GNU GPLv2, disponível publicamente. As linguagens de

programação utilizadas foram o *C++* para os módulos do *ns-3*, o *Python* para extrair e processar dados gerados nas simulações, e o *R* para gerar gráficos a partir desses dados.

A Figura 4.13 representa a estrutura do código dentro do *ns-3*. Esse simulador possui diversos módulos que cumprem funções específicas e permite a criação de módulos customizados para atender às necessidades de seus usuários. Um módulo, denominado *stealth*, dedicado ao sistema deste trabalho, foi implementado e acoplado ao diretório *src*, onde se encontram todos os módulos padrão, como por exemplo o *core*. No módulo *stealth* encontram-se os componentes da proposta no diretório *models*, assim como uma unidade com métodos utilitários denominada *utils* dentro do diretório *helper*. Além disso, o arquivo *stealth_simulator* contém a inicialização e informações necessárias para execução da simulação e encontra-se no diretório *scratch* que é de onde as simulações são realizadas no *ns-3*.

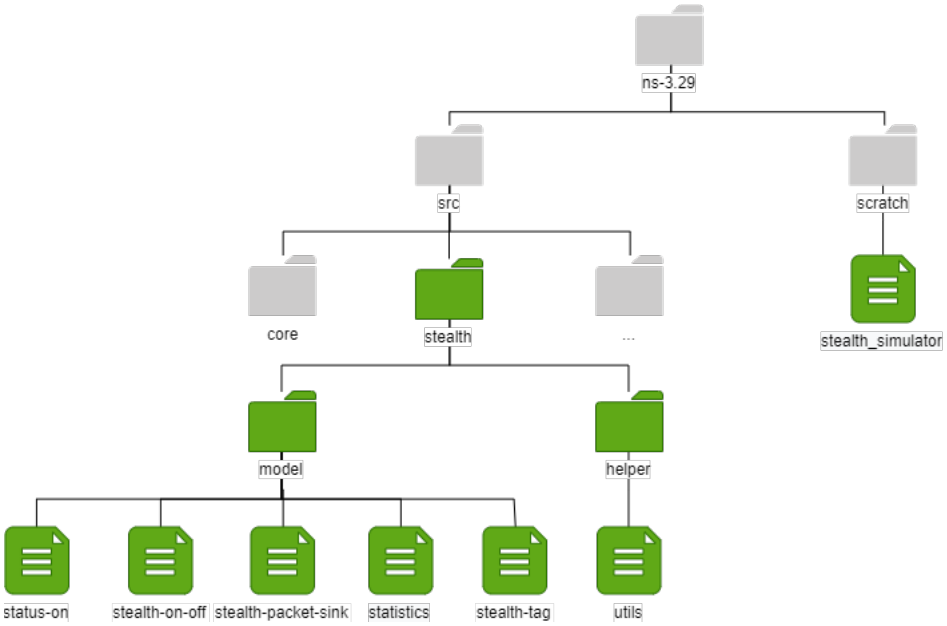


Figura 4.13: Estrutura do código no NS3

O arquivo *status-on* contém o componente Gestão de Eventos Críticos, que é dedicado a responder um evento crítico. Esse componente começa desligado e é inicializado quando o dispositivo de um indivíduo detecta um evento crítico, executando o Algoritmo 1. Essa execução ocorre apenas uma vez, onde o sistema indica o início de um evento crítico com o indicador *Status* (*l*.2) e anuncia sua parada imediata a todos os vizinhos com uma mensagem *broadcast* (*l*.3). Se a pessoa que entrou em estado crítico estiver atendendo outra, ela envia uma mensagem direta (*unicast*) para interromper esse atendimento (*l*.5-6). Caso o dispositivo não tenha nenhum vizinho, ele desliga todos os componentes e encerra suas atividades (*l*.8). Caso contrário, busca pelo melhor vizinho baseado no cálculo de confiança, explicado na Seção 4.2, e envia dados pessoais sensíveis de acordo com o nível da competência daquele que os receberá (*l*.10-13).

Algoritmo 1 Gerenciamento de inicialização de um evento crítico

```
1:  procedure StartApplication    // Executa apenas uma vez
2:      ThisNode.Status ← TRUE
3:      AnnounceStopping()
4:      if ThisNode.Attending = TRUE then
5:          SendUnicast(ThisNode.EmergencyNode, "Interrupting service", 5)
6:          ThisNode.Attending ← FALSE

7:      if ThisNode.IsThereAnyNeighbor() = FALSE then
8:          StopAllApplications()
9:      else
10:         bestNeighbor ← ThisNode.GetBestNeighbor()
11:         competence ← ThisNode.GetNeighborCompetence(bestNeighbor)
12:         criticalInfo ← ThisNode.GetCriticalInfo(competence)
13:         SendUnicast(bestNeighbor, criticalInfo, 2)
```

O sistema verifica o progresso do atendimento a cada quatro segundos ao executar o Algoritmo 2, após o componente Gestão de Eventos Críticos ser inicializado pelo Algoritmo 1. Com isso, se o serviço continua em andamento, isto é, não completou um intervalo mínimo de 24 segundos, o sistema continua normalmente (l.3). Caso o serviço complete 24 segundos, o dispositivo considera o que a disseminação do evento crítico foi um sucesso e encerra as atividades (l.5). Caso contrário, se o serviço foi interrompido nesse intervalo, o sistema repete a busca por um novo indivíduo e dissemina os dados relacionados ao evento crítico novamente (l.7-10).

Algoritmo 2 Gestão de atendimento a um evento crítico

```
1:  procedure SendPacket    // Executa a cada 4 segundos
2:      if ThisNode.Service = TRUE and ThisNode.ServiceTime < 24 then
3:          return

4:      if ThisNode.Service = TRUE and ThisNode.ServiceTime >= 24 then
5:          StopAllApplications()
6:      else
7:          bestNeighbor ← ThisNode.GetBestNeighbor()
8:          competence ← ThisNode.GetNeighborCompetence(bestNeighbor)
9:          criticalInfo ← ThisNode.GetCriticalInfo(competence)
10:         SendUnicast(bestNeighbor, criticalInfo, 2)
```

O arquivo *stealth-on-off* compreende o componente Gestão de Vizinhança, que é responsável pela manutenção da vizinhança dos dispositivos e da contagem de tempo do atendimento a um evento crítico. O Algoritmo 3 executa a cada 4 segundos, atualizando o tempo do serviço se determinado dispositivo está aguardando o intervalo mínimo de 24 segundos como atendente ou como paciente (l.3). Além disso, esse componente retira na vizinhança dispositivos que ficaram mais de uma rodada sem responder (l.4) e marca todos os dispositivos de sua vizinhança para que sejam atualizados nas próximas rodadas (l.5). Por fim, envia um sinal *broadcast* para todos os dispositivos em seu raio de alcance para que eles respondam com suas informações, com a finalidade de atualizar a vizinhança.

Algoritmo 3 Gestão da vizinhança

```
1: procedure SendPacket   // Executa a cada 4 segundos
2:     if ThisNode.Service = TRUE or ThisNode.Attending = TRUE then
3:         ThisNode.ServiceTime ← ThisNode.ServiceTime + 4

4:     ThisNode.UnregisterOffNeighbors()
5:     ThisNode.TurnOffLiveNeighbors()
6:     SendBroadcast("Hello", 0)
```

O arquivo *stealth-packet-sink* inclui o componente Gestão de Recebimento de Mensagens, que é voltado para responder ao recebimento de pacotes de outros dispositivos. Cada pacote recebido executa o Algoritmo 4, que por sua vez processa as informações recebidas. As respostas estão divididas em seis possibilidades, dependendo do pacote recebido. Se não estiver em estado crítico, o dispositivo responde com suas informações de competência e interesses ao enviar uma mensagem *unicast* ao dispositivo de origem do recebimento do *broadcast* para atualização de vizinhança (l.7), caso contrário ignora essa mensagem. Por sua vez, o dispositivo que recebe essas informações processa a competência e interesses recebidos. Se não houver nenhum interesse em comum, não executa nenhuma ação (l.12). Caso positivo, verifica se o dispositivo tem o interesse de referência e avalia a confiança entre os dois dispositivos (l.14). Com isso, se o dispositivo já existe na vizinhança, ele será marcado como disponível novamente (l.16), se não ele é inserido na vizinhança como um novo vizinho (l.18). No recebimento de uma mensagem de evento crítico, o dispositivo verifica se seu dono já está em estado de crítico. Se sim, ignora a mensagem e retira o emissor da vizinhança (l.26). Se não, atualiza seu estado para efetuar o atendimento (l.21), guarda o dispositivo que será atendido (l.22), inicia o tempo do serviço em 0 (l.23) e envia uma confirmação ao dispositivo que enviou a mensagem de evento crítico (l.24). Caso receba a mensagem de confirmação do atendimento, o dispositivo atualiza seu estado (l.28) e também inicia o tempo de serviço (l.29). O dispositivo retira de sua vizinhança o emissor do *broadcast* ao receber um anúncio de parada (l.31). Finalmente, caso receba a mensagem de interrupção do atendimento, o dispositivo atualizada seu estado (l.33), reinicia o tempo de serviço (l.34) e retira de sua vizinhança o emissor da mensagem (l.35).

Algoritmo 4 Gerenciamento do recebimento de mensagens

```
1: procedure PacketReceived(packet)   // Executa ao receber pacote
2:     tag ← packet.tag
3:     from ← packet.from
4:     switch tag do
5:         case 0
6:             if ThisNode.Status = FALSE then
7:                 SendUnicast(from, [ThisNode.Competence + ThisNode.Interests], 1)
8:         case 1
9:             compRec ← packet.competenceReceived
10:            intRec ← packet.interestsReceived
11:            if GetNCommonInterests(interestsReceived) = 0 then
12:                break
13:            if HasReferencialInterest(ThisNode.Interests) then
14:                nodeTrust ← EvaluateNeighborTrust(compRec, intRec)
15:            if ThisNode.IsAlreadyNeighbor(from) then
16:                ThisNode.TurnNeighborOn(from)
17:            else
18:                ThisNode.RegisterNeighbor(from, compRec, intRec, nodeTrust);
19:        case 2
20:            if ThisNode.Status = FALSE then
21:                ThisNode.Attending ← TRUE
22:                ThisNode.EmergencyNode ← from
23:                ThisNode.ServiceTime ← 0
24:                SendUnicast(from, "Can attend", 3)
25:            else
26:                ThisNode.UnregisterNeighbor(newFrom)
27:        case 3
28:            ThisNode.Service ← TRUE
29:            ThisNode.ServiceTime ← 0
30:        case 4
31:            ThisNode.UnregisterNeighbor(from)
32:        case 5
33:            ThisNode.Service ← FALSE
34:            ThisNode.ServiceTime ← 0
35:            ThisNode.UnregisterNeighbor(from)
```

4.6 RESUMO

Esta seção apresentou o sistema proposto para este trabalho. Dentro disso, mostrou as bases teóricas que o sustentam com a formação de comunidades de interesse, cálculo de confiança e a gestão de eventos críticos. Além disso, o funcionamento da proposta foi demonstrada com a interação entre os componentes e os possíveis fluxos. Finalmente, a implementação foi exibida e explicada com os principais algoritmos do sistema.

5 AVALIAÇÃO

Este trabalho aplicou o sistema proposto no Capítulo 4 ao contexto de saúde, com um cenário simulando eventos críticos relacionados à saúde dos indivíduos. O cenário considera 100 indivíduos portando dispositivos computacionais (nós) equipados com Wi-Fi, se movimentando nas ruas da cidade de Estocolmo, na Suécia, em uma área de 400m x 430m, com velocidades entre 0,5m/s e 2m/s. O trabalho (Helgason et al., 2014) validou esse modelo de mobilidade. Para essas pessoas foram distribuídas, de maneira aleatória, competências e interesses. A distribuição adotada está representada na Tabela 5.1. Cada indivíduo poderia ter apenas uma competência e entre um e cinco interesses.

Tabela 5.1: Distribuição dos aspectos sociais atribuídos aos indivíduos

Aspectos Sociais	**Competências**				**Interesses**				
	Médico	Enfermeiro	Cuidador	Outras	Saúde	Turismo	Música	Filmes	Livros
# de Indivíduos	10	15	20	55	20	30	45	60	15

5.1 AMBIENTE DE DESENVOLVIMENTO

O ambiente de desenvolvimento utilizado na avaliação do sistema proposto consistiu no emprego da ferramenta *ns-3*, versão 3.29, conforme comentado na Seção 4.5. Além disso, a ferramenta foi utilizada nos sistemas operacionais Elementary OS 5.0 Juno e Debian 9.1. O desenvolvimento ocorreu no ambiente de desenvolvimento integrado (do inglês, *Integrated Development Environment* - IDE) do *Visual Studio Code*, versão 1.40.2, utilizando a linguagem de programação *C++*. Durante as simulações, dados estatísticos foram coletados e armazenados em arquivos de texto. Utilizou-se também a linguagem de programação *Python* para organização dos dados e a linguagem de programação *R* para geração de gráficos na IDE *RStudio*.

5.2 METODOLOGIA

A metodologia de avaliação deste trabalho considerou 35 rodadas de simulações independentes proporcionando um intervalo de confiança de 95%, no qual cada rodada levou 900s para execução completa. Os nós foram numerados de 1 a 100 e os que poderiam entrar em estado crítico, 29 nós entre os 100, variaram a cada simulação, assim como os tempos em que os eventos críticos ocorreriam, a competência de cada nó e seu conjunto de interesses.

Três pares de nós foram escolhidos para manter competências e conjuntos de interesses fixos, a fim de avaliar o desempenho do sistema. Esses pares de nós fixos foram os (1,6), (14,17), (26,33). Além disso, dois cenários distintos foram considerados para avaliar a consistência do sistema, conforme mostra a Tabela 5.2. Os tempos foram definidos nos instantes em que os nós de mesmo par se encontram na vizinhança um do outro. O primeiro cenário foi a ocorrência de eventos críticos simultâneos entre os dois nós do par. O segundo cenário analisado considerou eventos críticos ocorridos com um intervalo de 10s entre os nós do par. Os seis nós fixos receberam a competência de médico e todos os interesses em todas as simulações. Desse modo, um nó teria uma probabilidade maior de escolher outro nó do mesmo par.

Par de Nós Avaliados	**Instante do Evento Crítico**	
	Eventos Sequenciais	**Eventos Simultâneos**
1 **6**	90s 100s	90s
14 **17**	110s 120s	110s
26 **33**	210s 220s	210s

Tabela 5.2: Configuração dos eventos críticos dos nós avaliados

As métricas utilizadas para avaliar o sistema proposto estão na Tabela 5.3. Elas foram pensadas para validar todos os mecanismos apresentados no Capítulo 4. A primeira métrica concerne ao agrupamento dos nós em comunidades. A segunda é utilizada para verificar o desempenho do sistema em relação ao atendimento bem sucedido de eventos críticos. A terceira delas mede a precisão do sistema na disseminação dos dados em relação ao número de envios até atingir sucesso. A quarta métrica avalia o número médio de disseminações, uma vez que os nós podem realizar mais de uma tentativa para obter uma garantia de atendimento de sucesso. Ademais, a quinta avalia o tempo médio em que qualquer disseminação de dados sensíveis leva para sair do transmissor e sua confirmação de recebimento pelo receptor retornar ao transmissor. Por fim, a última métrica é parecida com a anterior, porém ela mensura a média da diferença do tempo em que a primeira disseminação de dados sensíveis saiu do transmissor e a última confirmação de sucesso do receptor retornou ao transmissor.

Tabela 5.3: Métricas de avaliação de desempenho

Descrição	Equação
Número Médio de Comunidades de Interesse em Saúde (N_C) computa a média do somatório de todas as comunidades de saúde formadas em cada execução y, conforme o total de possibilidades de mudanças t_s das comunidades, por um nó x ao longo de todas as simulações (N_S).	$N_C = \sum_{x=1}^{N_S} \sum_{y=1}^{t_s} \frac{C_{xy}}{t_s \times N_S}$
Taxa de Sucesso na Disseminação dos Dados (TS) indica a taxa de sucesso na entrega dos dados à pessoa adequada, sendo a razão entre o total de acessos com sucesso aos dados sensíveis ($A_{Success}$) e o total de vezes que os dados estiveram disponíveis para acesso (A_{Disp}).	$TS = \frac{A_{Success}}{A_{Disp}} \times 100$
Taxa de Precisão na Disseminação dos Dados (TP) indica a taxa de sucesso na entrega dos dados à pessoa adequada em relação ao número de envios realizados, sendo a razão entre o total de acessos com sucesso aos dados sensíveis ($A_{Success}$) e o total de disseminações (A_{total}).	$TP = \frac{A_{Success}}{A_{total}} \times 100$
Número Médio de Disseminações de Dados Sensíveis (N_D) computa o número médio de disseminações de um determinado nó para todas as simulações realizadas. Ele corresponde à razão entre o número total de disseminações (N_{Dtotal}) e o total de simulações realizadas (N_S).	$N_D = \frac{N_{Dtotal}}{N_S}$
Tempo Médio de Acesso aos Dados Sensíveis (TM_{acc}) computa o tempo médio de acesso aos dados sensíveis de um determinado nó para todas as simulações realizadas. Ele corresponde ao somatório da razão entre as diferenças entre o momento em que os dados foram acessados (t_a) e o momento da sua disseminação (t_d) e o total de execuções (N_S).	$TM_{acc} = \sum_{i=1}^{N_S} \frac{ta_i - td_i}{N_S}$
Tempo Médio de Atendimento de Sucesso (TM_{att}) computa o tempo médio que um determinado nó levou para garantir um atendimento de sucesso em todas as simulações realizadas. Ele corresponde ao somatório da razão entre as diferenças entre o último momento em que os dados foram acessados com sucesso (t_s) e o momento da sua disseminação (t_d) e o total de execuções (N_S).	$TM_{att} = \sum_{i=1}^{N_S} \frac{ts_i - td_i}{N_S}$

5.3 RESULTADOS

Esta seção apresenta os resultados obtidos dos dois cenários explorados com base nas métricas definidas anteriormente. O primeiro cenário corresponde aos eventos críticos sequenciais na Subseção 5.3.1. Depois, os resultados para o cenário de eventos críticos simultâneos são exibidos e discutidos na Subseção 5.3.2.

5.3.1 Eventos Críticos Sequenciais

No cenário de eventos críticos sequenciais em todas as simulações os nós receptores confirmaram as disseminações dos nós transmissores, pois no momento em que avaliaram a vizinhança para enviá-las os nós receptores estavam em situação normal, porém após 10s os nós receptores entraram em estado crítico, quando se fez necessária a interrupção do atendimento. Esse cenário apresentou um número médio de comunidades de saúde entre 2 e 6, conforme mostra a Figura 5.1. Esses números demonstram que a formação de comunidades depende de cada nó, podendo variar em relação ao quanto ele se movimenta ao longo do tempo e com quais outros nós ele interage.

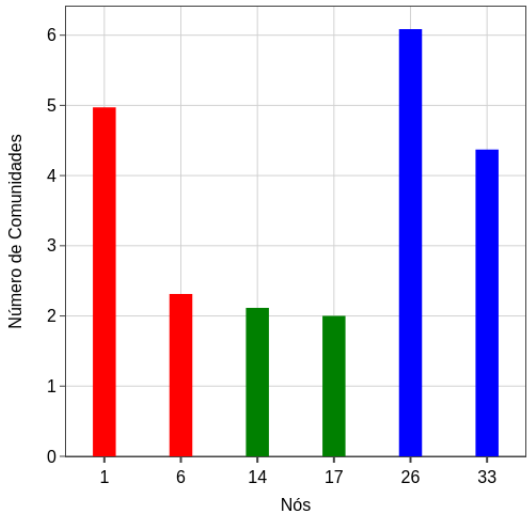


Figura 5.1: Número médio de comunidades de saúde estabelecidas

Na Tabela 5.4 observam-se as taxas de precisão e sucesso em relação às disseminações. Apesar do nó 6 apresentar uma TP igual a 100%, é importante notar que ele não obteve sucesso nas 35 rodadas, apresentando um TS de 28,57%. Por outro lado, o nó 1 apresentou um comportamento mais assertivo entre aqueles que obtiveram sucesso em todas as simulações pois além de apresentar um TP de aproximadamente 79,55% obteve um TS de 100%. Em seguida, os nós 14 e 26 também disseminaram seus dados com sucesso em todas as rodadas, porém precisaram de mais tentativas para isso. Os nós 17 e 33 não obtiveram sucesso em nenhuma rodada nem realizaram disseminações, portanto apresentaram um TP e um TS de 0%.

Tabela 5.4: Taxa de sucesso na disseminação dos dados

Nós	TP	TS
1	79,55%	100%
6	100%	28,57%
14	56,45%	100%
17	0%	0%
26	67,31%	100%
33	0%	0%

A Figura 5.2 representa o número médio de envios dos nós avaliados. O nó 14 apresentou o maior número médio de envios ao longo das 35 simulações, o que corresponde ao baixo TP mostrado na Tabela 5.4. Logo após, os nós 26 e 1 apresentaram números um pouco inferiores

aos do nó 14. Além disso, o nó 6 aparece com um número menor que um envio por simulação, confirmando que não teve a chance de disseminar seus dados em todas as rodadas.

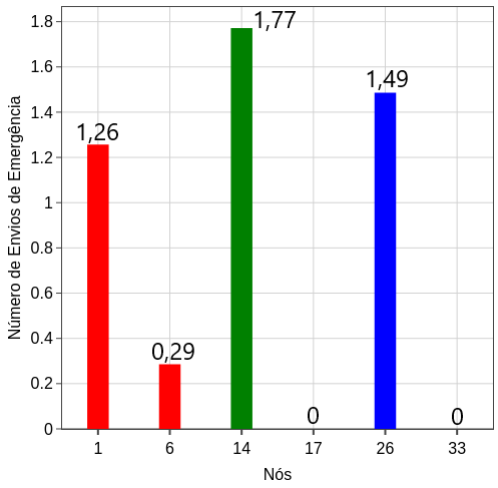


Figura 5.2: Número médio de disseminações

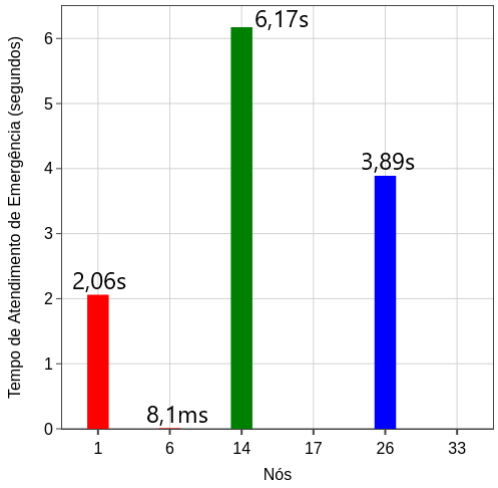


Figura 5.3: Tempo médio para uma disseminação de sucesso

A Figura 5.3 mostra resultados para o tempo médio para uma disseminação de sucesso que estão correlacionados com a métrica anterior. Esse comportamento é consistente, uma vez que quanto mais disseminações necessárias para garantia de uma disseminação bem sucedida, maior é o tempo de atendimento total. O nó 14 que apresentou o maior número de envios também apresenta um maior tempo médio de atendimento, e respectivamente com os nós seguintes. O nó 6 aparece com TM_{att} bem abaixo dos outros porque garantiu sua disseminação já nas primeiras tentativas, o que pode ser confirmado já que seu TP foi de 100%.

A Figura 5.4 exibe o tempo médio relativo à confirmação de recebimento da disseminação. Esse número depende basicamente da distância entre o nó transmissor e o nó receptor. Por isso, pode-se inferir que o nó 6 se comunicou com um vizinho mais distante para receber uma confirmação comparado aos outros nós avaliados. Os resultados se mostram satisfatórios para atender à latência máxima de 125ms estabelecida pela IEEE para entrega de alertas médicos (IEEE, 2012).

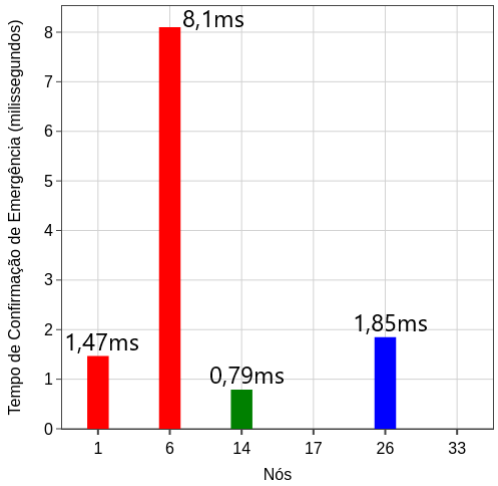


Figura 5.4: Tempo médio de confirmação de disseminação

Os nós 26 e 33 foram escolhidos para demonstrar a evolução do estabelecimento de suas comunidades de saúde ao longo do tempo durante uma simulação específica. Na Figura 5.5 observa-se que o nó 26 inicia com uma vizinhança grande devido a concentração de nós no início da simulação, porém ao longo do tempo sua vizinhança e comunidade de saúde se adaptam conforme as interações com outros nós ocorrem. Ao longo dessa simulação o nó 26 estabeleceu 13 diferentes comunidades em torno do interesse em saúde. O indivíduo 26 entra em estado crítico no instante de 210s, porém percebe-se que ele resiste mais algum tempo ao realizar a segunda tentativa e aguardar 24s para garantir uma disseminação de sucesso.

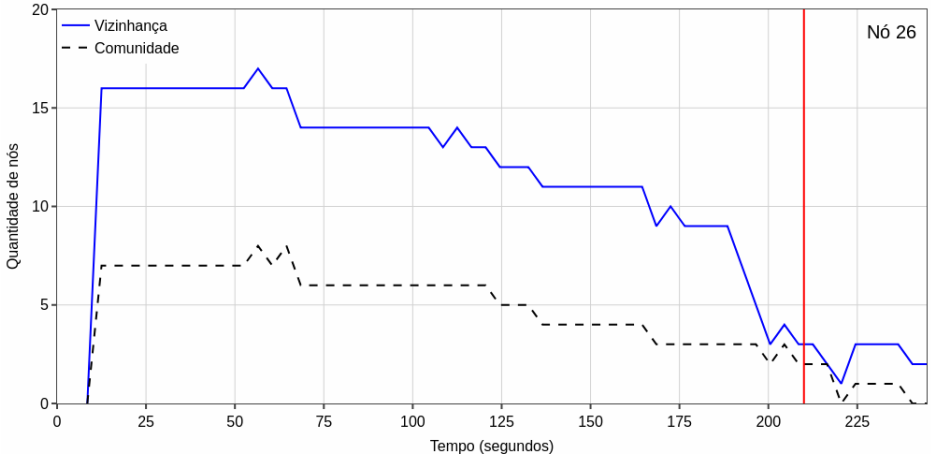


Figura 5.5: Evolução das comunidades de saúde do nó 26

Na Figura 5.6 nota-se o mesmo comportamento dinâmico da vizinhança e do estabelecimento de comunidades de saúde para o nó 33. Contudo, esse indivíduo entrou em estado crítico no instante de 220s e não seguiu para uma segunda tentativa pois não apresentou nenhum vizinho nesse instante, e consequentemente não formou comunidade de saúde com ninguém.

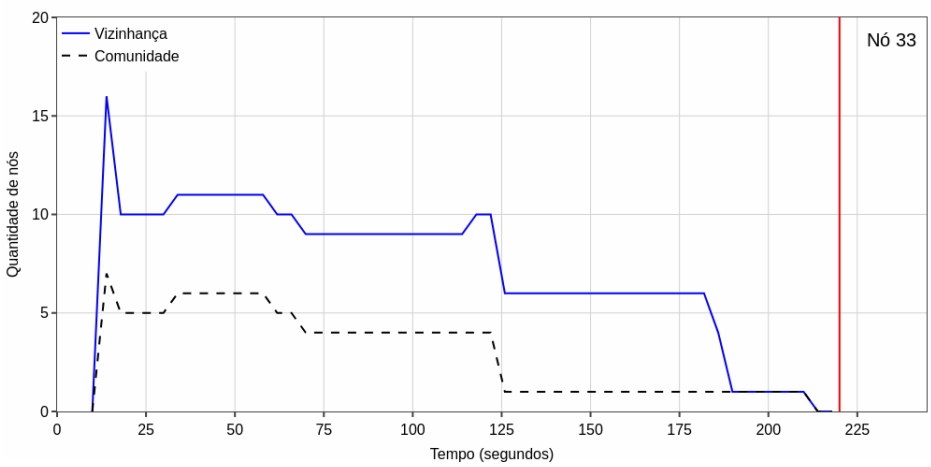


Figura 5.6: Evolução das comunidades de saúde do nó 33

5.3.2 Eventos Críticos Simultâneos

No cenário de eventos críticos simultâneos em todas as simulações os pares ignoraram as disseminações um do outro, pois no momento em que avaliaram a vizinhança para enviá-las os nós estavam em situação normal, porém ao recebê-las eles já se encontravam em estado crítico, não podendo confirmar o recebimento. Esse cenário apresentou um número médio de comunidades de saúde entre 2 e 6,23, conforme mostrado na Figura 5.7. Esse resultado é muito similar ao anterior, uma vez que o modelo de mobilidade é o mesmo e os nós percorrem o mesmo trajeto, interagindo com a mesma quantidade de nós.

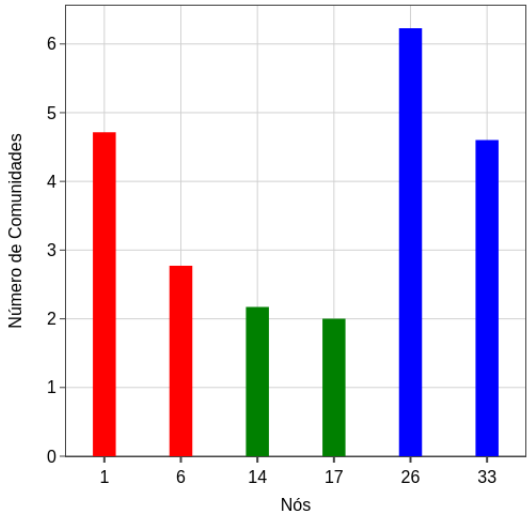


Figura 5.7: Número médio de comunidades de saúde estabelecidas

As taxas de precisão e sucesso em relação às disseminações são apresentadas na Tabela 5.5. Nenhum nó disseminou seus dados com sucesso em todas as rodadas nesse cenário. O nó que chegou mais próximo disso foi o 14 que obteve um TS de 88,71%, mas precisou de 66 envios para isso, atingindo um TS de 45,45%. Em seguida, observa-se que o nó 6 disseminou seus dados com sucesso em mais rodadas do que no cenário anterior, aumentando seu TS de 28,57% para 40%, mas precisou de muito mais tentativas para isso, diminuindo seu TS de 100% para 28,57%. Os nós 1 e 26 tiveram uma diminuição considerável tanto do seu TS quanto do

seu TP. Por fim, os nós 17 e 33 continuaram sem sucesso, mas dessa vez com pelo menos uma tentativa por rodada, que corresponde a tentativa realizada com o próprio par.

Tabela 5.5: Taxa de sucesso na disseminação dos dados

Nós	TP	TS
1	14,63%	17,14%
6	28,57%	40%
14	45,45%	88,71%
17	0%	0%
26	38,60%	62,86%
33	0%	0%

A Figura 5.8 representa resultados referentes ao número de disseminações. Em geral, os nós apresentaram números parecidos com o cenário anterior, com exceção do nó 6. O aumento considerável do número médio de envios do nó 6 corresponde com a queda do seu TP, apresentado na Tabela 5.5, em relação ao cenário anterior.

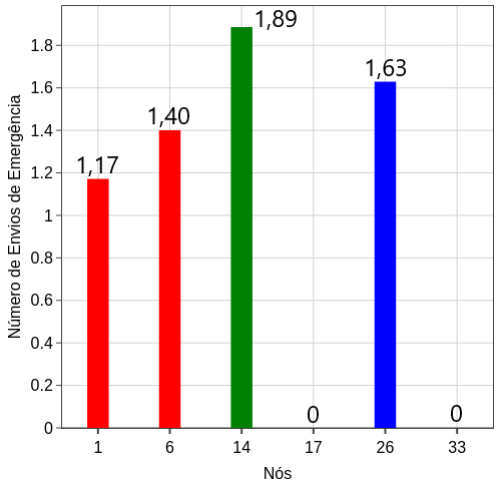


Figura 5.8: Número médio de disseminações

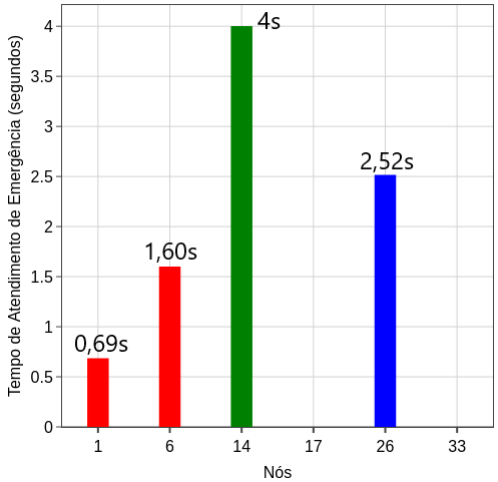


Figura 5.9: Tempo médio para uma disseminação de sucesso

A Figura 5.9 mostra novamente resultados correlacionados com a métrica anterior. O nó 1 apresentou uma queda em comparação com o cenário anterior devido a diminuição de seu TS, uma vez que obteve menos sucesso e portanto teve menos situações em que precisou esperar para garantir sua disseminação. Por outro lado, o nó 6 apresentou a situação inversa, onde realizou mais envios, conforme demonstrado com a diminuição de seu TP, e precisou aguardar mais tempo para garantir a disseminação.

A Figura 5.10 exibe o tempo médio relativo à confirmação de recebimento da disseminação. No geral os nós apresentaram resultados parecidos com o cenário anterior. Destaca-se a diminuição considerável do nó 6 de 8,1ms para 0,73ms, mostrando que possivelmente realizou seus envios para nós mais próximos no cenário atual do que no anterior. Com isso, os resultados continuaram satisfazendo a latência máxima de 125ms estabelecida pela IEEE para entrega de alertas médicos (IEEE, 2012).

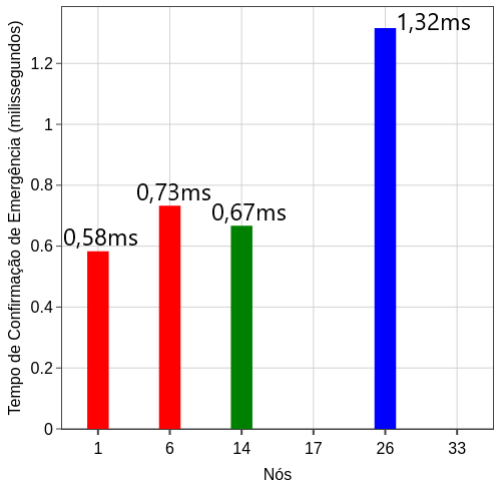


Figura 5.10: Tempo médio de confirmação de disseminação

Os nós 14 e 17 foram escolhidos nesse cenário para demonstrar o estabelecimento de comunidades ao longo de uma simulação específica. Na Figura 5.11 nota-se que o nó 17 interagiu com poucos nós até entrar em estado emergencial no tempo de 110s. Ele estabeleceu apenas duas comunidades de saúde distintas e no momento do evento crítico possuía apenas um vizinho com quem também formou uma comunidade de saúde. Esse vizinho era o nó 14, que não respondeu ao envio por ter entrado em estado crítico no mesmo instante. Com isso, o nó 17 encerrou suas atividades logo após, pois não havia outro vizinho e portanto não estabeleceu uma comunidade de saúde para realizar uma segunda tentativa, conforme mostra a Figura 5.12.

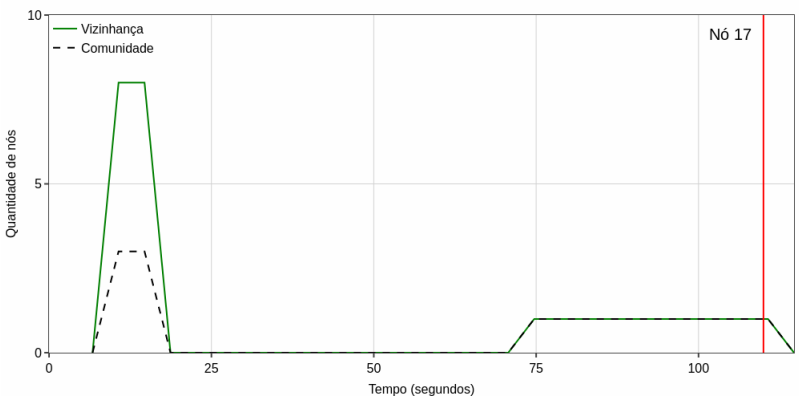


Figura 5.11: Evolução das comunidades de saúde do nó 17

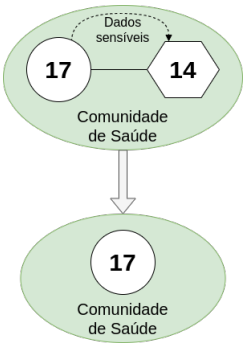


Figura 5.12: Comunidade de saúde do nó 17 no primeiro e segundo envio

O comportamento do nó 14 nessa simulação foi interessante, por ter realizado três envios ao todo para obter sucesso na disseminação de seus dados. Essa situação é bastante improvável de acontecer de maneira espontânea, mas possível no mundo real. O nó 14 entrou em estado crítico no instante 110s e primeiramente escolheu o nó 17, que por sua vez não respondeu por ter entrado em estado crítico no mesmo momento. Em um segundo envio o nó 14 escolheu o nó 98, o qual confirmou a disseminação. O intervalo de garantia de 24s começou a ser contado a partir de 118.1s, porém aos 135s o nó 98 também entrou em estado emergencial. Com isso, ele enviou um sinal de interrupção do atendimento para o nó 14. Por sua vez, o nó 14 removeu o nó 98 de sua vizinhança e partiu para uma terceira tentativa, na qual enfim obteve sucesso. A evolução da vizinhança e da comunidade de saúde do nó 14 está representada na Figura 5.13 e seu estado nos três envios realizados podem ser visualizados na Figura 5.14. Esse exemplo demonstra a capacidade do sistema proposto de reagir a múltiplos eventos críticos e de garantir que o nó receptor da disseminação de dados sensíveis terá um tempo suficiente para agir.

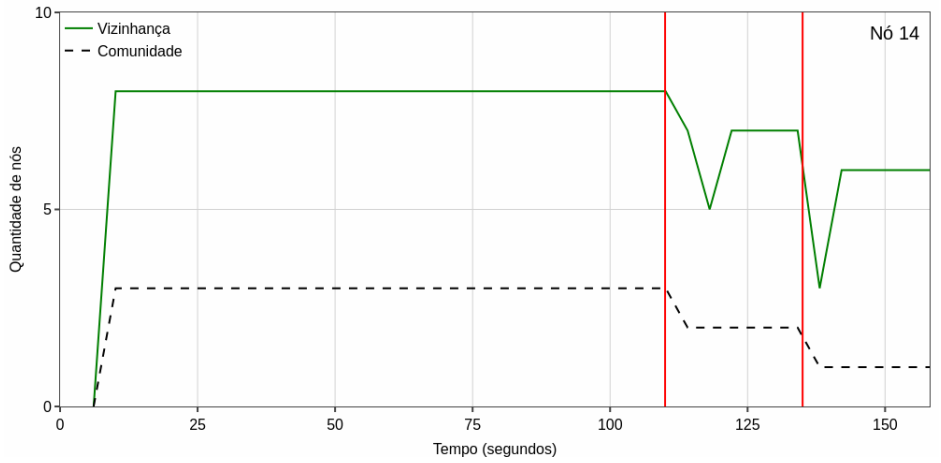


Figura 5.13: Evolução das comunidades de saúde do nó 14

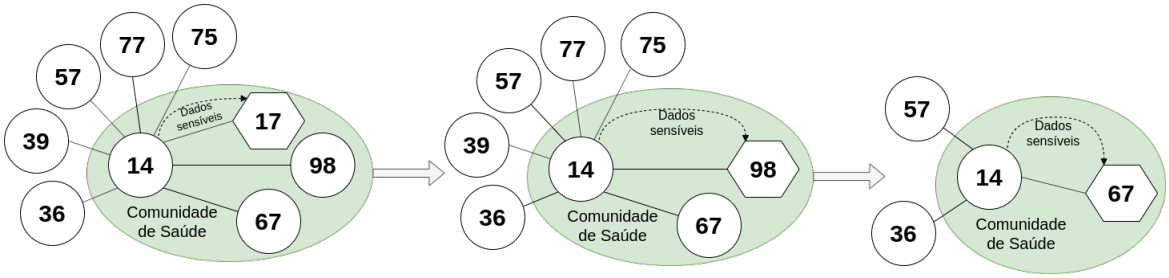


Figura 5.14: Comunidade de saúde do nó 14 no instante dos três envios realizados

5.4 RESUMO

Este capítulo apresentou uma avaliação do sistema proposto no Capítulo 4. Com a utilização de métricas e uma metodologia definida para os dois cenários, observou-se a consistência do sistema, assim como as particularidades de cada nó e de cada cenário. A formação dinâmica de comunidades foi demonstrada. Além disso, o desempenho em relação ao sucesso e precisão das disseminações de dados sensíveis variou consideravelmente dependendo do nó e do cenário. Os número de envios e o tempo de atendimento se mostraram correlacionados nos dois cenários. Ademais, os tempos de confirmação em todos os casos ficaram dentro da latência máxima esperada pela IEEE para entrega de alertas médicos. Por fim, demonstrou-se a capacidade do sistema em lidar com múltiplos eventos críticos.

6 CONCLUSÃO

O desenvolvimento de tecnologias de comunicação e o aumento do uso da Internet têm colaborado para expansão de pesquisas em IoT. Com a visão de uma computação cada vez mais onipresente, a tendência é que os dispositivos computacionais integrem o cotidiano das pessoas com o uso das redes sem fio, de modo a se tornarem indispensáveis. A união entre a IoT e as SNs deu espaço para o surgimento da SIoT, que incorporou as relações sociais e serviços centrados nos seres humanos. Nesse contexto, o conceito de confiança aparece em vários trabalhos e sua avaliação desponta como um fator determinante para a tomada de decisões. Além disso, o agrupamento de dispositivos em comunidades nas redes complexas mostra-se uma técnica viável para tentativa de modelar a complexidade do mundo real.

Esse trabalho propôs um sistema para gestão de múltiplos eventos críticos para disseminação de dados pessoais sensíveis com agrupamento dos dispositivos em comunidades de interesse e o uso de aspectos sociais para avaliação da confiança entre dois indivíduos. Os resultados demonstraram a capacidade do sistema em lidar com eventos críticos simultâneos e sequenciais de maneira autônoma, ágil e assertiva. A proposta é genérica e pode ser aplicada a qualquer domínio de aplicação que se encaixe nos cenários apresentados. A área da saúde foi explorada nas simulações para demonstrar com maior clareza os objetivos desse trabalho. O sistema satisfez a latência máxima de 125ms definida pela IEEE para entrega de alertas médicos. Por fim, atingiu uma taxa de sucesso de 100% na disseminação dos dados em alguns casos.

6.1 TRABALHOS FUTUROS

Entre as possibilidades de trabalhos futuros destaca-se o emprego de versões mais recentes do padrão IEEE 802.11, como por exemplo o 802.11n ou o 802.11ac. Com maior taxa de dados e menos ruídos seria necessário observar como o sistema reagiria e se ele se beneficiaria disso de algum modo. Além disso, como esses padrões possibilitam um maior raio de alcance na transmissão de dados, seria interessante investigar qual seria o valor mais adequado de modo a garantir uma disseminação rápida o suficiente e que ao mesmo tempo avaliasse o maior número de pessoas. Ademais, um trabalho futuro poderia adotar o IPv6 ao invés do IPv4, visto que a intenção de sua criação sempre foi substituir a versão mais antiga pela mais nova que tem a capacidade de identificar um maior número de dispositivos.

Um cenário a ser explorado é a execução do sistema com mobilidades heterogêneas, incluindo dispositivos com velocidades maiores como carros, bicicletas e patinetes. Com isso, é possível que os resultados com a formação de comunidades e a disseminação dos dados se alterem e sejam necessários ajustes no sistema para lidar com essas situações. A velocidade e direção poderiam ser calculadas pelo tempo de transmissão das mensagens entre os dispositivos para se tornarem métricas consideradas na tomada de decisão de disseminação dos dados.

A LGPD e a GDPR iriam impactar a operação do sistema, uma vez que existe um processamento de dados pessoais sensíveis relativos à saúde dos usuários e um armazenamento de dados que podem identificá-los. Apesar disso, apenas os interesses e a competência dos usuários são armazenados, já que os dados de saúde são utilizados apenas para disparar o evento crítico. O sistema não guarda nenhum histórico desses eventos ou de dados referentes ao atendimento. O funcionamento depende da participação voluntária das pessoas, onde existiria um consentimento explícito. O modelo de negócios também pode ser discutido em um trabalho futuro.

Por fim, é possível vislumbrar a utilização do sistema implementado nesse trabalho em cidades inteligentes do futuro, onde a utilização da IoT em ampla escala já seria uma realidade. Esse uso tornaria a cidade ainda mais preparada para atender as necessidades de uma população cada vez mais idosa (ONU, 2020). Além do sistema de reação imediata proposto, poderia haver uma integração com outros sistemas dessa cidade inteligente. No caso da saúde, por exemplo, haveria integração com os sistemas de saúde. Com isso, a pessoa que sofresse um evento crítico teria não apenas um auxílio imediato, como também uma assistência melhor equipada e especializada em um menor período de tempo, aumentando suas chances de recuperação.

REFERÊNCIAS

Al-Hamadi, H. e Chen, I. R. (2017). Trust-based decision making for health iot systems. *IEEE Internet of Things Journal*, 4(5):1408–1419.

Atzori, L., Iera, A. e Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805.

Bao, F., Chen, I. e Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. Em *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, páginas 1–7.

Barsotti, D. (2019). Leis GDPR e LGPD. `https://politica.estadao.com.br/blogs/fausto-macedo/lei-gdpr-e-lgpd-qual-a-relacao-na-seguranca-da-informacao-e-os-impactos-nas-organizacoes-no-mundo/`. Acessado em 11/11/2019.

Batista, A. d. S. (2019). Disseminação segura de dados pessoais vitais para apoio às tomadas de decisão em situações emergenciais. Dissertação de Mestrado, Universidade Federal do Paraná, Curitiba, Paraná, Brasil.

Beach, A., Gartrell, M., Akkala, S., Elston, J., Kelley, J., Nishimoto, K., Ray, B., Razgulin, S., Sundaresan, K., Surendar, B., Terada, M. e Han, R. (2008). Whozthat? evolving an ecosystem for context-aware mobile social networks. *IEEE Network*, 22(4):50–55.

Borisov, N., Goldberg, I. e Wagner, D. (2001). Intercepting mobile communications: The insecurity of 802.11. Em *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, MobiCom '01, páginas 180–189, New York, NY, USA. ACM.

Bottazzi, D., Montanari, R. e Toninelli, A. (2007). Context-aware middleware for anytime, anywhere social networks. *IEEE Intelligent Systems*, 22(5):23–32.

Carminati, B., Ferrari, E. e Guglielmi, M. (2016). Detection of unspecified emergencies for controlled information sharing. *IEEE Transactions on Dependable and Secure Computing*, 13(6):630–643.

Casteigts, A., Flocchini, P., Quattrociocchi, W. e Santoro, N. (2012). Time-varying graphs and dynamic networks. *International Journal of Parallel, Emergent and Distributed Systems*, 27(5):387–408.

Chen, I., Bao, F. e Guo, J. (2016). Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing*, 13(6):684–696.

Cho, J.-H., Chan, K. e Adali, S. (2015). A survey on trust modeling. *ACM Comput. Surv.*, 48(2):28:1–28:40.

Choffnes, D. R. e Bustamante, F. E. (2008). Taming the torrent: A practical approach to reducing cross-isp traffic in peer-to-peer systems. *SIGCOMM Comput. Commun. Rev.*, 38(4):363–374.

Eagle, N. e Pentland, A. (2005). Social serendipity: mobilizing social software. *IEEE Pervasive Computing*, 4(2):28–34.

Feige, U., Fiat, A. e Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94.

Gambetta, D. (1988). *Trust: Making and Breaking Cooperative Relations*. Blackwell.

Gazeta do Povo, C. (2019). Pela 2ª vez consecutiva, curitiba é finalista em prêmio mundial de cidades inteligentes. https://www.gazetadopovo.com.br/haus/inovacao/curitiba-finalista-premio-mundial-cidades-inteligentes-2019/. Acessado em 14/11/2019.

Guo, B., Yu, Z., Zhou, X. e Zhang, D. (2012). Opportunistic iot: Exploring the social side of the internet of things. Em *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, páginas 925–929.

Helgason, , Kouyoumdjieva, S. T. e Karlsson, G. (2014). Opportunistic communication and human mobility. *IEEE Transactions on Mobile Computing*, 13(7):1597–1610.

Holme, P. e Saramäki, J. (2012). Temporal networks. *Physics Reports*, 519(3):97 – 125. Temporal Networks.

IEEE (2012). IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. *IEEE Std 802.15.6-2012*, páginas 1–271.

Intersoft Consulting, E. (2019). General data protection regulation, definitions. https://gdpr-info.eu/art-4-gdpr/. Acessado em 24/11/2019.

Jr., H. S. J. (2002). The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization*, 47(3):291 – 307.

Latapy, M., Viard, T. e Magnien, C. (2018). Stream graphs and link streams for the modeling of interactions over time. *Social Network Analysis and Mining*, 8(1):61.

LBCA (2020). Lei geral de proteção de dados. https://www.lgpdbrasil.com.br/. Acessado em 07/03/2020.

Miorandi, D., Sicari, S., Pellegrini, F. D. e Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497 – 1516.

Mohammad, S. M. e Hirst, G. (2012). Distributional measures of semantic distance: A survey.

Mokhtar, S. B., Mashhadi, A. J., Capra, L. e McNamara, L. (2010). A self-organising directory and matching service for opportunistic social networking. Em *Proceedings of the 3rd Workshop on Social Network Systems*, SNS '10, páginas 5:1–5:6, New York, NY, USA. ACM.

Nuevo, D. A. L., Valles, D. R., Medina, E. M. e Pallares, R. M. (2015). Oiot: A platform to manage opportunistic iot communities. Em *2015 International Conference on Intelligent Environments*, páginas 104–111.

ONU (2020). A ONU e as pessoas idosas. https://nacoesunidas.org/acao/pessoas-idosas/. Acessado em 04/03/2020.

Ortiz, A. M., Hussein, D., Park, S., Han, S. N. e Crespi, N. (2014). The cluster between internet of things and social networks: Review and research challenges. *IEEE Internet of Things Journal*, 1(3):206–215.

Pelusi, L., Passarella, A. e Conti, M. (2006). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. *IEEE Communications Magazine*, 44(11):134–141.

Perahia, E. e Stacey, R. (2013). *Next Generation Wireless LANs: 802.11N and 802.11Ac*. Cambridge University Press, New York, NY, USA, 2nd edition.

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A. e Vasilakos, A. V. (2016). The quest for privacy in the internet of things. *IEEE Cloud Computing*, 3(2):36–45.

Ravindranath, L., Padmanabhan, V. N. e Agrawal, P. (2008). Sixthsense: Rfid-based enterprise intelligence. Em *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, MobiSys '08, páginas 253–266, New York, NY, USA. ACM.

Rossetti, G. e Cazabet, R. (2018). Community discovery in dynamic networks: A survey. *ACM Comput. Surv.*, 51(2):35:1–35:37.

Rossetti, G., Guidotti, R., Pennacchioli, D., Pedreschi, D. e Giannotti, F. (2015). Interaction prediction in dynamic networks exploiting community discovery. Em *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, páginas 553–558.

Schulz, P., Matthe, M., Klessig, H., Simsek, M., Fettweis, G., Ansari, J., Ashraf, S. A., Almeroth, B., Voigt, J., Riedel, I., Puschmann, A., Mitschele-Thiel, A., Muller, M., Elste, T. e Windisch, M. (2017). Latency critical iot applications in 5g: Perspective on the design of radio interface and network architecture. *IEEE Communications Magazine*, 55(2):70–78.

Tanenbaum, A., Wetherall, D. e Translations, O. (2011). *Redes de computadores*. PRENTICE HALL BRASIL.

Thibaud, M., Chi, H., Zhou, W. e Piramuthu, S. (2018). Internet of things (iot) in high-risk environment, health and safety (ehs) industries: A comprehensive review. *Decision Support Systems*, 108:79 – 95.

Truong, N. B., Lee, H., Askwith, B. e Lee, G. M. (2017). Toward a trust evaluation mechanism in the social internet of things. *Sensors*, 17(6).

Wakka, W. (2019). Internet acima de 1 gbps chega a 5% da população mundial. `https://canaltech.com.br/telecom/internet-acima-de-1-gbps-chega-a-5-da-populacao-mundial-156157/`. Acessado em 06/12/2019.

We Are Social Ltd, S. (2019). Relatório digital da Internet. `https://wearesocial.com/global-digital-report-2019`. Acessado em 26/10/2019.

Weiser, M. (1991). The computer for the 21 st century. *Scientific American*, 265(3):94–105.

Zorzi, M., Gluhak, A., Lange, S. e Bassi, A. (2010). From today's intranet of things to a future internet of things: a wireless- and mobility-related view. *IEEE Wireless Communications*, 17(6):44–51.