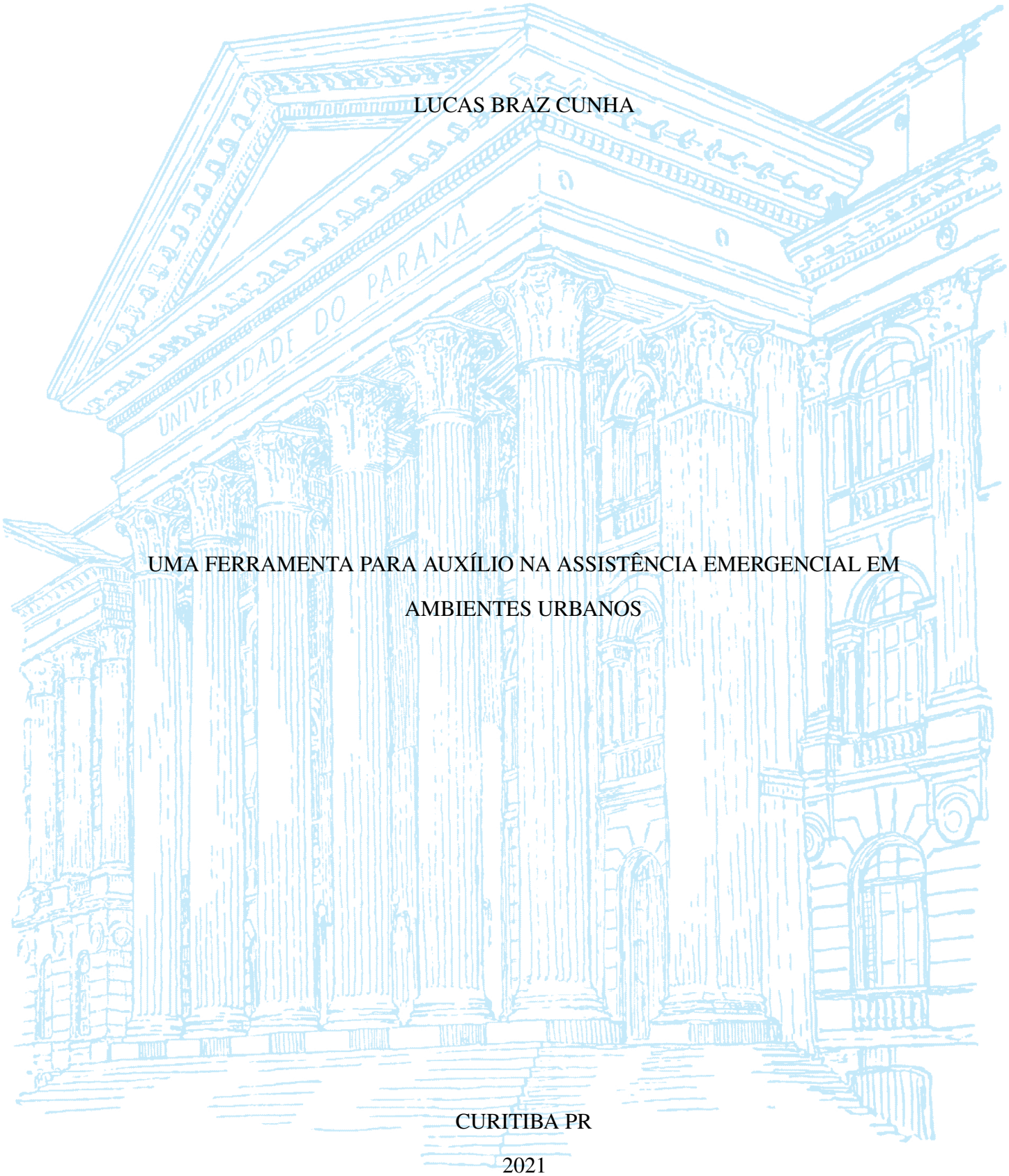
UNIVERSIDADE FEDERAL DO PARANÁ

LUCAS BRAZ CUNHA



UMA FERRAMENTA PARA AUXÍLIO NA ASSISTÊNCIA EMERGENCIAL EM AMBIENTES URBANOS

CURITIBA PR

2021

LUCAS BRAZ CUNHA

UMA FERRAMENTA PARA AUXÍLIO NA ASSISTÊNCIA EMERGENCIAL EM AMBIENTES URBANOS

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*.

Orientadora: Profa. Dra. Carmem Satie Hara.

Coorientador: Prof. Dr. Aldri Luiz dos Santos.

CURITIBA PR

2021

RESUMO

A utilização massiva da internet e sua presença quase constante na vida daqueles que têm acesso, são fontes de motivação para que organizações ofereçam serviços por meio dela. Esses serviços atendem aos mais diversos campos de atividade, como entretenimento, vendas, comunicação e saúde. Em especial, os serviços de saúde em redes (*e-health*) receberam um foco maior devido à sua importância na vida das pessoas. Isso ocorre pois a tecnologia pode auxiliar na melhoria da qualidade de vida das pessoas. Um exemplo dessa associação entre tecnologia e saúde é a implantação do uso da telemedicina durante a pandemia de COVID-19 no Brasil. Também existem outros serviços *e-health* com foco preventivo, como por exemplo através da mudança de hábitos das pessoas, focando em atividades saudáveis por meio de orientação disponibilizada em dispositivos móveis como smartphones. Entretanto, as situações de urgência e emergência fora do ambiente hospitalar são desafiadoras devido à sua imprevisibilidade e também à necessidade de atendimento imediato, sem conhecimento das condições do paciente. Nesse cenário, o desenvolvimento de tecnologias auxiliares é desafiador. Assim sendo, esta monografia tem por objetivo apresentar uma ferramenta que coordene e assegure a disseminação de dados de maneira segura em ambientes dinâmicos, não estruturados e sem conhecimento prévio entre os nós da rede, suportando as tomadas de decisão diante de situações emergenciais de saúde. Deste modo, torna-se possível reduzir o tempo de espera entre a ocorrência de uma situação de urgência ou emergência - evento crítico de saúde - e o primeiro atendimento. Esta monografia apresenta inicialmente os fundamentos necessários para o entendimento da ferramenta, bem como os trabalhos recentes que se relacionam com o tema. Em seguida, apresenta-se a ferramenta e detalha-se seu funcionamento. Ao final, uma avaliação a respeito da performance da ferramenta é apresentada, através da qual pode-se observar as restrições de tempo em que ela se enquadra.

Palavras-chave: Redes móveis. Computação sensível ao contexto. *E-Health*. Aplicativo Android.

ABSTRACT

The massive use of the internet, and it's almost constant presence in the lives of those who have access, are sources of motivation for organizations to provide services through it. These services serve the most diverse fields of activity, such as entertainment, sales, communication and health. In particular, network health services - e-health, have received a greater focus due to their importance in people's lives, since the technology can help improve people's quality of life. An example of this association between technology and health is the implementation of the use of telemedicine during the COVID-19 pandemic in Brazil. There are also other e-health services with a preventive focus, for example by changing people's habits by focusing on healthy activities through guidance available on mobile devices like smartphones. However, urgent care and emergency situations outside the hospital environment are challenging due to the unpredictability, and also the need for immediate care without knowledge of the patient's conditions. In this scenario, the development of auxiliary technologies is challenging. Therefore, this monograph aims to present a tool that coordinates and ensures the safe dissemination of sensitive data in dynamic, unstructured environments and without prior knowledge between the network nodes, supporting decision-making in emergency healthcare situations. In this way, it becomes possible to reduce the waiting time between the occurrence of an emergency situation - critical health event, and the first assistance. The monograph initially presents the necessary foundations for understanding the tool, as well as recent works related to the theme. Then, the tool is presented and its functioning is detailed. Lastly, an performance evaluation is carried out, through which it is possible to observe the time restrictions in which it fits.

Keywords: Mobile Networks. Context Sensitive Computing. E-Health. Aplicativo Android.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

AP	*Access Point*
	(Ponto de Acesso)
API	*Application Programming Interface*
	(Interface de Programação de Aplicação)
BSS	*Basic Service Set*
	(Conjunto Básico de Serviço)
CFM	Conselho Federal de Medicina
CNMS	*Context-aware Notification Management System*
	(Sistemas de Gerenciamento de Notificação Sensível ao Contexto)
CoI	*Community of Interest*
	(Comunidade de Interesse)
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
	(Acesso Múltiplo com Verificação de Portadora com Prevenção de Colisão)
DCF	*Distributed Coordination Function*
	(Função de Coordenação Distribuída)
DINF	Departamento de Informática
DSSS	*Direct Sequence Spread Spectrum*
	(Sequência Direta de Espalhamento do Espectro)
FHSS	*Frequency Hopping Spread Spectrum*
	(Espectro de Difusão em Frequência Variável)
GPS	*Global Positioning System*
	(Sistema de Posicionamento global)
IEEE	*Institute of Electrical and Electronics Engineers*
	(Instituto de Engenheiros Elétricos e Eletrônicos)
IOT	*Internet of Things*
	(Internet das Coisas)
iOS	*Iphone Operating System*
	(Sistema Operacional Iphone)
LAN	*Local Area Network*
	(Rede de Área Local)
LGPD	Lei Geral de Proteção de Dados Pessoais
MAC	*Medium Access Control*
	(Controle de Acesso ao Meio)
MAN	*Metropolitan Area Network*

	(Rede de Área Metropolitana)
MANET	*Mobile Ad hoc Network*
	(Rede Móvel Ad hoc)
NR2	Núcleo de Redes Sem Fio e Redes Avançadas
OSI	*Open Systems Interconnection*
	(Interconexão de Sistemas Abertos)
P2P	*Peer-to-Peer*
	(Ponto a Ponto)
PAN	*Personal Area Network*
	(Rede de Área Pessoal)
PDA	*Personal Digital Assistant*
	(Assistente Pessoal Digital)
PPGINF	Programa de Pós-Graduação em Informática
RCP	Reanimação Cardiopulmonar
SAMU	Serviço de Atendimento Móvel de Urgência
SIG	*Special Interest Group*
	(Grupo de Interesse Especial)
SMS	*Short Message Service*
	(Serviço de Mensagens Curtas)
STEALTH	*Social Trust-Based Health Information Dissemination Control*
	(Controle de Disseminação de Informações de Saúde Baseado em Confiança Social)
TCP	*Transmission Control Protocol*
	(Protocolo de Controle de Transmissão)
UDP	*User Datagram Protocol*
	(Protocolo de Datagramas de Usuário)
UFPR	Universidade Federal do Paraná
VANET	*Veicular Ad hoc Network*
	(Rede Veicular Ad hoc)
WECA	*Wi-Fi Alliance*
	(Aliança Wi-Fi)
WFA	*Wireless Ethernet Compatibility Alliance*
	(Aliança para Compatibilidade entre Redes Ethernet Sem Fio)
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
	(Rede de Área Local Sem Fio)
WPAN	*Wireless Personal Area Network*
	(Rede Pessoal Sem Fio)

SUMÁRIO

1 INTRODUÇÃO

A utilização massiva da internet e sua presença quase constante na vida daqueles que têm acesso motivam organizações a oferecerem serviços por meio dela. Esses serviços podem variar de contexto e aplicação de acordo com a organização proprietária. Empresas oferecem serviços como vendas online, enquanto governos possibilitam acesso à administração pública. Em ambos os casos, a transferência de informações é necessária e implica cuidados com o conteúdo, a frequência e o local pelo qual esses dados transitam. Além disso, de acordo com o serviço oferecido o *software* deve atender diferentes requisitos quanto a sua disponibilidade. Um serviço disponibilizado através da rede, que atenda situações de desastres naturais, necessita de robustez (Álvarez, 2020). Assim sendo, existem diferentes abordagens para a realização da comunicação em serviços oferecidos através da rede, dentre as quais existem as estratégias centralizadas e descentralizadas. As redes centralizadas são aquelas que estabelecem um ponto principal pelo qual as informações devem transitar, garantindo maior controle do tráfego. Por outro lado, as redes *ad hoc*, que constituem uma topologia descentralizada, não possuem dispositivo principal de transmissão, e portanto, cada integrante da rede é responsável por transmitir mensagens até o destinatário de maneira oportunística, isto é, suas conexões são estabelecidas de acordo com a disponibilidade de nós próximos e possuem duração limitada (Mohapatra e Krishnamurthy, 2004). Dessa forma os casos de indisponibilidade geral da rede na conexão não ocorrem, tendo em vista que não há ponto central de falha e cada dispositivo é responsável pela sua própria comunicação (Wu e Stojmenovic, 2004). Assim sendo, essas redes ficam dependentes da disponibilidades de dispositivos dentro do seu alcance para realizar a comunicação.

A abordagem descentralizada também oferece outras vantagens quando comparada à rede centralizada. Por não possuir um ponto central de manutenção da rede, os serviços que utilizam essa abordagem evitam o controle prejudicial das suas informações (Beierle e Eichinger, 2019). Ao utilizar um serviço de recomendação centralizado, como Google, Netflix e Youtube, o usuário está exposto à possibilidade de recomendações tendenciosas por um conflito de interesses entre o provedor e aquilo que seu serviço recomenda, por exemplo a recomendação prioritária de itens que geram maior lucro. As redes *ad hoc* podem ser bem aplicadas em contextos de alta mobilidade ou de falta de estrutura central, por exemplo, em áreas de recuperação de desastres. Em casos de eventos como esse, a infraestrutura de rede existente pode ter sido comprometida ou estar inoperante temporariamente. Dessa forma, a utilização de dispositivos que se comuniquem utilizando uma rede *ad hoc* permite mais flexibilidade na operação da rede (Wu e Stojmenovic, 2004) (Mohapatra e Krishnamurthy, 2004) (Álvarez, 2020).

Os serviços ofertados no âmbito de saúde, além do aspecto de disponibilidade, também possuem restrições maiores no que se refere à confidencialidade e confiabilidade (Batista, 2019). Essas aplicações podem atuar no âmbito preventivo, clínico ou emergencial, e os dados

compartilhados são sensíveis devido à sua natureza. Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD), vigente a partir de 2018 (Brasil, 2018), determina que, entre outros, os dados relativos a saúde devem ter sua privacidade preservada.

Em situações emergenciais como desastres naturais a utilização de redes descentralizadas oferece robustez, pois possibilita o compartilhamento de informações e auxilia no resgate de pessoas mesmo quando ocorre falha na infraestrutura de comunicação (Álvarez, 2020). Outros tipos de serviço *e-health* atuam no contexto de medicina preventiva, como por exemplo através da mudança de hábitos prejudicais à saúde. O sistema MobileCoach permite o desenvolvimento de intervenções digitais, através do envio de mensagens, para orientar os usuários acerca de seu comportamento (Filler et al., 2015). Dessa forma, contribuiu para redução no consumo de cigarro (Castro et al., 2017), ou até modificou traços de personalidade (Stieger et al., 2021). Nesse contexto, a utilização de mensagens adequadas é importante para garantir a aderência do paciente ao projeto. O ambiente e a situação no qual ele se encontra podem interferir na sua participação. Portanto, o envio de notificações deve considerar a circunstância atual do paciente (Künzler, 2019). Serviços do âmbito clínico podem incluir agendamento de consultas, obtenção de resultados de exames e realização de consultas remotas (telemedicina). A telemedicina é um tipo de aplicação recente, quando comparada com a medicina tradicional. Ela foi oficializada no ano de 2020, durante a pandemia de COVID-19 no Brasil, pelo Conselho Federal de Medicina (CFM) (CFM, 2020), que estabeleceu as normas e a validade desse tipo de atendimento. As características do atendimento são as seguintes:

- **Teleorientação**: para que profissionais da medicina realizem à distância a orientação e o encaminhamento de pacientes em isolamento;
- **Telemonitoramento**: ato realizado sob orientação e supervisão médica para monitoramento ou vigência à distância de parâmetros de saúde e/ou doença; e
- **Teleinterconsulta**: exclusivamente para troca de informações e opiniões entre médicos, para auxílio diagnóstico ou terapêutico.

As situações de urgência e emergência, no entanto, se diferenciam de outros tipos de atendimento pelas suas características de imprevisibilidade e a necessidade de atendimento imediato. Essas duas condições, quando associadas ao ambiente urbano, tornam a concepção de tecnologias auxiliares mais desafiadora. Uma situação de emergência pode ocorrer subitamente em qualquer lugar. Quando uma situação de emergência clínica ocorre fora do ambiente hospitalar, dependendo da gravidade da situação, o paciente precisa de atendimento médico especializado e, assim, há a necessidade de contato com o Serviço de Atendimento Móvel de Urgência (SAMU), por exemplo. Em 2019, de acordo com o levantamento da Rede Globo (Globo, 2019), o tempo médio de espera pelo atendimento de emergência em cinco capitais do Brasil foi de 15 a 38 minutos. Isso é muito relevante, dado que para cada minuto sem a realização de Reanimação Cardiopulmonar (PCR), a chance de sobrevivência de uma pessoa diminui entre 7 a

10%, enquanto que a execução imediata de PCR e desfibrilação com o equipamento adequado podem dobrar as chances de sobrevivência (American Heart Association, 2013). Entretanto, a natureza inesperada da situação dificulta a otimização desse atendimento, pois o deslocamento de profissionais capacitados é inevitável.

Nesse contexto, o atendimento emergencial fora da infraestrutura hospitalar eventualmente pode ser prestado por pessoas próximas do local e que possuam as habilidades necessárias para os primeiros-socorros da pessoa em situação de emergência, o paciente. No deslocamento diário de uma pessoa, como por exemplo para o trabalho, escola ou outras atividades, não há como prever quem estará disponível para ajudar caso ela precise de atendimento, são as situações chamadas de *Zero-Knowledge*, quando não há histórico de interações para avaliação (Feige et al., 1988) (Batista, 2019). Essa condição dificulta a realização de um auxílio emergencial efetivo, uma vez que ele varia conforme o estado do paciente e a competência de quem está prestando o atendimento. O atendimento também pode ser otimizado com o compartilhamento de dados acerca do histórico de saúde da pessoa, porém essa disseminação exige que o receptor seja qualificado para recebê-las, devido à natureza sensível das informações.

1.1 OBJETIVO

Diante de um evento crítico de saúde, o atendimento imediato do paciente é vital para ampliar a sua chance de sobrevivência. Nesse cenário, o atraso ocasionado pelo deslocamento dos profissionais de saúde é um fator prejudicial para a condição do paciente. Portanto, o objetivo desta monografia é apresentar uma ferramenta que coordene e assegure a disseminação de dados de saúde, disponibilizados pelo usuário, de maneira segura, em ambientes dinâmicos, *Zero-Knowledge* e não estruturados, suportando as tomadas de decisão diante de situações emergenciais de saúde. Assim sendo, a ferramenta reduz o tempo de espera até o primeiro atendimento, e possibilita uma redução nas consequências dessa demora, como sequelas e morte em casos mais graves. Além disso, são apresentados os conceitos fundamentais para o entendimento dessa ferramenta e a avaliação do seu comportamento em um cenário controlado.

1.2 ESTRUTURA DA MONOGRAFIA

Esta monografia está estruturada em seis capítulos. O Capítulo 2 define conceitos necessários para a compreensão da ferramenta e seu modelo de rede. O Capítulo 3 apresenta os trabalhos relacionados. O Capítulo 4 apresenta o modelo teórico utilizado como base para a ferramenta, as funcionalidades da aplicação e o seu fluxo de comunicação. O Capítulo 5 expõe a avaliação da aplicação com relação ao desempenho do seu mecanismo de análise da vizinhança e o envio de mensagem que auxilia na tomada de decisão. Por fim, o Capítulo 6 apresenta as considerações finais sobre o estudo realizado e os trabalhos futuros.

2 FUNDAMENTOS

Este capítulo apresenta os fundamentos necessários à compreensão e entendimento dos conceitos envolvidos nesse trabalho. A Seção 2.1 aborda o conceito de técnicas de comunicação e algumas tecnologias empregadas. A Seção 2.2 apresenta o conceito de confiança em redes de computadores e como pode ser modelado. A Seção 2.3 descreve o conceito de comunidades de interesse e sua aplicabilidade nesse contexto.

2.1 TÉCNICAS DE COMUNICAÇÃO

As redes de computadores foram criadas para estabelecer a comunicação entre dispositivos computacionais. Como qualquer atividade de comunicação, nessas redes existem 3 ingredientes para o seu funcionamento, um remetente e um destinatário que buscam trocar alguma informação, o segundo ingrediente é o meio pelo qual a mensagem é enviada e por último um conjunto de regras e protocolos para compreensão da mensagem (Kizza, 2005). No contexto das redes de computadores, os atores são os próprios dispositivos e o meio de comunicação - tais como através de cabo ou ondas de rádio, bem como o protocolo utilizado - por exemplo TCP ou UDP, que podem variar de acordo com o cenário específico.

A variação de aspectos da configuração da rede é possível graças ao modelo de interconexão de sistemas abertos (do inglês, *Open System Interconnection* - OSI), que estabelece 7 camadas com responsabilidades diferentes na tarefa de comunicação entre sistemas computacionais. Esse modelo foi criado em 1971 e formalizado em 1983 para ser um protocolo de comunicação para sistemas de rede local (Ethernet), garantindo a comunicação ponta a ponta de dois sistemas computacionais (Kizza, 2005). As camadas estão divididas no formato de pilha, sendo o nível mais baixo o mais próximo da comunicação física, a transmissão de dados através do meio (ondas de rádio, cabo de fio de cobre, etc) e o nível mais alto, aquele de maior abstração, chamado de nível de aplicação, na qual o software de interação com o usuário está localizado. As camadas podem ser observadas na Tabela 2.1 com uma breve descrição de suas responsabilidades.

Dentre os diferentes tipos de rede disponíveis, as redes sem fio se destacam ao possibilitar maior mobilidade dos usuários desses sistemas computacionais. Por não necessitarem do uso de cabos, essas redes possuem uma larga aplicabilidade em ambientes dinâmicos, como por exemplo a disponibilização do acesso à internet em aeroportos, shopping centers e escritórios. Além do uso massivo pelos smartphones, essas redes também são a base para a conexão de dispositivos como eletrodomésticos, lâmpadas e sensores, formando a Internet das Coisas (do inglês, *Internet of things* - IoT), que se constitui por redes com grande quantidade de integrantes, sendo objetos físicos com interação com o mundo e conectados à internet. Para formação dessas redes temos como exemplo de tecnologias de rede sem fio para curto alcance o Bluetooth, o *Wireless Fidelity* (Wi-Fi) entre outras. A Tabela 2.2, baseada no trabalho de Yin et. al. (Yin et al.,

Tabela 2.1: Camadas do modelo OSI

Nível	Camada	Responsabilidade
7	Aplicação	Interação entre máquina-usuário
6	Apresentação	Transformação do formato de dados
5	Sessão	Gerência da comunicação entre *hosts* distintos
4	Transporte	Des-/fragmentação dos dados para envio
3	Rede	Transporte dos dados entre *hosts* da mesma rede
2	Enlace	Correção de erros e transmissão entre *hosts* diretamente conectados
1	Física	Execução física da transmissão de informação

2019), apresenta as características dessas tecnologias. As caraterísticas do Bluetooth, Wi-Fi, e da plataforma Google Nearby são descritas com mais detalhes a seguir.

Tabela 2.2: Características de redes sem fio

Característica	Tecnologia	
	Bluetooth 5.0	**Wi-Fi**
Alcance em ambiente interno (m)	40	< 50
Taxa máxima de transferência	2 Mbps	600 Mbps
Eficiência de energia	Alta	Baixa
Número de nodos	32 767	255
Presente em celulares	Sim	Sim

2.1.1 Padrão 802.11

O Instituto de Engenharia Elétrica e Eletrônica (do inglês, *Institute of Electrical and Electronics Engineers* - IEEE) é uma organização sem fins lucrativos, que tem como objetivo o avanço da tecnologia para beneficiar a humanidade. Para esse fim, ele atua publicando padrões técnicos, pesquisas científicas e, também, na organização de eventos científicos. O estudo de novos padrões e tecnologias ocorre através de grupos de trabalho, dentre os quais há o grupo 802, que estuda a comunicação em redes de área local (do inglês, *Local Area Network* - LAN), redes de área pessoal (do inglês, *Personal Area Network* - PAN) e redes de área metropolitana (do inglês, *Metropolitan Area Network* - MAN), sendo focado nas camadas física e enlace do modelo OSI (Gast, 2005). Seus subgrupos de pesquisa incluem o 802.3, que atua com protocolos de rede cabeada como o Ethernet, e o 802.11, que desenvolve especificações para redes de área local sem fio (do inglês, *Wireless Local Area Network* - WLAN) (Hiertz et al., 2010).

A primeira especificação do 802.11 foi publicada em 1997. Após sua adoção pelo mercado, o grupo de trabalho, em conjunto com a indústria, avaliou que muitos produtos não atendiam ao nível de compatibilidade que os usuários necessitavam. Por exemplo, frequentemente o esquema de encriptação padrão não funcionava entre dispositivos de fabricantes diferentes.

Essa ausência de homologação e certificação dos produtos levou à criação da aliança para compatibilidade entre redes ethernet sem fio (do inglês, *Wireless Ethernet Compatibility Alliance* - WECA) em 1999, a qual foi renomeada Aliança Wi-Fi (do inglês, *Wi-Fi Alliance* - WFA) em 2003, dando origem ao apelido Wi-Fi para o padrão 802.11 (Hiertz et al., 2010).

Na publicação inicial do 802.11, a camada física provê três soluções distintas: espectro de difusão em frequência variável (do inglês, *Frequency Hopping Spread Spectrum* - FHSS), sequência direta de espalhamento do espectro (do inglês, *Direct Sequence Spread Spectrum* - DSSS) na faixa de frequência de 2,4 GHz, além de uma configuração de camada física utilizando infravermelho na faixa de 316–353 THz. Os três modos possuem uma taxa básica de transferência de 1 Mb/s, além de um modo opcional de 2 Mb/s. De maneira similar ao padrão 802.3, a subcamada da camada 2 do modelo OSI, chamada de controle de acesso ao meio (do inglês, *Medium Access Control* - MAC), da versão básica do 802.11, utiliza a estratégia de "escutar antes de falar", conhecida como função de coordenação distribuída (do inglês, *Distributed CoordinationFfunction* - DCF). O padrão 802.11 utiliza acesso múltiplo com verificação de portadora com prevenção de colisão (do inglês, *Carrier Sense Multiple Access with Collision Avoidance* - CSMA/CA) em oposição ao modo de detecção de colisão utilizado no 802.3. Isso ocorre pois as colisões não podem ser detectadas em transmissões de rádio, fazendo com que o 802.11 aguarda por um intervalo de tempo antes de cada transmissão (Hiertz et al., 2010).

As redes 802.11 podem substituir as redes cabeadas ou estender o sinal transmitido por essas redes. A topologia básica de uma rede Wi-Fi consiste num conjunto básico de serviço (do inglês, *Basic Service Set* - BSS). O BSS é formado por um ou mais nodos conectados sem fio e que estabeleceram comunicações entre si. Em sua forma mais básica, esses nodos, também conhecidos como estações, comunicam-se uns com os outros diretamente, compartilhando a sua área de cobertura. Esse modo é chamado de modo ponto-a-ponto (do inglês, *Peer-to-Peer* - P2P). Além disso, um BSS também pode conter um Ponto de Acesso (do inglês, *Access Point* - AP), o qual tem como principal função conectar a rede sem fio com outra rede, cabeada ou sem fio. Diferente de um BSS simples, quando um AP está presente, todas as comunicações devem passar por ele (Cordeiro, 2003). O sucesso de mercado da tecnologia e as limitações encontradas no 802.11 original impulsionaram a criação de uma grande quantidade de extensões e melhorias. A Tabela 2.3, construída com base em (Omar et al., 2016) e (IEEE, 2016), apresenta de modo condensado as versões publicadas do padrão 802.11. No ano de 2007, foi publicada a segunda versão do padrão incluindo mudanças como do 802.11a e 802.11b, que aumentaram a taxa de transmissão, além de trazer o 802.11d, que adicionava especificações para operação em outros domínios regulatórios e contemplava as adições do 802.11i, melhorando a segurança do MAC, além de outras emendas. No ano de 2012, a terceira versão foi publicada contendo as melhorias para aumento na taxa de transferência através da emenda 802.11n. No ano de 2016, uma nova versão foi publicada, incluindo mudanças que aumentaram a taxa de transmissão e configurações com largura de canal maior, 80 Mhz ou 160 Mhz, do que os 40 Mhz especificados anteriormente.

As aplicações do Wi-Fi são bastante extensas devido à sua versatilidade. O uso mais comum é o modo infraestrutura, no qual o AP serve de conector para uma outra rede, geralmente com acesso à internet. Para essa configuração existem aplicações residenciais, hospitalares, industriais e também em pontos comerciais. No modelo P2P existem aplicações em redes veiculares *ad hoc* (do inglês, *Veicular Ad Hoc Network* - VANET)(Su et al., 2012). Outra aplicação em estudo é a utilização das ondas produzidas pelo Wi-Fi para sensoriamento dentro de uma residência (Jiang et al., 2018), ou em qualquer outro tipo de ambiente interno (Kotaru et al., 2015), com precisão de até 40 cm. O Wi-Fi também pode ser utilizado para estimar a densidade de pessoas em multidões utilizando os sinais de smartphones como proposto em (Schauer et al., 2014) e (Tang et al., 2018).

Tabela 2.3: Versões do padrão 802.11

Ano	**Emendas**	**Mudanças**
1997	versão base	-
2007	a, b, d, g, h, i, j, e	Camada física de alta velocidade nas bandas 2,4 e 5 Ghz
2012	k, r, y, w, n, p, z, v, u, s	Melhora na taxa de transferência, redes *mesh*
2016	ae, aa, ad, ac, af	Melhorias na taxa de transferência

2.1.2 Tecnologia Bluetooth

A tecnologia Bluetooth teve seu início em 1994, sendo desenvolvida pela empresa L. M. Ericsson. O nome da tecnologia foi uma homenagem para o Rei da Dinamarca Haroldo I (Zeadally et al., 2019). Haroldo, também designado por O Dente-Azul, representa a unificação da Dinamarca e, por esta relação, a tecnologia que tinha como objetivo unificar os dispositivos móveis foi batizada em sua homenagem. Em 1998, as empresas Ericsson, IBM, Intel, Nokia e Toshiba associaram-se e formaram o Grupo de Interesse Especial sobre Bluetooth (do inglês, *Special Interest Group* - SIG). Essa associação tinha como objetivo desenvolver e promover uma solução global para comunicação sem fio de curto alcance, tendo como foco os dispositivos de baixo poder computacional. Além disso, foi definido em sua criação o requisito técnico de utilizar a frequência na faixa de 2,4 GHz-2,4483 GHz (Bisdikian, 2001). Previsões do SIG indicam uma produção anual de mais de 1.9 bilhão de dispositivos com a tecnologia Bluetooth até o ano de 2024. Esses dispositivos possuem aplicações em áudio e entretenimento, indústrias e casas inteligentes (SIG, 2020b).

Após sua concepção, o Bluetooth era visto como uma tecnologia capaz de participar de maneira ubíqua da vida das pessoas através de dispositivos tecnológicos como celulares, computadores portáteis, dispositivos de localização parte do sistema global de posicionamento (do inglês, *Global Positioning System* - GPS) e assistentes Pessoais Digitais (do inglês, *Personal Digital Assistants* - PDA) - os precursores dos smartphones (Bruno et al., 2002). Um exemplo de aplicação pode ser visto no trabalho de Choi et. al., que implementa um sistema de monitoramento da saúde de um morador vivendo em uma casa completamente conectada à rede, chamada de

casa ubíqua pelos autores (Choi et al., 2004). Nessas casas há um grande número de sensores e automações que visam melhorar a qualidade de vida dos moradores. Essas moradias também são conhecidas como casas inteligentes. A aplicação do Bluetooth no uso de sensores pode ser vista evoluindo no trabalho de (Qi e Zhai, 2017), que utiliza o Bluetooth para incrementar as funcionalidades de pulseiras médicas provendo comunicação com outros dispositivos. O Bluetooth é frequentemente encontrado nos smartphones e outros dispositivos de uso pessoal como fones de ouvido, relógios inteligentes e similares. Ele está presente até mesmo em veículos, como apresentado em (Cheah et al., 2017).

O principal objetivo da especificação Bluetooth é garantir a interoperabilidade entre diferentes aplicações, suportando qualquer serviço e provendo os meios de implementação. Para garantir esse objetivo, a tecnologia utiliza conceitos já validados na área de redes, por exemplo durante a comunicação Bluetooth existem dois papéis: mestre e escravo. Para cada agrupamento de dispositivos comunicando internamente existe 1 dispositivo mestre, e até 7 dispositivos escravos. O equipamento mestre é responsável por decidir qual dispositivo escravo terá acesso ao canal. Os dispositivos que compartilham o mesmo canal, ou seja, estão conectados ao mesmo mestre, formam uma rede *piconet*. Essa estrutura é considerada o bloco básico de formação de redes Bluetooth. Na sua primeira versão, uma *piconet* tinha uma taxa de dados de 1 Mbps, sem considerar a degradação de desempenho devido aos mecanismos de controle. No Bluetooth, um dispositivo pode participar como mestre em apenas uma rede, porém pode assumir o papel de escravo em diversas redes. Dessa forma é possível realizar a construção de redes com mais de 7 dispositivos através dos escravos, que exercem o papel de ponte entre essas redes anteriormente independentes. Esse tipo de rede recebe o nome de *scatternet* (Bruno et al., 2002).

Em todas as suas versões, a tecnologia Bluetooth utiliza a faixa de frequência 2,4 Ghz-2,4483 GHz. Nessa faixa de frequência são definidas 79 frequências com espaçamento de 1 Mhz. A especificação determina a utilização de espectro de difusão em frequência variável (do inglês, *Frequency Hopping Spread Spectrum* - FHSS) como técnica de transmissão. No FHSS é estabelecida uma sequência única de saltos (do inglês, *hop*) para cada rede estabelecida. Ela é pseudo-aleatória e dita quais os saltos a serem realizados, tendo uma sequência de 79 saltos antes da repetição de frequência, sendo gerada utilizando o *clock* do dispositivo mestre e o endereço Bluetooth único de 48 bits desse mesmo dispositivo. A faixa de frequência utilizada por essa tecnologia é muito suscetível à interferências de sinal devido ao seu compartilhamento com outros dispositivos como fornos de micro-ondas e redes Wi-Fi. Com isso, a utilização da técnica FHSS provê mais robustez para as comunicações ao evitar interferências na camada física de conexão (Bruno et al., 2002).

A Tabela 2.4, baseada no trabalho de Collota et al (Collotta et al., 2018), apresenta uma comparação entre o Bluetooth clássico e algumas versões recentes (4.x e 5). É possível constatar que houve uma diminuição muito grande na latência da comunicação, passando de um limite superior de 100 ms para um limite superior de 3 ms. Outro ponto interessante é o alcance dos dispositivos que passou de no máximo 100 metros para até 200 metros, demonstrando a evolução

na performance da tecnologia. A quantidade de nós participando da troca de dados (nós ativos) aumentou, criando assim, a possibilidade de redes maiores, e, além disso, o Bluetooth 5 também introduziu o suporte nativo a redes de malha (do inglês, *mesh networks*) que pode ser combinado com versões anteriores a partir da 4. As redes em malha possibilitam a comunicação muitos para muitos entre os dispositivos, sendo considerada um passo importante na adoção do Bluetooth para um contexto de Internet das Coisas (Yin et al., 2019).

Tabela 2.4: Diferenças entre as versões do Bluetooth

Característica	Tecnologia		
	Bluetooth Clássico	**Bluetooth 4.x**	**Bluetooth 5**
Alcance (m)	Até 100	Até 100	Até 200
Taxa nominal de dados (Mbps)	1-3	1	2
Latência (ms)	< 100	< 6	< 3
Nós ativos	7	Ilimitado	Ilimitado
Tamanho da mensagem (bytes)	Até 358	31	255

2.1.3 Tecnologia de conexão - Google Nearby

Além das tecnologias que estabelecem a comunicação entre dois dispositivos computacionais, existem ferramentas para unir diversas dessas tecnologias. Essa união permite o uso dos pontos fortes de cada tecnologia, como maior alcance ou taxa de transmissão de dados, sem a necessidade de implementação e configuração especificas para cada projeto. Dessa forma, essas ferramentas facilitam o desenvolvimento de *software* que utilize diversas tecnologias de comunicação. No contexto de dispositivos móveis, tais como smartphones, *notebooks*, entre outros, a comunicação direta entre os dispositivos possui um interesse adicional devido à mobilidade desses aparelhos. Com o objetivo de facilitar o desenvolvimento de aplicativos que utilizem esse conceito de rede, a empresa Google, mantenedora do sistema operacional Android, criou a plataforma *Google Nearby* (Google, 2021b), que possui funcionalidades para facilitar a implementação desse tipo de comunicação nos aplicativos para smartphones. Essa plataforma disponibiliza rotinas e funcionalidades de código através de uma interface de programação de aplicação (do inglês, *Application Programming Interface* - API) para descoberta e comunicação entre dois ou mais dispositivos próximos utilizando Bluetooth, Wi-Fi, entre outras estratégias. Existem três APIs diferentes - *Fast Pair*, *Nearby Messages*, *Nearby Connections* - na plataforma, as quais se propõem a contribuir em contextos de uso diferentes. O *Fast Pair* permite uma conexão Bluetooth mais simples e rápida entre periféricos e smartphones no que tange a experiência do usuário. O *Nearby Messages* é uma API que utiliza o esquema de Publicadores e Assinantes (do inglês, *Publish and Subscribe*) para transferir mensagens através de um misto entre Bluetooth e internet para dispositivos que estão próximos fisicamente. Essa é a única API dentre as três que está disponível para os sistemas operacionais Android e IOs. O terceiro pacote de código

é o *Nearby Connections*, que permite a descoberta, conexão e comunicação bidirecional de dispositivos próximos sem o uso da internet sendo adequado para construção de redes *ad hoc*.

A API do *Nearby Connections* utiliza as tecnologias Bluetooth e *Wi-Fi Direct* de maneira transparente para o desenvolvedor, escolhendo aquela que se adeque à situação do dispositivo. As conexões entre os dispositivos possuem banda larga, latência baixa e são criptografadas (Google, 2021c). Essa API permite três estratégias de formação da rede. A primeira estratégia é a formação ponto a ponto, que permite que um smartphone se conecte a apenas um dispositivo, 1-1, dessa forma proporcionando maior largura de banda (Google, 2021d). A estratégia denominada estrela permite a conexão no estilo de rede estrela, na qual um dispositivo se conecta com N outros. Nessa configuração o dispositivo pode apenas atuar em um dos papéis por vez. A terceira estratégia é o modo *cluster*, que permite a conexão do dispositivo para M dispositivos próximos e que ele receba conexão de N outros dispositivos. Essa estratégia utiliza apenas a tecnologia Bluetooth para construção da rede e resulta em velocidades menores de conexão, porém com maior flexibilidade de topologia.

2.2 CONFIANÇA EM REDES

A confiança faz parte das relações entre as pessoas, sendo um componente da vida em sociedade. Nesse contexto, os indivíduos interagem continuamente entre si devido à expectativa de resultados positivos de suas interações (Yamamoto, 1990). Confiança é uma relação estabelecida entre duas entidades, como por exemplo pessoas, para uma determinada ação. Em particular, uma entidade confia na outra para performar uma ação, e assume um risco de perdas caso sua análise de confiança esteja incorreta (Sun et al., 2005) (Cho et al., 2015). A confiança não é simétrica, o fato de que A confia em B para determinada ação não significa que B confia em A, onde A e B são entidades (Sun et al., 2005). Portanto, a colaboração é uma consequência da confiança presente nas relações interpessoais. Além disso, a ocorrência de cooperação entre duas pessoas fortalece o relacionamento e a possibilidade de novas colaborações futuras, gerando um círculo virtuoso de benefício mútuo baseado na confiança (Cho et al., 2015). Assim sendo, o conceito de confiança também pode ser aplicado no contexto de comunicação entre dispositivos computacionais para auxiliar nas tomadas de decisão.

A utilização da confiança em contextos computacionais também pode auxiliar na tomada de decisão quando não há conhecimento completo do domínio do problema. Nesses cenários, decisões críticas ocorrem em meio à informações incertas, incompletas e conflitantes. Para isso, existem diversos critérios que podem ser utilizados para avaliar e classificar os dispositivos existentes na rede. Essas avaliações podem ser feitas por observação direta, quando o avaliador está em contato direto com o dispositivo avaliado, ou de maneira indireta, através da recomendação de outros dispositivos. A qualidade do serviço, por exemplo, é um fator importante em serviços de roteamento, que podem utilizar a observação direta para avaliação. Nesses casos, o tempo de resposta e taxa de perda de pacotes são medidas auxiliares para determinar a confiança de

um servidor em relação à chance de sucesso na realização de determinada tarefa por parte do nó avaliado. Em redes de informação, aquelas que constituem serviços de compartilhamento de informação, existem outros critérios de avaliação aplicáveis, que podem incluir confiança com relação ao conteúdo da informação, através da verificação de credibilidade, veracidade e integridade do avaliado. Por outro lado, nas redes de interação social, aquelas baseadas nas relações entre os seres humanos, as características analisadas podem ser a reputação e a recomendação de determinada pessoa, por exemplo. Nesse caso, a avaliação de confiança com relação à uma informação recebida pode utilizar os laços sociais, prestígio ou semelhança entre as pessoas que trocam mensagens. Nesses contextos, a análise de confiança pode considerar diferentes domínios do problema, modelando-a como um atributo multifatorial que auxilia na tomada de decisão. Entretanto, a confiança não oferece segurança suficiente para garantir ausência de risco (Cho et al., 2015) (Sun et al., 2005) (Batista, 2019).

2.3 COMUNIDADES DE INTERESSE

As pessoas geralmente relacionam-se a partir de interesses comuns mantidos ao longo do tempo ou mesmo por oportunidade, como quando se encontram em um mesmo ambiente, por exemplo. Nessas condições, alguns desses interesses contribuem para reunir as pessoas em grupos, dentro dos quais elas podem trocar informações com mais facilidade e com alguma privacidade, devido à confiança existente entre si. Ademais, esses agrupamentos ou comunidades formados com base nos interesses em comum dos seus participantes podem servir como base para formação de agrupamentos de dispositivos de rede (Batista, 2019). Nessas redes, a relação entre os usuários é um fator determinante para o estabelecimento de conexão e troca de mensagens. Dessa forma, é possível estimar o grau de confiança existente entre esses usuários, e utilizar essa informação como auxílio para determinar quais informações podem ser compartilhadas com integrantes de um grupo.

O agrupamento de dispositivos pode ser feito através da classificação dos interesses de seus usuários como por exemplo gosto musical, profissão ou passatempos. Esses agrupamentos são chamados de comunidades de interesse (do inglês, *Community of Interest* - CoI) (Chakraborty et al., 2017). Através dessa classificação em comunidades, os integrantes da rede podem avaliar e se comunicar com os dispositivos úteis ao seu propósito, mesmo sem conhecer características específicas de cada um. Além disso, em redes móveis, a mobilidade dos usuários pode ser analisada através do histórico das diferentes configurações de suas comunidades ao longo do tempo, pois são formadas e mantidas de acordo com a posição e movimentação de cada dispositivo de rede (Batista, 2019).

As comunidades estabelecidas no mundo real podem ser classificadas em quatro tipos, que são apresentados na Figura 2.1, baseada no trabalho de (Chakraborty et al., 2017) - não sobrepostas, sobrepostas, hierárquicas e locais, de acordo com as relações entre os membros e as próprias comunidades. Conforme ilustra a Figura 2.1a, as comunidades não sobrepostas

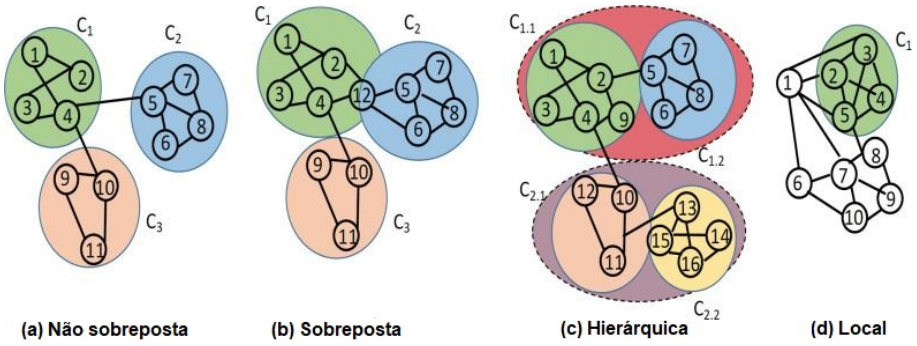


Figura 2.1: Categorias de comunidades de interesse.

são aquelas nas quais um dispositivo, ou nodo, participa de apenas uma comunidade, por exemplo, estudantes cursando somente um curso de graduação na universidade. Assim sendo, nas comunidades sobrepostas, representadas na Figura 2.1b, um nodo pode participar de múltiplas comunidades - matérias cursadas por estudantes da graduação, por exemplo. A classificação do tipo hierárquica é exemplificada pela Figura 2.1c, essa classificação refere-se as comunidades que possuem contextos a partir dos quais os grafos podem ser analisados em diferentes níveis, como as células do corpo que formam tecidos e esses, por sua vez, formam órgãos. As comunidades locais, apresentadas na Figura 2.1d, não apresentam uma estrutura quando vistas globalmente, mas possuem aspectos e configurações próprias dentro do seu contexto (Chakraborty et al., 2017).

2.4 RESUMO

Este capítulo apresentou técnicas de comunicação utilizadas na formação de redes de computadores. Além disso, também retratou o conceito de agrupamento de dispositivos em comunidades dinâmicas mediante interesses em comum, as chamadas comunidades de interesse, indicando a viabilidade de uso desse mecanismo em ambientes dinâmicos, como a IoT. A garantia da segurança dos dados no contexto de serviços de saúde mostrou-se de grande relevância, dado o seu impacto na vida das pessoas, especialmente quando em situações de emergência.

3 TRABALHOS RELACIONADOS

Nesse capítulo são apresentados trabalhos relacionados aos conceitos de confiança, contribuição colaborativa (*crowdsourcing*), atendimento em saúde e situações de emergência aplicados ao contexto dos dispositivos móveis. A Seção 3.1 discorre sobre um trabalho relacionado ao atendimento preventivo em saúde. A Seção 3.2 apresenta uma ferramentas para dispositivos móveis que auxilia no atendimento em situações de desastres naturais, utilizando redes *ad hoc*. A Seção 3.3 apresenta um trabalho que propôs uma arquitetura genérica para serviços descentralizados de recomendação. A Seção 3.4 apresenta trabalhos que utilizem o conceito de confiança em sistemas computacionais.

3.1 SERVIÇO DE SAÚDE

O trabalho de Kowatchs et al. (Kowatsch et al., 2017) propôs a aplicação MobileChat para a plataforma de código aberto para intervenções digitais MobileCoach[1]. Essa plataforma tem como objetivo criar sistemas inteligentes e totalmente automatizados para intervenções digitais e permitir estudos e avaliações dessas intervenções (Filler et al., 2015). Devido à sua estrutura modular e extensível, bem como seu formato de código aberto, plataforma MobileCoach pode ser aplicada em diversos contextos de mudança de comportamento, como, por exemplo, no design e avaliação de sistemas de intervenção digital para interrupção do uso do cigarro (Castro et al., 2017) ou até mesmo para a mudança de traços de personalidade (Stieger et al., 2021). A abordagem proposta pelos autores consiste em uma aplicação para dispositivos Android, que mitiga problemas na comunicação entre os voluntários e os pesquisadores que utilizem a plataforma MobileCoach. Para esse fim, a aplicação MobileChat não utiliza mensagens de conteúdo livre através do Serviço de Mensagens Curtas (do inglês, *Short Message Service* - SMS), como utilizado anteriormente pela plataforma. Em seu lugar, mensagens pré-configuradas são disponibilizadas para seleção do usuário, conforme apresenta a Figura 3.1. As mensagens de texto aberto dificultam a análise e classificação em escalas, necessitando de intervenção manual caso o usuário envie algum dado não compreendido pelo sistema. Além disso, em determinados casos, o usuário necessita de informações e respostas que apenas um operador humano poderia entregar, para esses casos, o MobileChat possui um canal dedicado de comunicação com humanos que podem ser os próprios pesquisadores, profissionais especializados no domínio da ação ou assistentes do estudo, conforme ilustra a Figura 3.2. Essa aplicação também provê informações contextuais do usuário, coletadas através dos sensores do smartphone, tornando o estudo mais completo e confiável. Portanto, através da melhoria de comunicação e captação de mais dados, esse sistema contribui para a execução de pesquisas sobre comportamento e a atuação de

[1]Site da plataforma: https://www.mobile-coach.eu/

profissionais de saúde nesses estudos. Na avaliação com onze adolescentes, realizada pelos autores, não foram encontrados pontos críticos de falha na usabilidade e experiência do usuário, tendo uma avaliação positiva nos quatro pontos observados.

Figura 3.1: *Chatbot* com opções de resposta pré-definidas (Kowatsch et al., 2017)

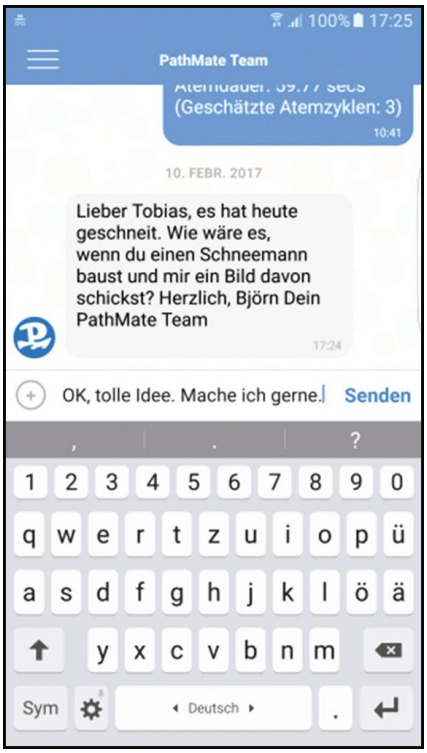


Figura 3.2: Canal de comunicação com o assistente do estudo (Kowatsch et al., 2017)

No contexto de intervenções digitais é primordial que o usuário interaja com as mensagens recebidas, independente do meio pelo qual ela foi enviada. No caso de intervenções em smartphones, essa comunicação pode ocorrer, por exemplo, através de mensagens SMS ou por notificações disponibilizadas pelo sistema operacional, as chamadas notificações *push*. Para melhorar a efetividade das intervenções, o contexto deve ser avaliado para decisão referente ao conteúdo da notificação e o seu potencial de interação com o usuário. Para esse fim, o trabalho de Künzler (Künzler, 2019) avaliou de maneira preliminar a combinação de sistemas de gerenciamento de notificação sensível ao contexto (do inglês, *context-aware notification management system* - CNMS) com o arcabouço de intervenções adaptativas "bem na hora" (do inglês, *Just-in-time adaptive intervention* - JITAI). No JITAI, as intervenções são personalizadas para o usuário e o contexto no qual ele está inserido. Entretanto, essas notificações com conteúdo personalizado ainda dependem da interação do usuário com seu smartphone para leitura ou execução de determinada ação. Assim sendo, o envio de notificações no momento de maior probabilidade de leitura é vital para o sucesso da mesma e, a utilização de CNMS pode aumentar a taxa de leitura e o tempo de resposta para as intervenções programadas. O estudo averiguou que o sistema operacional do aparelho tem uma relevância estatística para predizer o tempo de leitura e taxa de resposta das notificações, os dados indicaram que usuários do sistema Android

interagem mais. Além disso, traços de personalidade como de usuários neuróticos, por exemplo, indicam uma taxa de resposta maior e, quando o dispositivo está com a bateria cheia, os usuários tendem a não responder.

3.2 SERVIÇO DE EMERGÊNCIA

A tese de Álvarez (Álvarez, 2020) discute a comunicação segura nas redes dispositivo-dispositivo para situações de emergência, avaliando ferramentas e métodos que podem auxiliar a sociedade civil em caso de desastres naturais. Os sistemas de comunicação mais comuns, como internet e rede telefônica, dependem fortemente de uma infraestrutura existente e sua segurança é fornecida pelo provedor da rede. Comumente, esses sistemas são projetados de maneira centralizada visando atender bilhões de usuários simultâneos. Porém, caso ocorra alguma degradação ou interrupção no fornecimento desses serviços devido à sobrecarga, desastre natural, interrupção no fornecimento de energia elétrica ou até censura no país, os usuários ficam sem opções práticas para estabelecer comunicações seguras entre seus dispositivos móveis. Após casos de desastres naturais é comum ocorrer a perda da capacidade de telecomunicação nas regiões afetadas e, em decorrência da grande interdependência nas infraestruturas críticas, a interrupção na comunicação pode impor restrições em tarefas cotidianas como comprar combustível, alimentos e água, por exemplo. Nesse contexto, de acordo com Álvarez (Álvarez, 2020), a formação de MANETs auto-organizadas utilizando smartphones como componentes é adequada devido à sua flexibilidade. Essas redes são adaptáveis e permitem a comunicação dispositivo-dispositivo sem a necessidade de infraestrutura disponível. Além disso, devido à mobilidade humana, torna-se possível a troca de mensagens de maneira oportunista através de dispositivos intermediários, aumentando o alcance das mensagens compartilhadas na rede.

O processo de avaliação de soluções para cenários de desastres naturais enfrenta uma grande barreira devido à natureza desses eventos (Álvarez, 2020). Devido à natureza dos cenários, as soluções são avaliadas e validadas através de simulações virtuais, que representam os eventos que ocorrem durante desastres naturais. Porém, Álvarez (Álvarez, 2020) executou uma avaliação através de um cenário simulado de desastre natural com a participação de voluntários. Dessa forma, o autor pôde analisar de maneira mais precisa o efeito das interações humanas nas MANETs aplicadas em cenários de ausência de infraestrutura de comunicação. Para isso, o autor implementou uma aplicação para dispositivos Android com funcionalidades relevantes em um contexto de desastre, conforme apresentado na Figura 3.3. A aplicação utilizava uma estratégia de comunicação P2P e permitia o envio de mensagens de socorro através da funcionalidade "*SOS Emergency Message*". Além dessa funcionalidade, também havia o envio de notificação de vida ("*I am alive notification*"), serviço de localização de pessoa ("*Person-Finder*"), troca de mensagens, visualização de notícias e por fim uma funcionalidade de divulgação e requisição de suprimentos ("*Resource Market Registry*"), todas apresentadas na Figura 3.3. O teste de campo ocorreu em conjunto com autoridades locais envolvendo 125 participantes em três vilas na

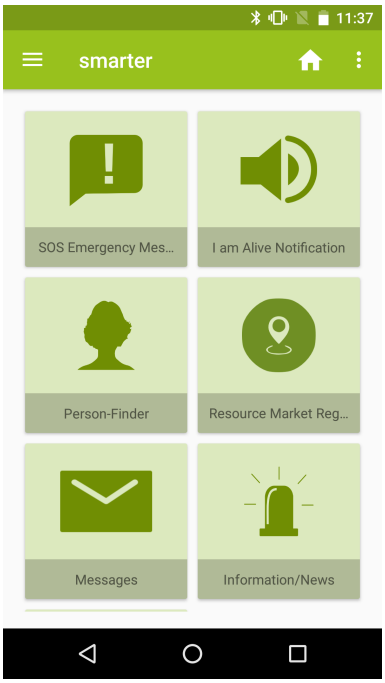


Figura 3.3: Funcionalidades da aplicação utilizada na avaliação de comportamento em um cenário de desastre (Álvarez, 2020)

Alemanha, conforme demonstrado na Figura 3.4. Ao longo de um dia, os participantes seguiram um roteiro de locomoção e atividades em um cenário fictício de desastre ocorrido em duas das vilas. A partir da execução desse cenário, o autor registrou métricas de interesse para seu caso de uso como a mediana da distância entre dois dispositivos conectados foi de 30,21 m. A velocidade média dos participantes do estudo foi de aproximadamente 0,5 km/h, e o número médio de vizinhos para um raio de 44 metros foi de 7,26. Nesse cenário, a maior parte das conexões durou 100 segundos devido à forma de movimentação dos participantes, que se locomoviam em pequenos grupos. Assim, o trabalho trouxe novos dados para análise de MANETs aplicadas em cenário de desastre, e, de maneira mais próxima à um cenário real ao considerar como as interações e comportamentos humanos podem afetar o funcionamento da rede.

Figura 3.4: Mapa do cenário utilizado para avaliação de uma MANET em cenário de desastre (Álvarez, 2020)

3.3 SERVIÇO DESCENTRALIZADO

O trabalho de Beierle e Eichinger (Beierle e Eichinger, 2019) propõe uma arquitetura genérica para serviços descentralizados de recomendação utilizando a proximidade de localização dos usuários para propagação dos dados. Os autores argumentam que os algoritmos centralizados de recomendação, como os utilizados pelos serviços de streaming, tais como Spotify, Netflix, entre outros, podem ser tendenciosos no seu algoritmo de recomendação, priorizando recomendações que proporcionem a maior margem de lucro para o seu negócio. Além desse conflito de interesses, também há a possibilidade do efeito de aprisionamento tecnológico (do inglês, *lock-in effect*), o que ocorre quando os provedores serviços projetam seus produtos para manter e fidelizar sua clientela, dificultando a mudança de provedor. Nesse cenário, a utilização de um sistema descentralizado de recomendação pode evitar esses efeitos (Beierle e Eichinger, 2019).

A arquitetura para serviços descentralizados de recomendação baseada na proximidade dos usuários proposta pelos autores Beierle e Eichinger é composta pelos componentes *Coleta de Dados*, *Sistema de recomendação* e *Troca de Dados*, que podem se conectar com outros sistemas para executar suas tarefas. O componente *Coleta de dados* representa a integração com um sistema que seja capaz de reunir informações acerca de uma entidade avaliada. Essa integração pode ser realizada com sensores de um smartphone (coletando informações de localização, uso do aparelho e outras), através de integração com um serviço externo, ou ainda através da interação com o próprio usuário. O componente *Sistema de recomendação* é responsável por utilizar todos os dados disponíveis para recomendar itens ao usuário. Na especificação do componente *Troca de dados*, a arquitetura permite que os usuários troquem avaliações de maneira automática, expandindo sua base de dados com as opiniões de outros usuários ao longo do tempo. Para esse fim, os autores avaliaram diferentes estratégias com três pontos teóricos do que seria uma solução ótima em mente. Em primeiro lugar, nessa solução ótima, a transferência de dados acontece sem interação do usuário. O segundo ponto é que a solução deve ser multiplataforma para trabalhar com o sistema operacional Iphone (do ingles, *Iphone Operating System* - iOS) e Android, os dois sistemas operacionais de smartphones que juntos compõem 99% do mercado. E, por último, essa solução deve ser capaz de enviar mensagens grandes contendo as preferências do usuário.

A partir da avaliação realizada, Beierle e Eichinger (Beierle e Eichinger, 2019) encontraram soluções que atendem com 2 dos três requisitos, par a par, e, por fim, propuseram uma arquitetura que atenda os três requisitos. Essa arquitetura utiliza um sistema remoto de armazenamento de dados (DropBox, GoogleDrive), e o *Google Nearby Messages* para transmissão de um endereço na internet, através do qual os dispositivos podem baixar os dados de avaliação e preferência uns dos outros. Com estratégia proposta, é possível enviar pequenas mensagens utilizando um mecanismo multiplataforma e que necessita de interação do usuário apenas para configuração do seu serviço de armazenamento em nuvem. Para o sistema de recomendação, os autores Beierle e Eichinger propuseram duas abordagens que podem mitigar a ausência de uma grande massa de dados para cálculo das recomendações. A primeira estratégia

consiste em disseminar dados de outros usuários que tenham interesses parecidos com o dos usuários conectados. Dessa forma, quando um novo dispositivo conecta-se à rede, o problema de "inicio frio", quando não existem dados no ínio da operação do sistema, é mitigado e, além disso, a propagação de dados torna-se mais rápida entre os usuários. A segunda estratégia apresentada pelos autores é baseada na proximidade dos usuários para cálculo de similaridade dos interesses das pessoas, sem necessariamente possuírem avaliações semelhantes. Em síntese, os três componentes que formam a arquitetura estabelecem a base para criação de um sistema de recomendação descentralizado que atenda aos três requisitos do sistema ótimo.

3.4 CONFIANÇA EM SISTEMAS COMPUTACIONAIS

A confiança pode ser aplicada de diferentes maneiras em sistemas computacionais. Por exemplo, o trabalho de Jiang et al. (Jiang et al., 2019) propôs uma abordagem baseada em confiança para a filtragem em um algoritmo de recomendação para *e-commerce*. Além de possibilitar o acesso à mais opções para o cliente, a expansão de serviços de venda online, *e-commerce*, causou um efeito de sobrecarga de informação nesses consumidores. Para encontrar rapidamente os seus produtos preferidos dentro de uma infinidade de possibilidades, os usuários estão ávidos por tecnologias que recomendem produtos relevantes para si. Esse contexto motiva o desenvolvimento de algoritmos para recomendação. Em especial, há um desafio no desenvolvimento de algoritmos de filtragem colaborativa devido a sua complexidade e dificuldade de implementação. A filtragem colaborativa é uma técnica de sistemas de recomendação que utiliza a opinião e avaliação de diversos usuários para predizer as preferências dos seus clientes, dessa forma, produzindo uma recomendação com maior potencial de agradar o cliente e gerar uma venda. Nesse contexto, os autores apresentaram uma abordagem com maior acurácia do que a utilização do algoritmo *Slope One* ao combinar seu funcionamento com dados confiáveis e a similaridade de usuários. Nesse caso, a inovação do trabalho consiste em utilizar uma avaliação de confiança com relação aos comentários dos usuários. No sistema da empresa Amazon, os usuários podem selecionar de zero a cinco estrelas para classificar um produto e outros usuários podem registrar se determinada avaliação foi útil ou não. Assim sendo, os autores combinaram essas informações através de um método de cálculo para validar se as avaliações de determinado produto são confiáveis ou não. Com isso, em cenários onde a confiança com relação as avaliações era maior do que 0.8, sendo 1 o valor máximo, o algoritmo proposto atingiu uma acurácia na predição maior do que o algoritmo tradicional (Jiang et al., 2019).

O trabalho de Fang et al. (Fang et al., 2020) utiliza o conceito de confiança aplicado em IoT. Nesse trabalho os autores propuseram um sistema de segurança baseado em confiança para coleta de dados em cidades inteligentes. O avanço da IoT apresenta diversas oportunidades de desenvolvimento para cidades inteligentes. Durante esse processo, a coleta de dados é um ponto crucial para o bom funcionamento dos sistemas devido ao seu impacto. Esses dados podem contribuir para a implantação de políticas públicas efetivas e eficientes. Entretanto, muitos

sensores são alocados em locais sem acompanhamento, como por exemplo sensores de nível de água ou sensores de iluminação em sistemas de iluminação inteligente. Nesse casos, os dados podem ser espionados ou adulterados por um agente hostil. Esses dados incorretos podem impactar severamente a acurácia da análise e, posteriormente, a tomada de decisão. Enquanto isso, sistemas complexos de segurança não podem ser implementados nesses sensores devido às restrições de armazenamento e capacidade computacional. Nesse contexto, o trabalho utiliza um sistema de avaliação de confiança com base no histórico de interações entre os nós da rede para identificar nós não cooperativos. A cada interação entre os nós, o valor numérico que representa a confiança é recalculado. O sistema foi avaliado em uma simulação, e mostrou-se capaz de resistir à ataques do tipo *On-Off*, quando os nós maliciosos alternam entre períodos de cooperação e não cooperação, dificultando sua detecção. Além disso, constatou-se que ele é eficiente com relação ao uso de energia e o nível de segurança alcançado, quando comparado à outras abordagens.

3.5 RESUMO

Este capítulo apresentou trabalhos relacionados, através dos quais constatou-se a importância de sistemas que auxiliem nos atendimentos de saúde. Em especial, foi apresentado um trabalho que auxilia em casos de desastres naturais utilizando uma abordagem descentralizada. Dessa forma, facilitando a comunicação entre as pessoas mesmo durante a ausência de infraestrutura para telecomunicação. Além disso, foram apresentadas as vantagens de uma comunicação descentralizada e uma proposta de arquitetura genérica para sistemas de recomendação que utilizem essa estratégia. Por fim, foram apresentados estudos que utilizam a confiança como auxílio para tomada de decisão em diferentes contextos.

4 MOBANGELO: UMA FERRAMENTA PARA AUXÍLIO NA ASSISTÊNCIA EMERGENCIAL EM AMBIENTES URBANOS

Este capítulo apresenta a ferramenta MobAngelo, desenvolvida para auxiliar na tomada de decisões em situações emergenciais de saúde em ambientes urbanos, fora da infraestrutura hospitalar. Essa ferramenta tem por objetivo reduzir o tempo entre a ocorrência de um evento crítico de saúde e o primeiro atendimento, contribuindo para um aumento da chance de sobrevivência do paciente. A Seção 4.1 apresenta as especificações técnicas da ferramenta, descrevendo o modelo de rede utilizado para comunicação entre os integrantes da rede e detalhando a arquitetura do sistema e seus componentes. A Seção 4.2 explica o modelo de confiança social utilizado na comunicação da redes, enquanto que a Seção 4.3 detalha o funcionamento do sistema, sua operação e suas funcionalidades.

4.1 VISÃO GERAL

O MobAngelo é uma aplicação para dispositivos smartphones que utilizam o sistema operacional Android. Ele atua de maneira distribuída na formação de uma rede de dispositivos, que trocam informações sobre si e seus usuários, para que em caso de evento crítico de saúde, um dos integrantes da rede possa auxiliar o outro. A aplicação é baseada no mecanismo para disseminação de dados sensíveis baseado em confiança social STEALTH (Batista, 2019). O MobAngelo é implementado através das linguagens Kotlin e Java, que são as mais comuns para desenvolvimento de aplicações para a plataforma Android, e recomendadas pela Google, a mantenedora da plataforma. Além disso, a linguagem Kotlin oferece uma sintaxe mais concisa e segura com relação à Java, sem perder as bibliotecas e referências desta, devido à interoperabilidade das duas linguagens. Logo, o uso desses recursos facilita a compreensão de outros desenvolvedores, acostumados com a linguagem Java, para com o código fonte do MobAngelo. O sistema é compatível com dispositivos que possuam sistema operacional Android a partir da versão 7.0 (apelidada Nougat). A tecnologia Bluetooth é utilizada na comunicação entre os dispositivos da rede devido à sua presença massiva em smartphones da atual geração (SIG, 2020a). Essa tecnologia permite a identificação de dispositivos próximos, e a conexão direta entre eles sem a necessidade de interação do usuário.

4.1.1 Modelo de Rede e Comunicação

A disseminação de dados sensíveis, em ambientes dinâmicos e *Zero-Knowledge*, exige a existência de uma rede capaz de lidar com as características desse contexto. Essas características incluem a mobilidade dos nós da rede, a ausência de informações históricas para analisar o comportamento desse nó, entre outros desafios já apresentados. Para tal, o

MobAngelo implementa o modelo de rede do STEALTH (Batista, 2019). Nesse modelo, as comunicações são executadas entre dispositivos portáteis interligados numa rede sem fio, os quais possuem a capacidade de agrupar dispositivos e disseminar dados. Cada dispositivo possui um identificador exclusivo (Id), no caso do MobAngelo é o seu endereço MAC da interface Bluetooth. Além disso, cada dispositivo possui um atributo individual de confiança referente ao conjunto de competências $S_n = \{s_1, s_2, s_3, \ldots, s_z\}$, tal que $|S_n| \neq 0$ e $S_n \subset S$, onde S é conjunto de todas as competências (Batista, 2019). As competências representam a capacidade ou o conhecimento em atendimentos de saúde. Cada dispositivo também possui um conjunto de interesses $I_n = \{i_1, i_2, ..., i_z\}$, tal que $|I_n| \neq 0$ e $I_n \subset I$, onde I é o conjunto de todos os interesses (Batista, 2019). Um interesse é um passatempo, ocupação ou gosto do usuário daquele dispositivo, por exemplo música, esportes ou filmes. Os dispositivos agrupam-se por interesses em comum, formando comunidades durante um intervalo de tempo. Por simplicidade, o mecanismo STEALTH assume que todos os nós apresentam um comportamento não malicioso, sendo desconsiderada a ocorrência de ataques ao funcionamento do sistema (Batista, 2019). As comunidades formadas são sobrepostas, pois cada dispositivo pode participar de diversas CoIs diferentes simultaneamente, e sua formação e manutenção estão associadas à movimentação dos dispositivos no ambiente. Quando os dispositivos se aproximam, ocorre a troca de informações e a formação da comunidade, que é desfeita quando eles se afastam e perdem a conexão entre si.

4.1.2 Arquitetura

A arquitetura de implementação do MobAngelo baseia-se na arquitetura do modelo STEALTH, proposta em (Batista, 2019). Essa arquitetura, conforme apresentado na Figura 4.1 baseada em (Batista, 2019), possui dois módulos: (*i*) **Gestão de comunidades**, que cria e realiza a manutenção das comunidades de interesse a partir dos dispositivos presentes na sua vizinhança, e computa a confiança com relação aos vizinhos; e (*ii*) **Gestão de eventos críticos**, que controla e dissemina os dados em caso de emergência, escolhendo para qual dispositivo deve ser enviada uma mensagem de alerta.

4.1.3 Gestão de Comunidades

O módulo *Gestão de Comunidades*, apresentado na parte superior da Figura 4.1, é responsável por coordenar a formação das comunidades através da identificação de vizinhos e cálculo da confiança. Esse processo ocorre através das mensagens de identificação, que contém a competência e os interesses do dispositivo. Esse módulo também é responsável pela identificação do dispositivo em face de outros dispositivos que estejam executando a formação das suas próprias comunidades. Ele é composto por cinco componentes: o componente *Interesses* é responsável por avaliar os interesses recebidos na mensagem de identificação e identificar os interesses em comum. O componente *Competência* lida com a competência recebida na mensagem, identificando-a de acordo com as competências configuradas pela aplicação. O

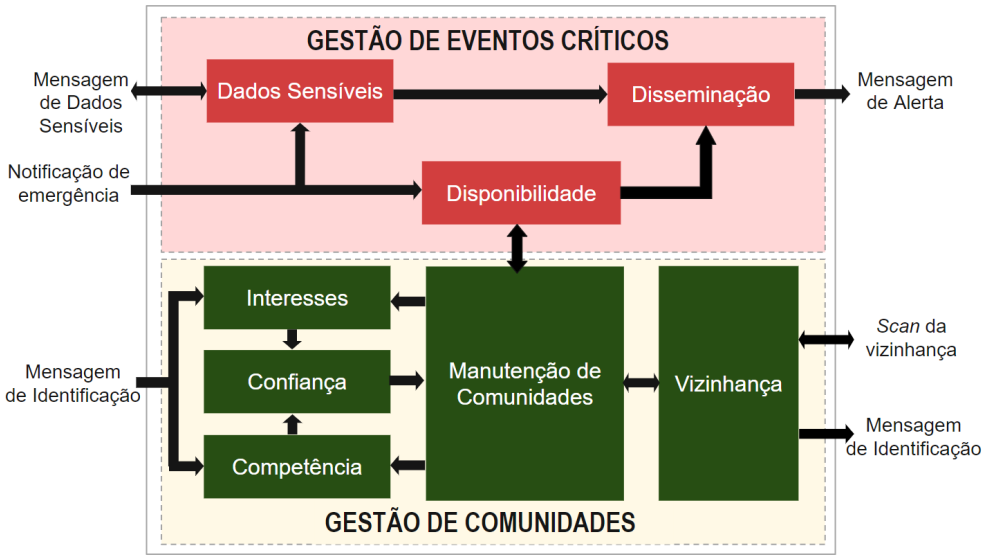


Figura 4.1: Arquitetura do MobAngelo

componente *Confiança* é encarregado de, utilizando as informações dos módulos anteriores, calcular a confiança com relação ao dispositivo que está sendo identificado para determinar dentre os atuais integrantes da comunidade qual é o mais confiável. O componente *Vizinhança* realiza um *scan* Bluetooth da sua vizinhança para identificar os dispositivos próximos. Na sequência ele se conecta a cada um dos dispositivos e recebe uma mensagem de identificação. Ele também é o responsável por enviar a mensagem de resposta aos pedidos de identificação de outros dispositivos. o componente *Manutenção de Comunidades* gerencia a criação e dissolução das CoIs ao longo do tempo, assegurando que as CoIs contemplem as mudanças nas redes locais.

4.1.4 Gestão de Eventos Críticos

O módulo *Gestão de Eventos Críticos*, presente na parte inferior da Figura 4.1, coordena o fluxo da aplicação durante eventos críticos. A notificação de emergência ocorre através de uma interação do usuário, ao pressionar um botão, sinalizando a ocorrência de um evento crítico de saúde. O componente *Dados Sensíveis* armazena os dados sensíveis da pessoa e é responsável por certificar a sua disseminação apenas nos momentos de emergência. O componente *Disponibilidade* é responsável por verificar, dentre a comunidade atual, qual é a pessoa mais adequada para receber a mensagem de emergência. O componente *Disseminação* coordena o envio dessa mensagem, que contém os dados sensíveis e o aviso de emergência, para a pessoa selecionada pelo componente *Disponibilidade*.

4.2 AVALIAÇÃO DE CONFIANÇA ENTRE DISPOSITIVOS

Conforme comentado anteriormente, a confiança é o recurso utilizado para auxiliar nas decisões do sistema, e sua metodologia de avaliação e cálculo, no MobAngelo, é baseada no mecanismo STEALTH (Batista, 2019). Ela é representada por um valor numérico T calculado

entre o dispositivo avaliador *i* e o dispositivo avaliado *j* (T^I_{ij}), através de dois atributos configurados pelo usuário, *Competência* e *Similaridade de Interesses*. O primeiro item utilizado no cálculo é a *Competência* em saúde do usuário. Competência, nesse contexto, refere-se à profissão, atividade ou *hobby* que as pessoas possuem e as possibilita exercer diversas atividades. Mais especificamente, esse conceito está relacionado ao nível de conhecimento que a pessoa possui para realizar atendimentos de saúde. Um médico, por exemplo, é mais capacitado para prestar primeiros socorros do que um engenheiro de *software*. O segundo item é a *Similaridade de Interesses*, que se refere aos interesses em comum que as duas pessoas possuem. Dessa forma, quanto mais interesses iguais as pessoas tiverem, maior será a confiança entre elas.

Para realizar a distinção entre diferentes níveis de competência, o MobAngelo utiliza como base a taxonomia de profissões definida pelo STEALTH e o seu modelo de cálculo. Esse cálculo utiliza a similaridade entre duas competências que estão presentes na taxonomia. No caso do STEALTH, e consequentemente no MobAngelo, a competência de médico é a referência utilizada para determinar a confiança com relação à atendimentos de saúde de outras competências (T^{Skill}) (Batista, 2019). Essa taxonomia é ilustrada na Figura 4.2, baseada em (Batista, 2019). O cálculo de similaridade Sim_s é realizado através da Equação 4.1,onde c_3 corresponde à quantidade de saltos entre entre o nível comum mais próximo das competências avaliada e de referência até a raiz da taxonomia. O c_1 equivale à quantidade de níveis entre a competência de médico até a raiz da taxonomia, e c_2 equivale à quantidade de saltos entre a competência que se deseja verificar a similaridade até a raiz da taxonomia (Batista, 2019). Os valores de Sim_s variam no intervalo $]0, 1]$ e não há valor de confiança menor ou igual a 0, pois, a medição ocorre apenas quando ambos os usuários possuem pelo menos o interesse em *saúde*. Existem duas competências com classificação especial no método de cálculo. A primeira é a competência Outras, pois refere-se a profissões não relacionadas com o contexto de saúde, e por isso, possui confiança zero. A segunda é a competência Médico, que por ser aquela com maior nível de preparo e conhecimento recebe sempre o valor maíximo (1).

Considere-se o cálculo da confiança para competência da profissão Policial utilizando como referência a competência Médico e a estrutura da taxonomia da Figura 4.2 junto à Equação 4.1. Nesse caso, temos que a distância entre a competência Médico e a raiz é de 3 níveis, logo $c_1 = 3$. A competência de Policial está 4 níveis abaixo da raiz, portanto $c_2 = 4$. A variável c_3 refere-se à distância da classe que é comum às duas competências avaliadas, Saúde, e a raiz, portanto $c_3 = 1$. Assim sendo, a confiança com relação à competência Policial em referência à competência Médico possui o valor $0,4$. A Figura 4.2 apresenta todas as competências mapeadas na taxonomia. Porém, o MobAngelo possui apenas um subconjunto dessas competências, conforme apresentado na figura. A Tabela 4.1 apresenta a confiança calculada para as competências disponíveis no aplicativo.

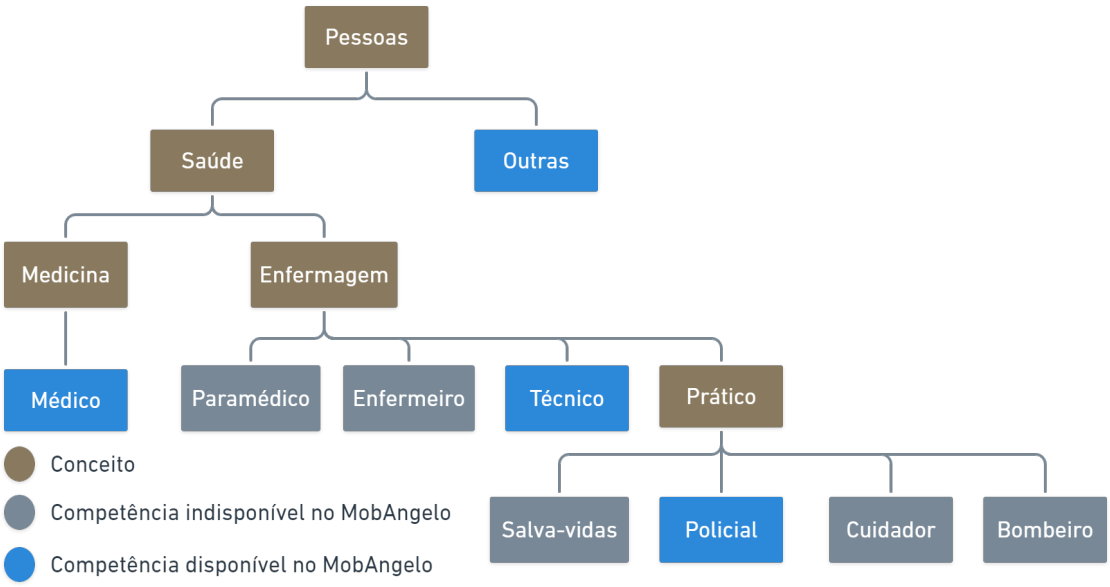


Figura 4.2: Taxonomia de competências

Tabela 4.1: Confiança atribuída às competências

Competência	**Confiança (T^{Skill})**
Médico(a)	1,00
Técnico em enfermagem	0,33
Policial	0,28
Outra	0,00

$$Sim_s = \frac{2 \times c_3}{c_1 + c_2} \qquad (4.1)$$

O segundo atributo no cálculo da confiança é a *Similaridade de interesses*. Ela é calculada através da razão entre os interesses comuns de i (I_i) e j (I_j), e os interesses do dispositivo avaliador i, conforme apresentado na Equação 4.2. A confiança do dispositivo avaliador i sobre o dispositivo avaliado j (T_{ij}) é calculada pela soma da confiança em relação à competência de i (T_{ij}^{Skill}) e a confiança em relação aos seus interesses em comum (T_{ij}^{I}), conforme Equação 4.3. Pressupondo que um dispositivo i mensure a confiança T_{ij} sobre um dispositivo j, cuja competência seja Técnico em Enfermagem e que ambos possuam apenas o interesse em saúde. Logo, pela Tabela 4.1, temos que $T_{ij}^{Skill} = 0,33$. Assim, $T_{ij}^{I} = 1$, visto que os dois dispositivos possuem interesses idênticos e, portanto, aplicando a Equação 4.3, temos $T_{ij} = 0,64$. Caso a competência de j seja "Outra", $T_{ij}^{Skill} = 0$, indicando que ele não possui habilidade para o atendimento de saúde. Como $T_{ij}^{I} = 1$, a confiança de i em j terá o valor de 0,5.

$$T_{ij}^{I} = \frac{|I_i \cap I_j|}{|I_i|} \qquad (4.2) \qquad\qquad T_{ij} = \frac{T_{ij}^{I} + T_{ij}^{Skill}}{2} \qquad (4.3)$$

4.3 OPERAÇÃO

Uma vez configurado, o MobAngelo constrói redes e as mantém sem a necessidade de interação do usuário. A tela principal do aplicativo, apresentada na Figura 4.3, contém na parte superior as informações sobre o sistema e seu estado, isto é, o nome do dispositivo - configurado na interface Bluetooth -, a competência cadastrada pelo usuário e o estado atual da aplicação, como por exemplo *Buscando* (vizinhos) ou *Descoberta Finalizada*. O estado da aplicação também é apresentado na tela para acompanhamento do fluxo. Assim, caso a comunidade de interesses esteja vazia, o usuário pode verificar se a execução está correta ou a aplicação parou sua operação. Além disso, após a realização do *scan* de vizinhança é atualizada a contagem de dispositivos encontrados, que serão identificados para formação da CoI, facilitando a compreensão acerca da quantidade de dispositivos Bluetooth dentro da sua área de alcance. Nessa tela também há o botão "Emergência", que é responsável por iniciar o processo de disseminação dos dados. O botão "Configurações"apresenta ao usuário a tela para configuração da sua competência, seus interesses e sua mensagem de emergência, como apresentado na Figura 4.4. Nessa tela, o usuário pode selecionar dentre as competências Médico(a), Téc. Enfermagem, Policial e Outra, de acordo com o seu conhecimento. Os interesses possíveis são saúde, esportes e filmes. Além disso, há um campo de texto livre que deve ser preenchido com sua mensagem de emergência. Quando um dispositivo recebe uma mensagem de emergência, o conteúdo recebido é apresentado para auxiliar o usuário na tomada de decisão, tendo em vista o evento crítico de saúde em curso.

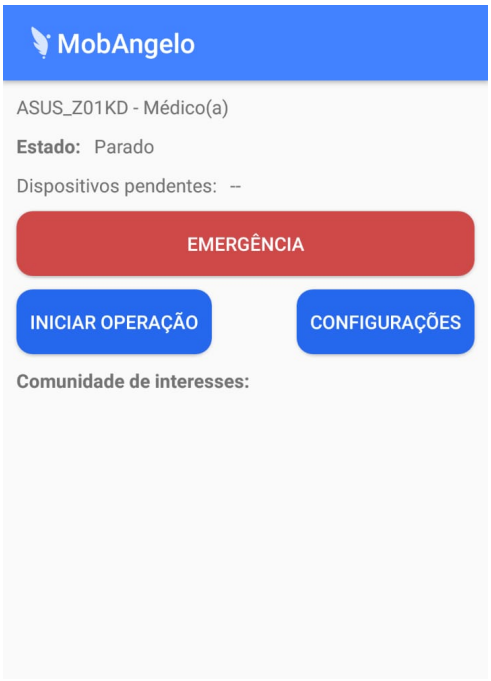


Figura 4.3: Tela principal do sistema MobAngelo

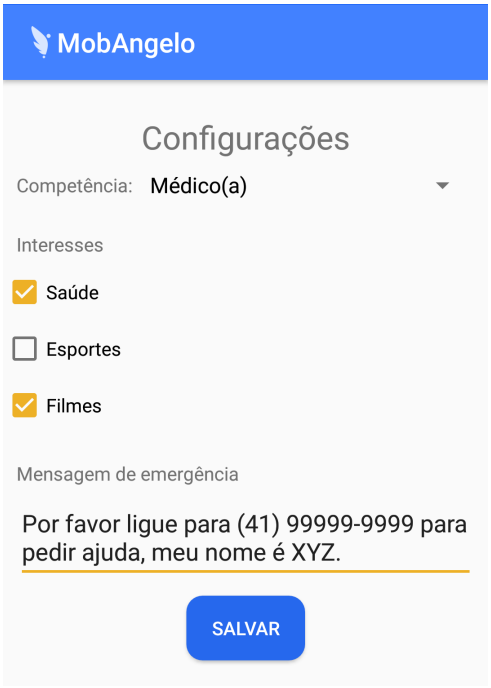


Figura 4.4: Tela de Configurações do MobAngelo

Para criação e manutenção da rede, o usuário deve pressionar o botão *Iniciar Operação*, presente no lado esquerdo da Figura 4.3. Essa interação inicia a execução do módulo *Gestão de*

Comunidades. Na sequência, o usuário deve habilitar o Bluetooth e permitir que seu dispositivo torne-se visível para outros dispositivos, como apresentado na Figura 4.5. Após sua autorização, o dispositivo continua visível para outros dispositivos Bluetooth por até 1 hora, que é o tempo máximo permitido pelo sistema operacional. A Figura 4.6 apresenta a modificação no conteúdo da tela principal quando o MobAngelo identifica os dispositivos vizinhos. Nesse momento, o sistema apresenta os integrantes da sua comunidade de interesses em uma lista com informações de nome do dispositivo, endereço MAC, confiança em porcentagem e competência.

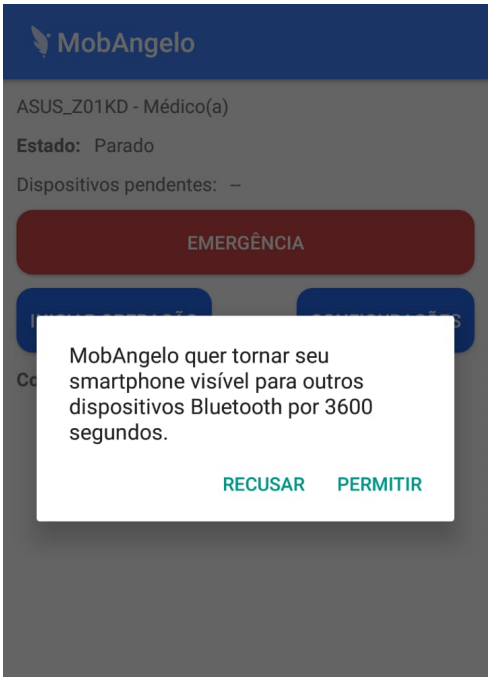


Figura 4.5: Modal para habilitar visibilidade do dispositivo

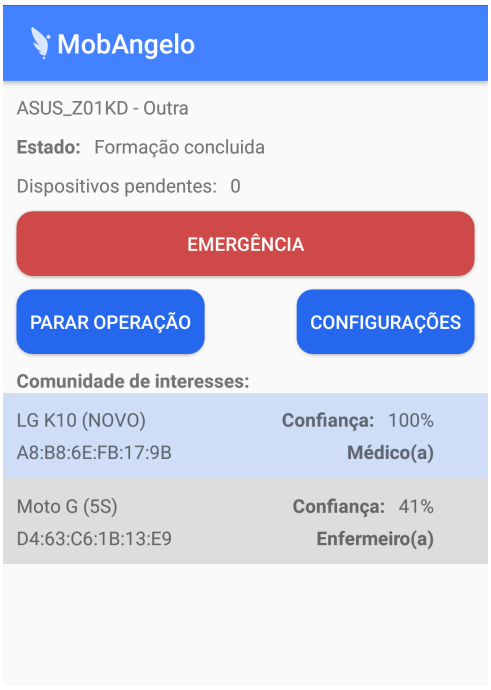


Figura 4.6: Tela do MobAngelo em execução

4.3.1 Fluxo de comunicação e emergência

A partir do ponto de vista de um dispositivo, são descritas as rotinas executadas durante o seu ciclo de vida. Assim, após o inicio da execução do MobAngelo, sinalizado pelo usuário, o sistema inicia as rotinas de gestão das comunidades, responsáveis por recriar a comunidade de interesses a cada intervalo de aproximadamente 5 segundos, tendo tempo máximo de *scan* de 13 segundos. Primeiramente, executa-se um *scan* Bluetooth dos dispositivos que estão dentro do raio de cobertura. Em seguida, para cada dispositivo encontrado é estabelecida uma conexão Bluetooth, e essa comunicação deve ser respondida com os dados de identificação do outro dispositivo codificada como uma sequência de caracteres que respeite o formato "$c; i_1, i_2, i_3$"onde c é a competência e i é um inteiro que representa um interesse configurado pelo usuário, i.e. $i \in \{Saúde, Filmes, Esportes\}$

A cada interação e identificação, o dispositivo descoberto é avaliado com base nos critérios explicados anteriormente e adicionado com sua confiança à comunidade de interesses. A Figura 4.7 ilustra um usuário - paciente - caminhando com o sistema MobAngelo ativo e durante

seu trajeto interage com outros usuários formando a sua comunidade de interesse em saúde com participação daquelas pessoas que também possuem interesse em saúde: a médica, o técnico em enfermagem e o bombeiro. As comunidades são formadas somente pelos dispositivos que se encontram na área de cobertura, embora possam existir dispositivos Bluetooth que não façam parte da rede. Nesse caso, eles são ignorados após não responderem a mensagem de identificação ou em caso de recusa no estabelecimento da comunicação. Usuários que não possuem interesse em saúde também são excluídos na formação das comunidades, uma vez que a rede se propõe a facilitar e agilizar o auxílio no atendimento de saúde. Nesse caso, o dispositivo realiza o processo de identificação, mas seus dados são descartados pelo receptor. Essa situação é vista na Figura 4.7 pelo usuário de competência *Outro* (i.e., não possui qualquer competência na área de saúde) e que também não possui interesse em saúde. A Figura 4.8 apresenta essa circunstância, pois após a formação da comunidade esse dispositivo é ignorado pelo dispositivo do paciente.

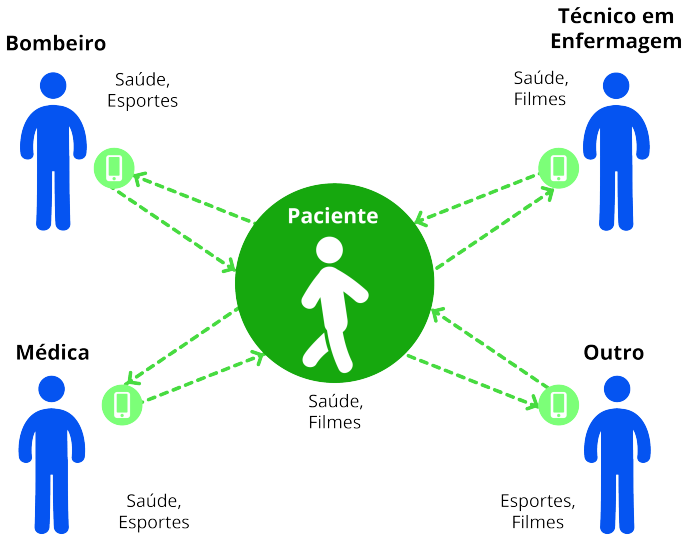


Figura 4.7: Fluxo de formação de CoIs

Diante da ocorrência de um evento crítico de saúde com o usuário, ele pode sinalizar que necessita de ajuda pressionando o botão *Emergência* disponível na tela principal do MobAngelo. Essa ação simula a integração com sensores externos que monitorem a saúde do usuário, por exemplo, um medidor de pressão ou de batimentos cardíacos. Ao receber esse sinal, o funcionamento do MobAngelo é alterado para priorizar o disparo da mensagem de evento crítico, tal que suas atividades de descoberta da vizinhança são interrompidas. A aplicação tenta, então, se conectar ao dispositivo melhor avaliado no quesito de confiança dentre aqueles que pertencem a sua comunidade de interesses vigente.

Conforme demonstrado na Figura 4.4, a mensagem a ser enviada é configurável de acordo com o que o usuário cadastrou e servirá como meio de identificação e direcionamento da ajuda, caso exista alguma condição preexistente que o usuário queira compartilhar (diabetes, pressão alta ou outras). Após o envio dessa mensagem para a médica, o MobAngelo do paciente

aguarda a confirmação de seu recebimento para encerrar sua operação. Caso o sistema não receba a confirmação dentro de um intervalo estabelecido, a mensagem é encaminhada ao segundo usuário mais confiável da sua comunidade de interesses - técnico em enfermagem, como apresentado na Figura 4.8. Na circunstância em que o dispositivo desse usuário também não confirme o recebimento da mensagem do paciente, o processo seguirá sucessivamente até que a mensagem seja entregue ou que não existam vizinhos na sua comunidade de saúde.

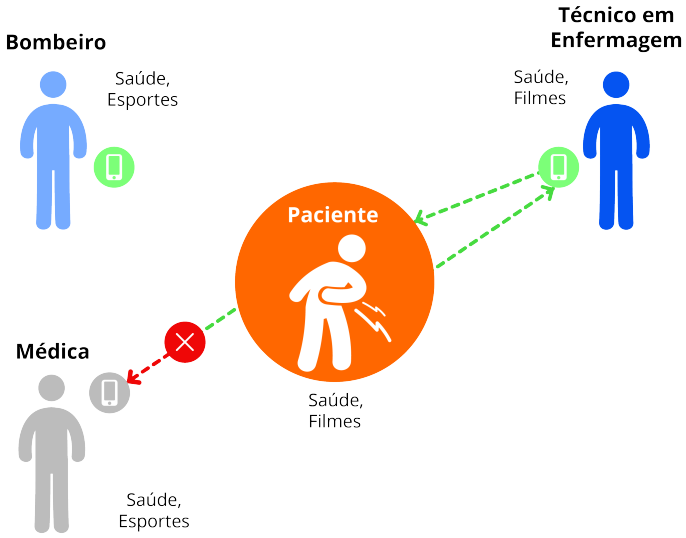


Figura 4.8: Fluxo de sinalização de evento crítico de saúde

4.4 RESUMO

Este capítulo apresentou o MobAngelo, um aplicativo Android para auxilio na tomada de decisão em situações emergenciais de saúde. Apresentamos os conceitos utilizados no desenvolvimento da ferramenta e o embasamento teórico para seu funcionamento. A ferramenta é baseada no mecanismo de disseminação de dados sensíveis baseado em confiança social, e através da tecnologia Bluetooth utiliza o modelo de rede desse mecanismo.

5 METODOLOGIA DE AVALIAÇÃO E RESULTADOS

Este capítulo apresenta a metodologia de avaliação do funcionamento da ferramenta proposta, bem como os resultados obtidos. Primeiramente, a Seção 5.1 descreve os dispositivos utilizados na avaliação e a metodologia utilizada. A Seção 5.2 apresenta o cenário e os resultados da avaliação da identificação de vizinhança. A Seção 5.3 expõe o contexto e os resultados da avaliação do envio de mensagens de emergência.

5.1 VISÃO GERAL

Para a avaliação e validação da aplicação foram utilizados três smartphones executando o MobAngelo[1] em dois experimentos diferentes. O primeiro para avaliar o tempo para formação de comunidades. E o segundo, para examinar o tempo de envio da mensagem de evento crítico. Nesses cenários, os três dispositivos permitem validar o mecanismo de formação da rede, avaliar o processo decisório do sistema e o cálculo de confiança. As configurações dos dispositivos utilizados na avaliação são apresentados na Tabela 5.1. Os três dispositivos possuíam uma versão similar da tecnologia Bluetooth (4.x), diferenciando-se pelas suas subversões.

Tabela 5.1: Configuração dos dispositivos da rede

Modelo	**Sistema Operacional**	**Versão do Bluetooth**
Asus Zenfone 4	Android 8.0	4.2
Motorola G5s	Android 8.1	4.2
LG K10	Android 7.0	4.0

Em ambas as avaliações, os dispositivos foram dispostos em ambiente fechado, próximos uns aos outros. Portanto, a distância e a interferência causada por obstáculos foi reduzida ao mínimo. A Figura 5.1 apresenta o posicionamento dos dispositivos na avaliação de formação de comunidades. Nesse momento também havia um dispositivo visível através do *scan* Bluetooth, mas que não estava executando o MobAngelo. Logo, esse cenário aproxima-se de um contexto real onde existem diversos dispositivos Bluetooth, como por exemplo fones de ouvido, *smartbands* e *smartwatches*, que não são compatíveis com o MobAngelo.

5.2 FORMAÇÃO DE COMUNIDADES

O experimento para avaliação do processo de identificação de vizinhos e formação da comunidade foi executado duas vezes, cada uma com 15 minutos de duração. Durante

[1]Código fonte e manual disponíveis em https://github.com/LucasBCunha/mob_angelo

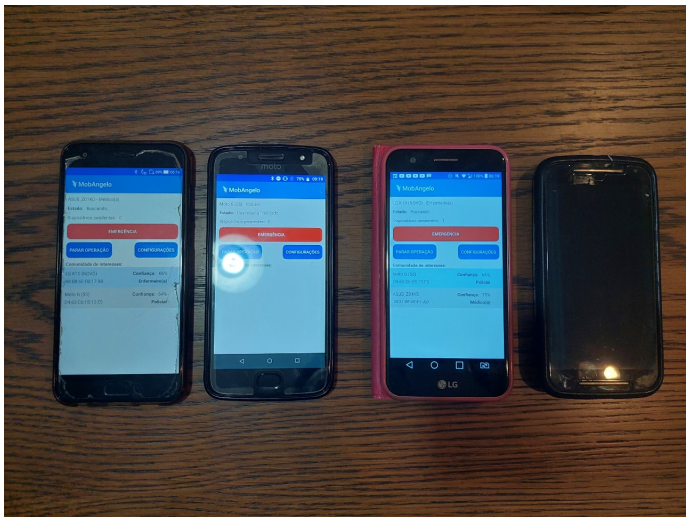


Figura 5.1: Disposição dos smartphones na avaliação

esse período cada dispositivo executou em média 10 ciclos completos - *scan* de dispositivos, conexão e identificação dos vizinhos e ,por fim, o período ocioso. Para contabilizar o tempo do processo utilizou-se de *logs* com *timestamp* do smartphone. Através do intervalo entre o início da descoberta Bluetooth e o fim do processo de identificação dos vizinhos, chegamos aos resultados apresentados na Figura 5.2. Observa-se que os dois dispositivos com a mesma versão da tecnologia Bluetooth - Asus Zenfone 4 e Motorola G5s - tiveram um desempenho semelhante, com uma diferença desprezível entre suas médias aferidas. Contudo, o dispositivo LG K10, que possui uma versão inferior da tecnologia Bluetooth, *4.0*, demorou em média 2 segundos a mais para a identificação e construção da sua comunidade de interesses. Observou-se, também, que em alguns casos, dois dispositivos não se reconheceram após determinado momento, enquanto mantiveram a operação. Isso ocorre devido à sincronização dos seus períodos de busca. Apesar de os dois dispositivos continuarem visíveis um para o outro, o processo de *scan* Bluetooth prejudica seu tempo de resposta (Google, 2021a) e, assim sendo, os dispositivos não respondiam em tempo hábil um ao outro. Isso mostrou-se um desafio para a execução do experimento.

Tendo como base um modelo realista de mobilidade de pedestres (Kouyoumdjieva et al., 2014), empregado por (Helgason et al., 2013) e (Batista, 2019), temos que a velocidade de deslocamento das pessoas em ambiente urbano varia de 0,5m/s a até 2,0m/s. Considerando o alcance de 100 metros da versão 4 do Bluetooth, tem-se que uma pessoa andando na velocidade máxima prevista levaria 100 segundos para atravessar o diâmetro da área cobertura do dispositivo realizando a identificação de vizinhança. Nesse cenário, o tempo de 17 segundos é adequado e permite o funcionamento correto da aplicação. Porém, como o sistema deve estabelecer uma conexão com cada dispositivo encontrado para realizar sua identificação, um cenário com alta densidade de vizinhos pode prejudicar o funcionamento do sistema. Para mitigar essa situação, a utilização de tecnologias que permitam o uso de mensagens do tipo *Broadcast*, quando todos os participantes da rede recebem a mensagem com apenas uma ação do remetente, pode reduzir o impacto da densidade de dispositivos na performance da identificação de vizinhos.

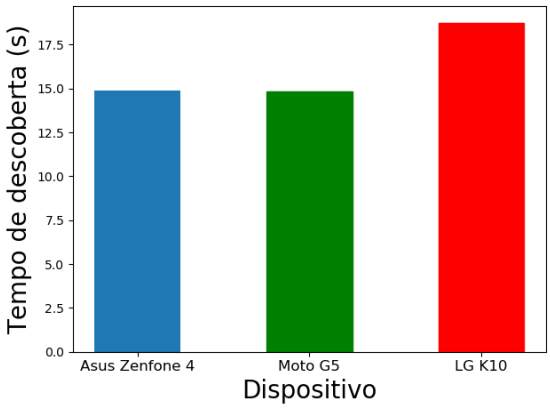


Figura 5.2: Duração média do *scan* de vizinhança

5.3 ENVIO DE MENSAGEM DE EMERGÊNCIA

No segundo experimento, executado 5 vezes para cada dispositivo, avaliou-se o tempo para que os dispositivos disparem uma mensagem de emergência e recebam a confirmação, possibilitando que seja contabilizado o tempo total da entrega. Em todas as execuções, a mensagem foi enviada para o vizinho com maior nível de confiança. Na Figura 5.3, temos a média do tempo para o envio da mensagem de evento crítico, originada pelo dispositivo nomeado, com destino aos 2 outros dispositivos presentes. Para o Zenfone 4, observou-se um grande intervalo, o tempo total para envio variou de 0,163s a até 7,34s. Isso aparenta ter relação com o tempo de espera pela confirmação, devido ao estado de execução do dispositivo que recebeu a mensagem. Como comentado anteriormente, durante o processo de *scan* Bluetooth, o dispositivo que o está executando demora mais para responder os pedidos de conexão. Por isso, quando a mensagem de emergência é encaminhada para um dispositivo que está executando o processo de descoberta dos vizinhos, a mensagem de evento crítico demora mais para ser recebida, processada e respondida.

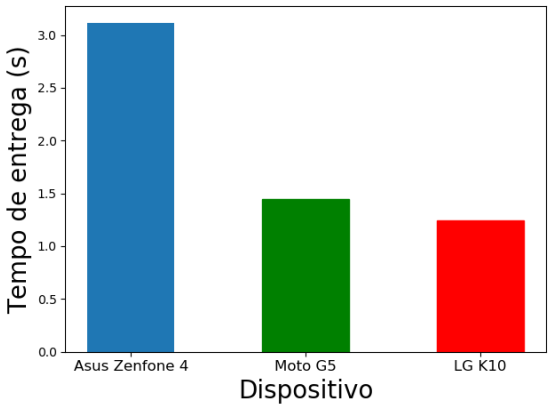


Figura 5.3: Tempo médio de entrega da mensagem de emergência

5.4 RESUMO

Este capítulo apresentou a avaliação da performance da ferramenta em seus dois fluxos. Observou-se que a ferramenta é capaz de identificar a sua vizinhança e medir a confiança com relação aos dispositivos participantes da rede. No caso dos dispositivos utilizados no teste, seu tempo de execução ficou abaixo dos 17 segundos, que é adequado considerando-se o tempo de deslocamento das pessoas como 2,0m/s e o alcance de 100 metros da tecnologia Bluetooth. O envio da mensagem de emergência, em média, ficou abaixo dos 3 segundos, entretanto ocorreram casos de atraso no qual a mensagem demorou até 7,34 segundos.

6 CONCLUSÃO E TRABALHOS FUTUROS

Existe uma gama grande de serviços que utilizam recursos computacionais oferecidos à população. Esses serviços facilitam o dia-a-dia e trazem mais conforto para a humanidade, desde serviços bancários através da internet, automações industriais e e-health. Os serviços digitais de saúde podem auxiliar a medicina a manter a saúde, tratar e prevenir doenças. Existem avanços no contexto de atendimento clínico e prevenção através da telemedicina, por exemplo. Entretanto, nos casos de atendimento de emergência, há espaço para, através da colaboração entre os cidadãos, ajudar as pessoas que necessitem. Tendo em vista os impactos causados pelo atraso no atendimento em situações críticas de saúde, nosso estudo apresentou uma ferramenta que permite a cooperação entre as pessoas em ambientes urbanos, *Zero-Knowledge* e não estruturados. Essa ferramenta diminui o tempo entre a ocorrência do evento e o primeiro auxílio, pois aqueles próximos do local do paciente podem ajudar antes da chegada da equipe especializada.

A avaliação do sistema, através de uma experimentação, demonstrou as suas características de performance dentro do contexto de três dispositivos compondo a rede. A identificação da vizinhança ocorre em até 17 segundos, e o envio da mensagem de emergência está na média de 3 segundos. Entretanto, para alguns casos há uma variação grande no fluxo de evento crítico, no qual a confirmação de resposta ocorreu em 7,4 segundos. Considerando-se o tempo de deslocamento de pedestres caminhando como até 2,0m/s, a performance é apropriada pois o sistema é capaz de identificar vizinhos e enviar as notificações de emergência. Por fim, a ferramenta proposta por esse estudo rendeu uma publicação no XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, mais precisamente no fórum Salão de Ferramentas (Cunha et al., 2021).

6.1 TRABALHOS FUTUROS

A partir da ferramenta desenvolvida, bem como da avaliação realizada, essa seção apresenta pontos de melhoria e evolução da ferramenta. Esses tópicos incluem melhorias nas funcionalidades, aplicação de novas tecnologias e considerações de segurança que não fizeram parte do presente trabalho.

6.1.1 Gestão de comunidades

A quantidade de vizinhos próximos afeta diretamente o desempenho do MobAngelo. Devido à sua arquitetura e a utilização da tecnologia Bluetooth, o processo de identificação ocorre de maneira serial, de modo que para cada vizinho deve ser estabelecida uma conexão. Em situações de alta densidade de vizinhos na região o tempo de identificação da vizinhança pode ser comprometido, prejudicando o propósito da ferramenta de reduzir o tempo de espera

para o primeiro atendimento. A utilização de tecnologias alternativas para a comunicação dos dispositivos pode mitigar esse problema, por exemplo, a utilização de mensagens *broadcast* para divulgar os atributos de competência e interesses de cada dispositivo. Outro ponto de melhoria nesse módulo inclui o ajuste do algoritmo de formação de comunidades. Além disso, a avaliação do desempenho do sistema em ambientes urbanos reais, em diferentes cenários de densidade de vizinhos, seria de grande valia para determinar a efetividade de novas tecnologias. Assim como uma avaliação com relação ao consumo de energia durante a utilização do MobAngelo. Conforme observado na avaliação, existem situações em que dois dispositivos não identificam um ao outro, e consequentemente não integram a comunidade do vizinho. Para esses casos, uma abordagem possível para sua mitigação é a aplicação de um fator de aleatoriedade entre cada intervalo de tempo para descoberta de vizinhos, ou propagação de mensagem *broadcast* no caso de outra tecnologia. Por exemplo, a descoberta de vizinhos poderia ser realizada a cada $20 + X$ segundos, onde X é um numero inteiro gerado de maneira aleatória.

6.1.2 Integrações externas

Outra direção de evolução é a integração com sistemas de monitoramento da saúde do paciente. Um dispositivo que monitore a pressão, por exemplo, poderia automaticamente iniciar o processo de evento crítico caso os dados ultrapassem um limite estabelecido. Isso promoveria mais segurança na utilização do sistema, pois mesmo que o usuário fique incapacitado o sistema notificaria as pessoas próximas. O sistema também poderia se integrar a sistemas externos de validação da competência. Através de uma checagem de registro em conselho de classe, por exemplo, haveria maior confiança com relação à competência dos usuários. Não obstante, o cadastro separado de informações não sensíveis e informações da ficha médica do usuário, aliado à disseminação controlada por competência, aperfeiçoaria a mensagem de evento crítico, auxiliando ainda mais a tomada de decisão. Usuários sem competência em saúde teriam, por exemplo, acesso ao número de emergência cadastrado. Por outro lado, usuários com competência em saúde poderiam ter acesso à informações como tipo sanguíneo, presença de doenças crônicas ou outras informações de acordo com a Lei Geral de Proteção de Dados Pessoais.

REFERÊNCIAS

Álvarez, F. (2020). *Secure device-to-device communication for emergency response*. Tese de doutorado, Technische Universität Darmstadt, Darmstadt.

American Heart Association, A. S. a. (2013). https://www.heart.org/idc/groups/heart-public/@wcm/@adv/documents/downloadable/ucm_301646.pdf. [Online] Acesso em: Mar. 2021.

Batista, A. (2019). Disseminação Segura de Dados Pessoais Vitais Para Apoio às tomadas de decisão em situações emergenciais. Dissertação de Mestrado, Universidade Federal do Paraná, Curitiba, PR.

Beierle, F. e Eichinger, T. (2019). Collaborating with Users in Proximity for Decentralized Mobile Recommender Systems. Em *2019 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, páginas 1192–1197.

Bisdikian, C. (2001). An overview of the Bluetooth wireless technology. *IEEE Communications magazine*, 39(12):86–94.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF:15 Ago 2018.

Bruno, R., Conti, M. e Gregori, E. (2002). Bluetooth: Architecture, Protocols and Scheduling Algorithms. *Cluster Computing*, 5(2):117–131.

Castro, R. P., Haug, S., Filler, A., Kowatsch, T. e Schaub, M. P. (2017). Engagement within a mobile phone–based smoking cessation intervention for adolescents and its association with participant characteristics and outcomes. *Journal of medical Internet research*, 19(11):e356.

CFM (2020). Ofício CFM Nº1756/2020. https://portal.cfm.org.br/images/PDF/2020_oficio_telemedicina.pdf. [Online] Acesso em: Maio 2021.

Chakraborty, T., Dalmia, A., Mukherjee, A. e Ganguly, N. (2017). Metrics for community analysis: A survey. *ACM Computing Surveys (CSUR)*, 50(4):1–37.

Cheah, M., Shaikh, S. A., Haas, O. e Ruddle, A. (2017). Towards a systematic security evaluation of the automotive Bluetooth interface. *Vehicular Communications*, 9:8–18.

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

Choi, J. M., Choi, B. H., Seo, J. W., Sohn, R. H., Ryu, M. S., Yi, W. e Park, K. S. (2004). A System for Ubiquitous Health Monitoring in the Bedroom via a Bluetooth Network and Wireless LAN. Em *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, volume 2, páginas 3362–3365.

Collotta, M., Pau, G., Talty, T. e Tonguz, O. K. (2018). Bluetooth 5: A Concrete Step Forward toward the IoT. *IEEE Communications Magazine*, 56(7):125–131.

Cordeiro, C. D. M. (2003). *Medium access control protocols and routing strategies for wireless local and personal area networks*. Tese de doutorado, University of Cincinnati.

Cunha, L. B., de Souza Batista, A. e Santos, A. (2021). Mobangelo: Assistência emergencial em ambientes urbanos. Em *Anais Estendidos do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, Porto Alegre, RS, Brasil. SBC. No Prelo.

Fang, W., Cui, N., Chen, W., Zhang, W. e Chen, Y. (2020). A trust-based security system for data collection in smart city. *IEEE Transactions on Industrial Informatics*, 17(6):4131–4140.

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

Filler, A., Kowatsch, T., Haug, S., Wahle, F., Staake, T. e Fleisch, E. (2015). Mobilecoach: A novel open source platform for the design of evidence-based, scalable and low-cost behavioral health interventions: Overview and preliminary evaluation in the public health context. Em *2015 Wireless Telecommunications Symposium (WTS)*, páginas 1–6. IEEE.

Gast, M. (2005). *802.11 wireless networks: the definitive guide*. O'Reilly Media, Inc.

Globo, T. (2019). Samu demora mais do que o tempo recomendado para atender casos graves em 5 capitais. https://g1.globo.com/ciencia-e-saude/noticia/2019/12/26/samu-demora-mais-do-que-o-tempo-recomendado-para-atender-casos-graves-em-5-capitais.ghtml. [Online] Acesso em: Mar. 2021.

Google (2021a). Find Bluetooth devices. https://developer.android.com/guide/topics/connectivity/bluetooth/find-bluetooth-devices. [Online] Acesso em: Ago. 2021.

Google (2021b). Nearby. https://developers.google.com/nearby. [Online] Acesso em: Jul. 2021.

Google (2021c). Overview - Nearby Connections. https://developers.google.com/nearby/connections/overview. [Online] Acesso em: Jul. 2021.

Google (2021d). Overview - Nearby Connections. https://developers.google.com/nearby/connections/strategies. [Online] Acesso em: Jul. 2021.

Helgason, Ó., Kouyoumdjieva, S. T. e Karlsson, G. (2013). Opportunistic communication and human mobility. *IEEE Transactions on Mobile Computing*, 13(7):1597–1610.

Hiertz, G. R., Denteneer, D., Stibor, L., Zang, Y., Costa, X. P. e Walke, B. (2010). The ieee 802.11 universe. *IEEE Communications Magazine*, 48(1):62–70.

IEEE (2016). IEEE 802.11-2016 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. https://standards.ieee.org/standard/802_112016.html. [Online] Acesso em: Jan. 2020.

Jiang, H., Cai, C., Ma, X., Yang, Y. e Liu, J. (2018). Smart home based on wifi sensing: A survey. *IEEE Access*, 6:13317–13325.

Jiang, L., Cheng, Y., Yang, L., Li, J., Yan, H. e Wang, X. (2019). A trust-based collaborative filtering algorithm for e-commerce recommendation system. *Journal of Ambient Intelligence and Humanized Computing*, 10(8):3023–3034.

Kizza, J. M. (2005). *Computer network security*. Springer Science & Business Media.

Kotaru, M., Joshi, K., Bharadia, D. e Katti, S. (2015). Spotfi: Decimeter level localization using wifi. Em *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, páginas 269–282.

Kouyoumdjieva, S. T., Ólafur Ragnar Helgason e Karlsson, G. (2014). CRAWDAD dataset kth/walkers (v. 2014-05-05). Downloaded from `https://crawdad.org/kth/walkers/20140505`.

Kowatsch, T., Volland, D., Shih, I., Rüegger, D., Künzler, F., Barata, F., Filler, A., Büchter, D., Brogle, B., Heldt, K., Gindrat, P., Farpour-Lambert, N. e l'Allemand, D. (2017). Design and Evaluation of a Mobile Chat App for the Open Source Behavioral Health Intervention Platform MobileCoach. Em Maedche, A., vom Brocke, J. e Hevner, A., editores, *Designing the Digital Transformation*, páginas 485–489, Cham. Springer International Publishing.

Künzler, F. (2019). Context-aware notification management systems for just-in-time adaptive interventions. Em *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, páginas 435–436.

Mohapatra, P. e Krishnamurthy, S. (2004). *AD HOC NETWORKS: technologies and protocols*. Springer Science & Business Media.

Omar, H. A., Abboud, K., Cheng, N., Malekshan, K. R., Gamage, A. T. e Zhuang, W. (2016). A survey on high efficiency wireless local area networks: Next generation wifi. *IEEE Communications Surveys & Tutorials*, 18(4):2315–2344.

Qi, W. e Zhai, Y. (2017). The Study on the Life Signs of Clinical Patients Monitored by Electronic Wrist Band. Em *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, volume 2, páginas 356–359.

Schauer, L., Werner, M. e Marcus, P. (2014). Estimating crowd densities and pedestrian flows using wi-fi and bluetooth. Em *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, páginas 171–177.

SIG, B. (2020a). 2020 Bluetooth Market Update. https://www.bluetooth.com/bluetooth-resources/2020-bmu/. [Online] Acesso em: Ago. 2021.

SIG, B. (2020b). Overview - Bluetooth Markets. https://www.bluetooth.com. [Online] Acesso em: Nov. 2020.

Stieger, M., Flückiger, C., Rüegger, D., Kowatsch, T., Roberts, B. W. e Allemand, M. (2021). Changing personality traits with the help of a digital personality change intervention. *Proceedings of the National Academy of Sciences*, 118(8).

Su, K.-C., Wu, H.-M., Chang, W.-L. e Chou, Y.-H. (2012). Vehicle-to-vehicle communication system through wi-fi network using android smartphone. Em *2012 International conference on connected vehicles and expo (ICCVE)*, páginas 191–196. IEEE.

Sun, Y., Yu, W., Han, Z. e Liu, K. R. (2005). Trust modeling and evaluation in ad hoc networks. Em *GLOBECOM'05. IEEE Global Telecommunications Conference, 2005.*, volume 3, páginas 6–pp. IEEE.

Tang, X., Xiao, B. e Li, K. (2018). Indoor crowd density estimation through mobile smartphone wi-fi probes. *IEEE transactions on systems, man, and cybernetics: systems*, 50(7):2638–2649.

Wu, J. e Stojmenovic, I. (2004). Ad hoc networks. *Computer*, 37(2):29–31.

Yamamoto, Y. (1990). A morality based on trust: Some reflections on japanese morality. *Philosophy East and West*, 40(4):451–469.

Yin, J., Yang, Z., Cao, H., Liu, T., Zhou, Z. e Wu, C. (2019). A survey on bluetooth 5.0 and mesh: New milestones of iot. *ACM Transactions on Sensor Networks (TOSN)*, 15(3):1–29.

Zeadally, S., Siddiqui, F. e Baig, Z. (2019). 25 years of bluetooth technology. *Future Internet*, 11(9):194.