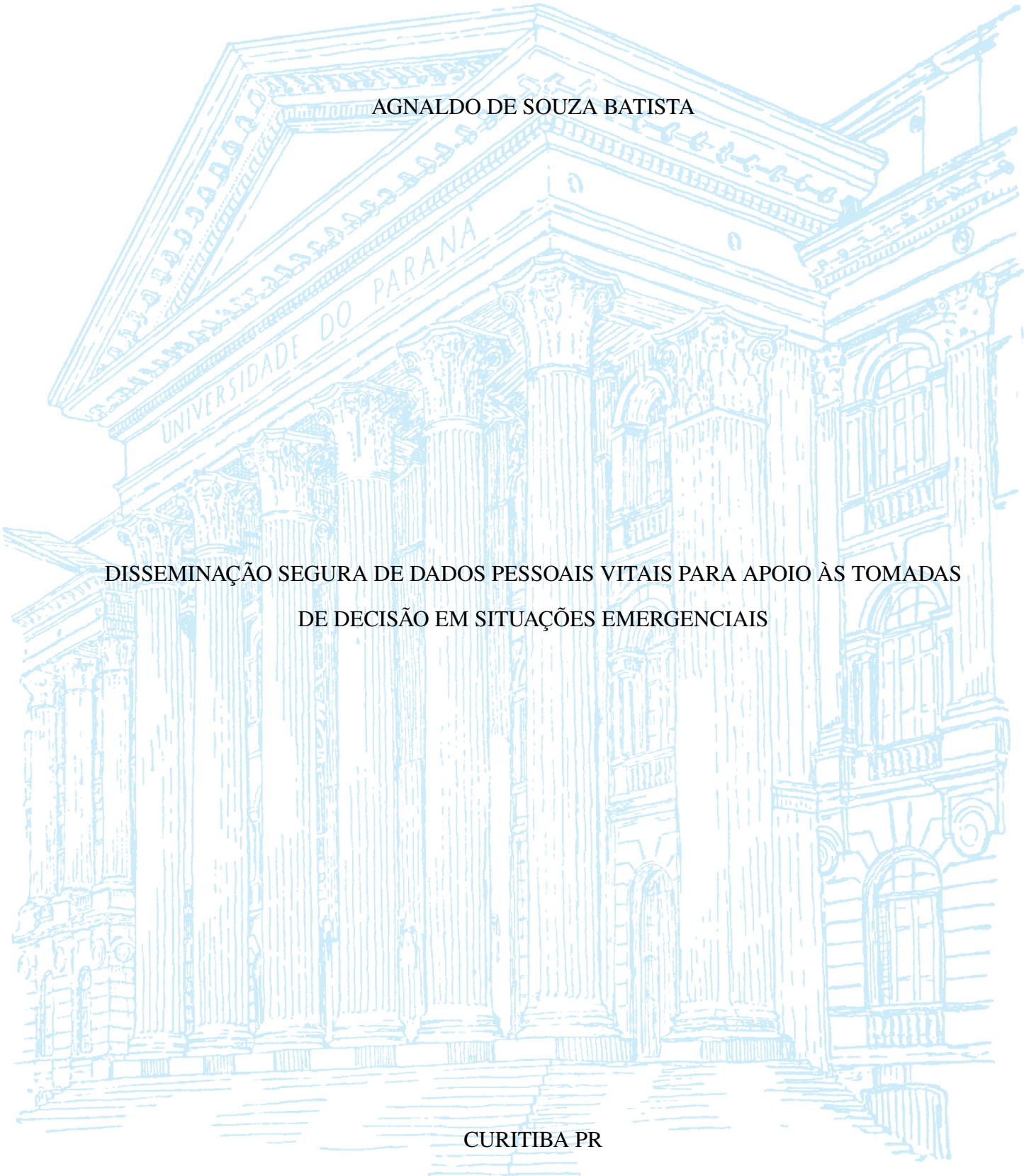
UNIVERSIDADE FEDERAL DO PARANÁ

AGNALDO DE SOUZA BATISTA



DISSEMINAÇÃO SEGURA DE DADOS PESSOAIS VITAIS PARA APOIO ÀS TOMADAS DE DECISÃO EM SITUAÇÕES EMERGENCIAIS

CURITIBA PR

2019

AGNALDO DE SOUZA BATISTA

DISSEMINAÇÃO SEGURA DE DADOS PESSOAIS VITAIS PARA APOIO ÀS TOMADAS DE DECISÃO EM SITUAÇÕES EMERGENCIAIS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Informática no Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Aldri Luiz dos Santos.

CURITIBA PR

2019

Catalogação na Fonte: Sistema de Bibliotecas, UFPR
Biblioteca de Ciência e Tecnologia

S729d Batista, Agnaldo de Souza
Disseminação segura de dados pessoais vitais para apoio às tomadas de decisão em situações emergenciais [recurso eletrônico] / Agnaldo de Souza Batista – Curitiba, 2019.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em Informática.
Orientador: Aldri Luiz dos Santos.

1. Redes de computadores. 2. Redes Locais Dinâmicas (Computação). I. Universidade Federal do Paraná. II. Santos, Aldri Luiz dos. III. Título.

CDD: 004.67

Bibliotecária: Roseny Rivelini Morciani CRB-9/1585

MINISTÉRIO DA EDUCAÇÃO
SETOR SETOR DE CIENCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO INFORMÁTICA - 40001016034P5

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **AGNALDO DE SOUZA BATISTA** intitulada: **DISSEMINAÇÃO SEGURA DE DADOS PESSOAIS VITAIS PARA APOIO ÀS TOMADAS DE DECISÃO EM SITUAÇÕES EMERGENCIAIS**, após terem inquirido o aluno e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 20 de Março de 2019.

ALDRI LUIZ DOS SANTOS
Presidente da Banca Examinadora (UFPR)

MICHELE NOGUEIRA LIMA
Avaliador Interno (UFPR)

DENIS LIMA DO ROSARIO
Avaliador Externo (UFPA)

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
Setor de Ciências Exatas
Coordenação de Pós-Graduação em Informática

Para Rosângela, minha esposa, com amor e carinho.

AGRADECIMENTOS

Ao Prof. Dr. Aldri Luiz dos Santos, meu orientador, sou imensamente grato pela confiança depositada em mim desde o processo de seleção e ao longo de todo o Mestrado. Pela sua paciência, estímulo e, especialmente, compreensão das minhas limitações durante as orientações no decorrer de todo o curso de Mestrado em Informática da Universidade Federal do Paraná (UFPR).

À Profa. Dra. Michele Nogueira Lima pelos ensinamentos e estímulos dispensados durante todo o percurso do curso de mestrado enquanto coordenadora do Centro de Ciência de Segurança Computacional (CCSC) da UFPR, assim como pelos conteúdos ministrados durante sua disciplina Gerência de Redes.

Ao Programa de Pós-Graduação em Informática da Universidade Federal do Paraná, pelo auxílio administrativo que possibilitou minha participação em eventos e pela infraestrutura computacional. Agradeço também aos funcionários do departamento pelo auxílio com processos burocráticos da instituição

Aos amigos do NR2 e CCSC Andressa Vergütz, Arthur Emilio Garcete Ferreira, Benevid Felix Silva, Bruno Henrique Schwengber, Bruno Marquez Cremonezi, Cainã Passos, Carlos Alberto Pedroso Junior, Danilo Rodrigo Possati, Diego Milhomem Schmitt, Euclides Peres Farias Junior, Fernando Nakayama, Gustavo Henrique Carvalho de Oliveira, Igor Steuck Lopes, Ligia Francielle Borges, Marcos Antônio Dellazari, Mateus Pelloso, Nelson Gonçalves Prates Junior, Paulo Lenz Junior, Rafael Araújo da Silva e Yan Uehara de Moraes pela convivência, pelas argumentações e discussões técnicas e científicas, bem como pelo apoio durante o andamento das disciplinas e desenvolvimento da pesquisa.

Aos meus pais, Adão (*in memorian*) e Neuza, pelos valores e educação que me ofereceram com todo seu esforço e dedicação, mesmo diante das muitas dificuldades que se impuseram. Aos meus irmãos, Eduardo e Simone, pelo companheirismo e incentivo constante.

À minha esposa Rosângela, pela sua compreensão, confiança, dedicação e estimulo, especialmente nos momentos de grandes dificuldades. Pela sua sabedoria em me guiar e auxiliar nas tomadas de decisões ao longo de todo o curso.

RESUMO

A expansão do uso da Internet tem levado à disponibilização cada vez maior de serviços online. Muitos destes serviços em razão das suas caraterísticas de interatividade têm exigido a criação e manutenção de infraestruturas de redes locais ou globais estabelecidas dinamicamente de modo a garantir o seu funcionamento. Recentemente, tem se destacado a demanda por serviços de saúde em redes (*e-health*), dada sua importância na vida das pessoas. Por conta da natureza dos serviços prestados, o *e-health* lida com dados pessoais sensíveis e críticos, cuja segurança deve ser preservada na entrega e do acesso não autorizado. A disseminação desses dados deve observar o contexto e a urgência das informações envolvidas, visto que sua disponibilização de maneira ágil é essencial para auxiliar a definir o atendimento de saúde apropriado. Disseminar dados implica o compartilhamento de informações. Logo, é essencial garantir a disponibilidade e confiabilidade da disseminação desses dados sensíveis a terceiros diante de situações emergenciais, a fim de evitar prejuízos à saúde das pessoas envolvidas. A literatura apresenta diversas soluções para garantir esses atributos. Contudo, em geral elas são propícias para ambientes estruturados, como hospitais, que dispõem de infraestrutura para prover os atendimentos necessários às pessoas. Portanto, elas ainda não atendem adequadamente nos momentos de eventos críticos que ocorram subitamente em ambientes externos, tais como o surgimento de uma emergência até o atendimento de saúde, especialmente por conta da falta de infraestrutura, inclusive de redes de comunicação, que muitas vezes acontece nesses locais. Nesses ambientes estabelecem-se redes locais dinâmicas, cuja topologia se modifica ao longo do tempo, na medida em que as pessoas interagem entre si. Nesta fase, particularmente nas condições em que se desconhece interações passadas, caracterizadas como *Zero-Knowledge*, a adoção de abordagens distintas, que se valham de aspectos sociais das pessoas e de suas relações, contribuem nas tomadas de decisão acerca da entrega dos dados sensíveis. Esta dissertação tem como objetivo garantir uma disseminação segura de dados sensíveis em ambientes dinâmicos e não estruturados, a fim de apoiar as tomadas de decisão diante de situações emergenciais de saúde. Foram investigadas técnicas de confiança social, mecanismos de controle de disseminação de dados e o emprego de aspectos sociais das pessoas, de modo a identificar suas características, possibilidades de uso e contribuições. Assim, este trabalho apresenta um mecanismo para disseminação de dados sensíveis baseado em confiança social, denominado STEALTH (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control*), que busca controlar a disseminação dos dados sensíveis das pessoas em situações emergenciais em ambientes não estruturados. O STEALTH baseia-se em confiança social e comunidades de interesse. A confiança social, estabelecida pela similaridade de interesses dos proprietários dos dispositivos, permite a formação de comunidades de interesse e garantir a disponibilidade do serviço. Através do atributo de competência das pessoas, a confiança social possibilita ao STEALTH garantir a confiabilidade do serviço. O STEALTH foi avaliado através de simulações no NS-3 e os resultados obtidos demonstram sua capacidade de assegurar a disseminação de dados sensíveis às pessoas que possam contribuir para apoiar um atendimento eficiente no momento. Ele obteve uma confiabilidade de até 100% no acesso aos dados disseminados, uma latência máxima de 170ms e uma disponibilidade de até 100% para atender situações emergenciais.

Palavras-chave: Compartilhamento de Informações, Redes Locais Dinâmicas, Eventos Críticos, Dados Pessoais Sensíveis, Controle de Disseminação, Segurança

ABSTRACT

The rise of Internet usage has led to the increasing availability of online services. Many of these services, due to their interactivity characteristics, have required the creation and maintenance of dynamically established local or global network infrastructures in order to ensure their operation. Recently, the demand for health services in networks (e-health) has been highlighted, given their importance in people's lives. Due to the nature of the provided services, e-health handles sensitive and critical personal data, thus security must be preserved on delivery and from unauthorized access. The dissemination of these data should observe the context and the urgency of the information involved, since its availability in an agile way is essential to help define the proper attendance. Disseminating data involves information sharing. Therefore, it is essential to ensure the availability and reliability of the dissemination of such sensitive data to third parties in the event of emergency situations to avoid harm to the health of the persons involved. The literature presents several solutions to guarantee these attributes. However, they are generally conducive to structured environments, such as hospitals, which have the infrastructure to provide the services people need. Therefore, they still do not adequately attend to the moments of critical events that suddenly occur in external environments, such as the emergence of an emergency until health care, especially due to the lack of infrastructure, including communication networks, which often happens in these locations. In these environments, dynamic local networks are established, whose topology changes over time, as people interact with one another. At this stage, particularly in Zero-Knowledge conditions, when past interactions are unknown, the adoption of different approaches based on the social aspects of people and their relationships, contributes to decision-making about the delivery of sensitive data. This dissertation address to ensure a safe dissemination of sensitive data in dynamic and unstructured environments, in order to support decision making in the face of emergency health situations. Social trust techniques, data dissemination control mechanisms and the use of social aspects of people were investigated, in order to identify their characteristics, possibilities of use and contributions. Thus, this work presents a mechanism for the dissemination of sensitive data based on social trust, called STEALTH (**S**ocial **T**rust-Based **HEALTH** Information Dissemination Control), to control the dissemination of sensitive data in emergency situations in unstructured environments. STEALTH is based on social trust and communities of interest. Social trust, established by the similarity of interests of the owners of the devices, allows the formation of communities of interest and guarantee the availability of the service. Through people's competence attribute, social trust enables STEALTH to guarantee the reliability of the service. STEALTH was evaluated through simulations in NS-3 and the results demonstrate its ability to ensure the dissemination of sensitive data to people who can contribute in supporting efficient patient care at the time. It has achieved up to 100% reliability in accessing disseminated data, a maximum latency of 170ms and up to 100% availability for emergency situations.

Keywords: Information Sharing, Dynamic Local Networks, Critical Events, Critical Data, Dissemination Control, Safety

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks (IPv6 sobre redes sem fio pessoais de baixa potência)
ABAC	Attribute-Based Access Control (Controle de acesso baseado em atributo)
BtG	Break-the-Glass (Quebre o vidro)
CoI	Community of Interest (Comunidade de Interesse)
DINF	Departamento de Informática
GPS	Global Positioning System (Sistema de posicionamento global)
IEEE	Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Elétricos e Eletrônicos)
IDS	Intrusion Detection System (Sistema de Detecção de Intrusão)
IMD	Implantable Medical Devices (Dispositivos Médicos Implantáveis)
INTI	**I**nstrusion detection for Si**N**khole attacks over 6LoWPAN for Interne**T** of Th**I**ngs (Detecção de intrusão de ataques Sinkhole em 6LoWPAN para Internet das Coisas)
IoT	Internet of Things (Internet das Coisas)
IPv4	Internet Protocol - version 4 (Protocolo de Internet - versão 4)
MANET	Mobile Ad Hoc Network (Rede Ad Hoc Móvel)
NS-3	Network Simulator 3 (Simulador de Rede 3)
PBAC	Policy-Based Access Control (Controle de acesso baseado em política)

PPGINF	Programa de Pós-Graduação em Informática
P2P	Peer-to-Peer (Par-a-Par)
QoS	Quality of Service (Qualidade de Serviço)
QS^2	Quorum Systems, Quorum Sensing Sistema de quórum, quórum de sensoreamento
RBAC	Role-Based Access Control (Controle de acesso baseado em papel)
RFID	Radio-Frequency Identification (Identificação por rádio frequência)
SRBAC	Spatial-RBAC (RBAC Espacial)
STEALTH	**S**ocial **T**rust-Based H**EALTH** Information Dissemination Control (Controle de disseminação de informações de saúde baseado em confiança social)
TBAC	Trust-Based Access Control (Controle de acesso baseado em confiança)
UFPR	Universidade Federal do Paraná
UCON	Usage Control (Controle de uso)
VANET	Vehicular Ad hoc Network (Rede Ad hoc veicular)
WBAN	Wireless Body Area Network (Rede Corporal Sem Fio)
WLAN	Wireless Local Area Network (Rede Local Sem Fio)
WSN	Wireless Sensor Network (Rede de Sensores Sem Fio)

LISTA DE SÍMBOLOS

α	alfa, primeira letra do alfabeto grego
β	beta, segunda letra do alfabeto grego

SUMÁRIO

1 INTRODUÇÃO

A expansão do uso da Internet entre as pessoas tem levado à disponibilização cada vez maior de serviços online por parte de empresas, sejam elas privadas ou públicas, bem como na esfera governamental. Geralmente esses serviços coletam e entregam dados, muitas vezes por contatos oportunísticos, quando as interações permitem a comunicação com pessoas próximas geograficamente (Garyfalos e Almeroth, 2008). Contudo, entregar dados implica seu compartilhamento e exige observar questões como a frequência, o local e o conteúdo a ser disseminado (Vivekavardhana e Sudhindra, 2014). Muitos destes serviços, em razão das suas caraterísticas, naturalmente têm exigido a criação e a manutenção de redes locais ou globais, estabelecidas dinamicamente, de modo a garantir o seu funcionamento. Nesse contexto, a área de saúde oferece uma variada gama de serviços em redes como o agendamento de consultas, a obtenção de resultados de exames realizados, e, recentemente, direciona a atenção ao monitoramento remoto das condições de saúde das pessoas, com destaque ao acompanhamento do estado dos pacientes (Gharaibeh et al., 2017). Assim, as aplicações médicas auxiliam nos cuidados com a saúde, englobando a monitoração contínua, o diagnóstico médico e o desempenho físico humano (Movassaghi et al., 2014) (Innovation, 2016).

Os serviços de saúde em redes gradativamente auxiliam a acompanhar remotamente o estado de saúde dos cidadãos e os *feedbacks* auxiliam a mudar comportamentos nocivos ao seu bem estar (Mosenia, 2017). Para isso, eles têm adotado algumas soluções para as situações do dia-a-dia das pessoas de modo a apoiar a prevenção e o acompanhamento do estado da saúde das pessoas; entre elas destacam-se aquelas orientadas ao atendimento de situações emergenciais em ambientes externos aos ambientes hospitalares, que tratam de situações de saúde das pessoas e que muitas das vezes demandam uma resposta rápida. Esse atendimento é aquele prestado a pessoas em situação emergencial fora de um ambiente hospitalar ou de uma infraestrutura de saúde. Normalmente, o atendimento emergencial é prestado em tempo real por pessoas consideradas adequadas que estejam próximas do local do evento, conforme sua competência, não necessariamente em saúde. Pessoas adequadas são aquelas que possuem interesse em saúde, independente de sua competência específica nessa área, e acessam os dados sensíveis de pessoas em situação emergencial na medida da sua competência em saúde. A efetividade do atendimento emergencial varia conforme o estado emergencial observado.

O serviço *Bon Samaritan*, oferecido pelo Corpo de Bombeiros da cidade de Haute-Saône na França (l'est Republicain, 2018), é um exemplo de *e-health*. Ele está disponível na cidade de Paris, desde 2016, e na cidade de Lot-et-Garonne, desde outubro de 2017. Seu objetivo é prover acesso a um desfibrilador próximo da pessoa que se encontra em uma situação emergencial. O *Bon Samaritan* depende de uma infraestrutura prévia de rede e de acesso à Internet. Isso possibilita aos usuários usarem serviço e contribuírem no atendimento a outras pessoas que necessitem de ajuda. O *Bon Samaritan* atua como um complemento àqueles serviços prestados em ambientes hospitalares e afins, que possuem infraestrutura para atendimento especializado, inclusive de redes, por exemplo.

A preservação da segurança dos dados em locais fora dos ambientes hospitalares torna-se um grande desafio, especialmente diante da possibilidade de ausência de infraestrutura, como de redes, por exemplo. Contudo, prover segurança demanda garantir os seguintes atributos aos dados - confidencialidade, disponibilidade e integridade (Avizienis et al., 2004). Esse trabalho busca oferecer um serviço de disseminação de dados robusta (do inglês, *dependability*), por meio da garantia das suas propriedades de confiabilidade e disponibilidade, e segura (do inglês, *safety*),

através da garantia da sua propriedade de disponibilidade. Segundo Avizienis et al. (2004), a robustez de um sistema é sua habilidade de evitar falhas no serviços que sejam mais frequentes e mais severas que o aceitável. Ainda segundo os autores, a robustez abrange os seguintes atributos: disponibilidade, confiabilidade, segurança (do inglês, *safety*, integridade e mantenabilidade. Por disponibilidade entende-se a prontidão para o serviço correto, enquanto a confiabilidade indica a continuidade do serviço correto.

Em condições de grande mobilidade dos dispositivos, a robustez e a garantia da entrega dos dados estão associadas ao espaço - localização dos dispositivos - e ao tempo - instante da interação entre dispositivos. Além disso, recentemente, o aumento expressivo no volume de dados gerados pelas pessoas passou a incorporar as informações temporais relativas a esses dados, possibilitando a caracterização de redes dinâmicas, como as redes de sensores (do inglês, *Wireless Sensor Networks* - WSN), que coletam dados de diferentes naturezas continuamente ao longo do tempo, tomando decisões localmente e encaminhando dados às unidades de controle centrais; e as redes de produção coletiva, do inglês *crowdsourcing*, onde a participação das pessoas varia ao longo do tempo. Essas redes consideram que as interações sociais das pessoas evoluem ao longo do tempo, assim como sua mobilidade, influenciando na topologia da rede (Rossetti e Cazabet, 2018). Logo, o acesso ubíquo aos dados nessas redes é influenciado por fatores, como o momento que ele ocorre, as interações entre as pessoas nesse instante e sua localização.

A literatura apresenta diversas abordagens com o objetivo de garantir a segurança dos dados em ambientes de redes, tanto naqueles estruturados, como não estruturados. Entre as abordagens disponíveis, encontram-se o emprego de mecanismos de autenticação de usuários, a criptografia dos dados e o uso de mecanismos de controle de acesso. Os mecanismos de controle de acesso miram a expansão do uso das redes sociais, na medida do emprego dos atributos sociais oriundos das pessoas e de suas relações para identificá-las ou obter padrões de comportamento. Os indicadores de confiança das pessoas são obtidos por meios desses atributos e são elaborados a partir de diversas técnicas, tais como *reputação* (Son et al., 2017; Truong et al., 2017), *recomendação* (Al-Hamadi e Chen, 2017) e *comunidades de interesse* (Bao et al., 2013), entre outras. Dessas técnicas, as baseadas em reputação são as mais aplicadas. Elas consideram as opiniões de vários nós da rede, que representam os dispositivos dentro da rede, sobre um determinado nó para medir a confiança nele. Nas técnicas baseadas em recomendação, um nó recomenda o uso de outro nó observando experiências anteriores semelhantes que já manteve com ele. Para que sejam empregadas, essas duas técnicas dependem de informações obtidas de maneira indireta, ou seja, um nó depende de outro nó da rede para medir a confiança de um terceiro nó, por exemplo. Logo, tratam-se de técnicas apropriadas às redes estáticas ou nas quais a mobilidade dos nós seja reduzida, onde a manutenção de um histórico de interações entre os nós seja viável, isto é, ambientes estruturados. Nas comunidades de interesse, os nós da rede agrupam-se por interesses em comum que possuem, relacionados aos proprietários dos dispositivos quando das interações entre eles. Esse comportamento reduz a necessidade de manutenção de um histórico de interações da rede, ou seja, considera-se que as interações anteriores são desconhecidas - *Zero-Knowledge* (Feige et al., 1988), ou seja, há informações apenas de interações atuais. Esse contexto vai ao encontro das características presentes em um ambiente sem qualquer infraestrutura de rede. A dinamicidade das redes faz com que essas comunidades variem ao longo do tempo conforme os interesses em comum entre os proprietários dos dispositivos, restringindo a comunicação, em grande medida, aos membros dessas comunidades (Bao e Chen, 2012a) (Bao e Chen, 2012b) (Bao et al., 2013). Essa técnica dirige-se aos ambientes de rede dinâmicos, não estruturados, onde a mobilidade dos dispositivos frequente, contribuindo para a robustez na disseminação de dados nesses contextos.

A dinamicidade das redes possibilita a formação de várias comunidades de interesse ao longo do tempo, conforme os interesses dos proprietários dos dispositivos. Segundo Chakraborty et al. (2017), essas comunidades são disjuntas ou não sobrepostas, sobrepostas, hierárquicas e locais. Nesse conjunto destacam-se as comunidades de interesse sobrepostas, cujos membros possuem vários interesses e, assim, participam de mais de uma comunidade simultaneamente. Além disso, as comunidades são abordadas a partir de diversas perspectivas, tais como dos interesses dos seus usuários, de cliques e de si próprias (Wang et al., 2018). Os aspectos sociais oriundos das pessoas e de suas relações sociais são empregados em apoio à tomada de decisão acerca da disseminação dos dados ou do uso de recursos disponíveis nas redes. Eles são usados para auxiliar na garantia da disponibilidade e confiabilidade dos dados. Os controles de acesso baseados em atributos, papéis, controle de uso e confiança, dentre outros fatores. Aqueles baseados em confiança empregam os aspectos sociais como critério para concessão de acesso aos recursos da rede. Esse procedimento permite uma troca segura de informações entre entidades que venham a criar uma relação de confiança entre si (Bernabe et al., 2016). As comunidades de interesse adaptam-se à escalabilidade da rede, visto que os nós em comunidade necessitam manter informações somente do subconjunto de nós com os quais interagem (Bao et al., 2013).

1.1 PROBLEMA

Nas doenças humanas, quando ocorrem transições críticas no estado estável das pessoas, tais como alterações na frequência dos seus batimentos cardíacos, limites críticos são ultrapassados repentinamente, vindo a serem interpretados como mudanças abruptas no seu estado da saúde (van de Leemput et al., 2014). Assim, a identificação antecipada de eventos críticos atinge seu ápice quando ocorre a entrega imediata dos alertas médicos aos profissionais de saúde (Cavallari et al., 2014), ou seja, quanto antes esses alertas médicos referentes a aqueles eventos sejam detectados pelos centros hospitalares, maiores são as chances de prevenir os pacientes de futuras implicações na sua saúde (Health Organization, 2015). Dada sua natureza emergencial, os alertas médicos demandam sua transmissão imediata (Movassaghi et al., 2014), aceitando uma latência máxima de 125 milisegundos (Association et al., 2012). Eventuais perdas ou atrasos desses alertas acarretam consequências graves na saúde dos pacientes (Latré et al., 2011).

As condições de saúde das pessoas mudam a qualquer momento e local diante de eventos críticos, que são aqueles eventos que ocorrem, seja diretamente com a pessoa ou ao seu redor, e levam-na à uma situação emergencial. Nos ambientes hospitalares, há infraestrutura disponível, seja de profissionais e equipamentos de saúde, bem como de redes.As providências necessárias para um atendimento emergencial são adotadas rapidamente. Contudo, fora desses ambientes, o suporte ao atendimento à uma situação emergencial enfrenta diversos desafios, tendo em vista a falta de infraestrutura de toda ordem em alguns locais. Nesses casos, desde um evento crítico até o instante da prestação do atendimento emergencial, a pessoa fica sem qualquer apoio de saúde. Essa condição se agrava na ocorrência de conflitos urbanos, quando diversas pessoas podem ferir-se simultaneamente, por exemplo. Nesses casos, geralmente a infraestrutura existente para atendimento de saúde é insuficiente diante da demanda das situações emergenciais, exigindo a tomada de decisões sobre a prioridade que deve ser adotada para a realização dos atendimentos.

O atendimento à uma situação emergencial fora do ambiente hospitalar é impactado pela ausência de infraestrutura apropriada. Nesse cenário, diante de um evento crítico, uma pessoa em condições normais de saúde entra em uma situação emergencial em um dado momento, t_e, como ilustrado na Figura 1.1. Essa pessoa permanece nessa condição até o momento em que ocorre o atendimento especializado, t_a, que é aquele atendimento à pessoas em situação emergencial prestado por profissional de saúde com a devida competência. Durante esse tempo,

os dados sensíveis da pessoa são úteis para um atendimento emergencial, se acessados por um cidadão qualquer, que esteja próximo, e no menor tempo possível. Os sinais vitais da pessoa, por exemplo, são coletados por algum dispositivo junto ao seu corpo, ou alguma informação de identificação são disseminados a um cidadão próximo. Esse atendimento será eficaz na medida da competência em saúde do cidadão e seria prestado em tempo real. Todavia, o acesso a esses dados deve ocorrer imediatamente ou no menor tempo possível. Portanto, o principal problema abordado nesta dissertação consiste em **como garantir a disseminação segura de dados sensíveis pessoais em ambientes dinâmicos e não estruturados em apoio às tomadas de decisões diante de situações emergenciais de saúde**.

Figura 1.1: Evolução das condições de saúde de uma pessoa

A literatura apresenta várias soluções para resolver esse problema. Uma delas envolve o emprego da política chamada Quebre o Vidro (do inglês, *Break-the-Glass* - BtG) (Security e Committee, 2004). Ela prevê que um usuário ignore um mecanismo de controle de acesso diante de um problema de saúde observado. Ela considera que, como a pessoa já se encontra em situação de emergência médica, não haveria motivos para negar acesso aos seus dados médicos. Porém, o uso dessa política de maneira arbitrária impacta diretamente na segurança dos dados pessoais (Carminati et al., 2016, 2013). Khaliq et al. (2017) propuseram o emprego de redes veiculares em apoio à situações emergenciais. Nesses casos, os veículos servem como ponto de acesso do usuário ao serviço de monitoração mantido em um ambiente hospitalar. Nesses casos, além do atendimento emergencial ser dependente da proximidade do veículo com a pessoa que dele necessita, também demanda a existência de uma rede *ad hoc* veicular (do inglês, *Vehicular Ad hoc Network* (VANET)), ou seja, trata-se de uma solução para um ambiente estruturado. Vimalachandran et al. (2017) propuseram que o próprio proprietário das informações de saúde controle o acesso a elas. Os resultados serão satisfatórios enquanto o proprietário das informações estiver em boas condições de saúde. Ainda assim, ele estará restrito àquelas pessoas das quais detenha alguma referência ou indicação para concessão do acesso. Isso se agrava em ambientes esparsos e dinâmicos. Em situações emergenciais, o proprietário das informações não estará em condições de verificar quem solicita acesso a elas ou até possibilitar acesso a um indivíduo qualquer que esteja próximo. Diante disso, as seguintes questões precisam exploradas:

- *Em que medida disseminar dados em situação emergencial em ambientes urbanos contribui para atendimentos emergenciais de saúde?*

  Situações emergenciais ocorrem a qualquer momento e local, especialmente em ambientes urbanos, fora de unidades de saúde. Nesses locais, muitas vezes as infraestruturas de apoio inexistem, inclusive redes. Assim, a prestação de um atendimento emergencial eficiente é dificultada. Até que esse atendimento ocorra, uma pessoa em situação emergencial dispõe de dados, principalmente seus sinais vitais, que auxiliam em um primeiro atendimento por algum indivíduo próximo. Nessa condição, essa pessoa atuará na medida da sua competência em saúde. Se ela não possuir qualquer competência nessa área, terá acesso a um contato telefônico de emergência da pessoa em situação emergencial e informá-la da sua situação. Contudo, para que isso ocorra, há necessidade

de se ter acesso aos dados da pessoa em situação emergencial, sejam seus sinais vitais ou algum contato de emergência, por exemplo. Assunm disseminar esses dados nessas condições auxilia nos atendimentos emergenciais de saúde na medida que complementa os serviços de saúde já existentes, contribuindo para um atendimento mais eficaz.

- *Quais são os desafios de disseminar dados em ambientes urbanos e esparsos?*

  As dimensões espaciais e temporais influenciam na disponibilidade de serviços em redes em ambientes urbanos e esparsos. A mobilidade das pessoas altera frequentemente sua localização espacial ao longo do tempo e implica disseminar dados a pessoas distintas, conforme essa necessidade se impõe. Assim, a verificação de uma pessoa adequada para a qual os dados de um indivíduo em situação emergencial serão disseminados nesses ambientes precisa ser um processo cíclico, que demanda medidas específicas. A dinamicidade das redes locais nesses ambientes sofre impacto direto da mobilidade das pessoas e inviabiliza a manutenção de um histórico de suas interações. Logo, as interações anteriores são quase que desconhecidas nesses ambientes, configurando-se uma condição *Zero-Knowledge* (Feige et al., 1988). Eventuais interações anteriores entre dispositivos da rede são insuficientes ou os padrões de comportamento não são passíveis de avaliação, restringindo o apoio às tomadas de decisões para controlar a disseminação dos dados daqueles indivíduos.

- *Como lidar com ambientes urbanos e esparsos para disseminar dados de maneira robusta?*

  As abordagens tradicionais focam na disseminação de dados em instituições de saúde. No entanto, disseminar dados de maneira robusta em ambientes urbanos e esparsos requer soluções distintas. É vital prover uma infraestrutura de rede, ainda que eventual, para que os dados possam ser disseminados. A mobilidade dos dispositivos, sua participação intermitente na rede e a ausência de uma entidade central para garantir a segurança na disseminação dos dados, entre outros fatores, devem ser considerados. Portanto, esses ambientes dinâmicos demandam o emprego de abordagens que empreguem informações que as pessoas detém consigo ao longo do tempo, considerando que históricos de interações passadas nem sempre estarão disponíveis. Aspectos sociais das pessoas - individuais e relacionais -, por conta da sua participação em redes sociais, são úteis na verificação do seu comportamento. Além disso, eles viabilizam a obtenção de indicadores de confiança, a serem usados como critérios para a disseminação dos dados.

1.2 OBJETIVOS

Esta dissertação tem como objetivo garantir uma disseminação segura de dados sensíveis em ambientes dinâmicos e não estruturados, a fim de apoiar as tomadas de decisão diante de situações emergenciais de saúde. A base para garantia da segurança na disseminação dos dados está na segregação da rede em agrupamentos formados mediante aspectos sociais e no emprego de um mecanismo de controle de disseminação de dados baseado em confiança. O controle de acesso aos dados ocorre na perspectiva de que os dados são disseminados somente às pessoas adequadas, ou seja, uma pessoa recebe os dados na medida de sua competência em saúde. Essa estratégia considera a dinamicidade das redes e a mobilidade de seus dispositivos ao longo do tempo, adaptando-se às redes não estruturadas móveis. Estruturas temporais como grafos podem ser empregados para representar essas redes, incorporando sua dinamicidade ao longo do tempo

(Latapy et al., 2018). Para atingir o objetivo proposto, os seguintes objetivos específicos foram estabelecidos:

- Investigar as técnicas de confiança social empregadas em ambientes de rede não estruturados e dinâmicos, a fim de compreender suas características, princípios de operação, qualidades e limitações.
- Investigar os mecanismos de controle de disseminação para redes, de modo a verificar as possibilidades de emprego em ambientes de rede não estruturados e dinâmicos.
- Investigar o emprego de aspectos sociais das pessoas no controle da disseminação dos dados, de modo a identificar suas características e contribuições em ambientes de rede não estruturados e dinâmicos.

1.3 CONTRIBUIÇÕES

O desenvolvimento dessa dissertação resultou em contribuições científicas na área de computação, com enfase em redes sem fio não estruturadas e segurança de redes. A seguir, as contribuições deste trabalho estão descritas de forma detalhada:

- Um estudo do estado da arte da literatura sobre o uso de técnicas de confiança em redes não estruturadas. Essas técnicas foram classificadas de acordo com os tipos de redes pesquisados: Internet das Coisas, Par-a-Par e MANETs. Os requisitos essenciais para a garantia da segurança foram verificados por esse estudo, isto é, a garantia da disponibilidade e confiabilidade na disseminação de dados em redes dinâmicas.
- Proposição do STEALTH, um mecanismo para disseminação segura de dados sensíveis de pessoas diante de uma situação emergencial em ambientes dinâmicos. Ele compreende duas fases distintas - *a manutenção das comunidades de interesse* e *a gestão de eventos críticos*. Essas duas fases associadas suportam a disponibilidade do serviço de disseminação de dados sensíveis à pessoas adequadas diante de situações emergenciais.
- Avaliação e análise da eficácia do STEALTH na disseminação de dados sensíveis de maneira robusta diante de situações emergenciais realísticas. Foram analisados três cenários distintos, onde o primeiro cenário representou uma situação onde os dados são disseminados sem haver uma confirmação de que foram acessados por uma pessoa adequada. O segundo cenário considera a disseminação dos dados sensíveis levando em conta a necessidade de confirmação do do recebimento dos dados pela pessoa adequada. Em ambos os cenários, os acessos aos dados ocorreu na ordem de recebimento pela pessoa adequada. No último cenário, avaliou-se o acesso aos dados diante da tomada de decisão quanto à ordem do atendimento emergencial frente ao recebimento simultâneo de dados sensíveis de várias pessoas em situação emergencial, seja pela ordem de chegada desses dados e por uma ordem de prioridade pré-definida.

1.4 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada em seis capítulos. O Capítulo 2 apresenta os fundamentos imprescindíveis ao entendimento do contexto de solução apresentada. Ele descreve as características gerais das redes e as formas de agrupar dispositivos, além de conceitos na área de saúde móvel. Além disso, alguns domínios de redes não estruturadas são abordados. O capítulo

finaliza detalhando o uso de confiança em redes e as técnicas mais comuns encontradas na literatura. O Capítulo 3 apresenta o estado-da-arte do uso da confiança em redes não estruturadas. Diversos trabalhos foram alvo de pesquisas e estudos. Eles propiciaram a avaliação das possibilidades de uso dessa técnica, assim como das técnicas de disseminação de dados mais comuns encontradas na literatura. O Capítulo 4 detalha o mecanismo proposto, que emprega atributos e técnicas de confiança social, além de comunidades de interesse para controlar a disseminação dos dados sensíveis de saúde das pessoas. O Capítulo 5 descreve o processo de avaliação do mecanismo implementado, detalhando o cenário empregado e as métricas selecionadas para mensurar os resultados. Por fim, o Capítulo 6 conclui essa dissertação com as considerações finais, possibilidades de trabalhos futuros e cenários de aplicação.

2 FUNDAMENTOS

Este capítulo apresenta os fundamentos necessários à compreensão e entendimento dos assuntos envolvidos nessa pesquisa, especialmente acerca do problema constatado. A Seção 2.1 rever os conceitos e as abordagens comuns sobre agrupamento de dispositivos em redes. A Seção 2.2 destaca as particularidades do cenário da saúde móvel, especialmente em redes móveis não estruturadas. A Seção 2.3 apresenta os conceitos relacionados ao controle de disseminação de dados em redes. A Seção 2.4 aborda conceitos de segurança em redes e as ameaças à sua garantia. A Seção 2.5 destaca as técnicas de confiança existentes, bem como as formas de mensuração e construção.

2.1 AGRUPAMENTO DE DISPOSITIVOS

Os dispositivos conectados em redes agrupam-se e desagrupam-se diante de suas necessidades de comunicação, conforme o comportamento de seus proprietários. Como essa comunicação acontece de maneiras distintas ao longo do tempo, ela influencia na formação desses agrupamentos, que são dinâmicos por natureza. Em razão dos dispositivos conectarem-se às redes de forma intermitente, o chamado efeito *churn*, isso contribui para a dinamicidade dos agrupamentos formados. Esses agrupamentos, também conhecidos como comunidades, formam-se baseados em algum critério ou interesse em comum dos proprietários dos dispositivos. São formados, também, por leituras similares, como nas redes de sensores sem fio, agilizando a consulta de dados em ambientes urbanos (Carrero et al., 2015) (Gielow et al., 2015) Furlaneto et al. (2012). Logo, os interesses e mudanças de comportamento das pessoas refletem-se na operação dos seus dispositivos dentro da rede, impactando na construção dos agrupamentos. Além disso, as relações sociais das pessoas ao longo do tempo promovem interações entre seus dispositivos, que também mantêm relações entre si. Isso faz com a dimensão temporal tenha grande importância na análise do comportamento da construção dessas comunidades (Rossetti e Cazabet, 2018).

2.1.1 Comunidades de Interesse

Os dispositivos conectam-se em redes para compartilhar informações e acessar aos recursos ali disponíveis (Bao e Chen, 2012b,a; Bao et al., 2013). Para isso, sua mobilidade exerce um papel crítico na disseminação das informações, pois impacta tanto na forma como as mensagens irão trafegar, como no conteúdo dos dados envolvidos, expondo-os a dispositivos diversos e muitas vezes desconhecidos. Esse impacto se estende em alguma medida à segurança dos dados envolvidos. Isso exige contramedidas para que ela seja garantida no ambiente, conforme os requisitos previstos para os serviços envolvidos.

Os dispositivos conectam-se às redes baseados em características ou comportamentos de seus proprietários, além daquelas relacionadas à sua interface de rede, aos protocolos de comunicação, ao tipo da rede existente, à disponibilidade de acesso, entre outras. Isso leva à criação de comunidades de dispositivos baseadas em algum interesse comum existente entre essas pessoas, tais como música, profissão ou amizade, por exemplo. Como ilustra a Figura 2.1, baseada nos trabalhos de Bao e Chen (2012a,b) e Bao et al. (2013), os dispositivos nas comunidades criam relações de confiança entre si e, enquanto pertencerem à uma comunidade, eles manterão a conectividade entre si. Logo, reduzem sua computação às interações relacionadas ao subconjunto

de dispositivos pertencentes à comunidade (Bao e Chen, 2012a,b; Bao et al., 2013). Essa forma de agrupamento de dispositivos é conhecida como Comunidade de Interesse (CoI).

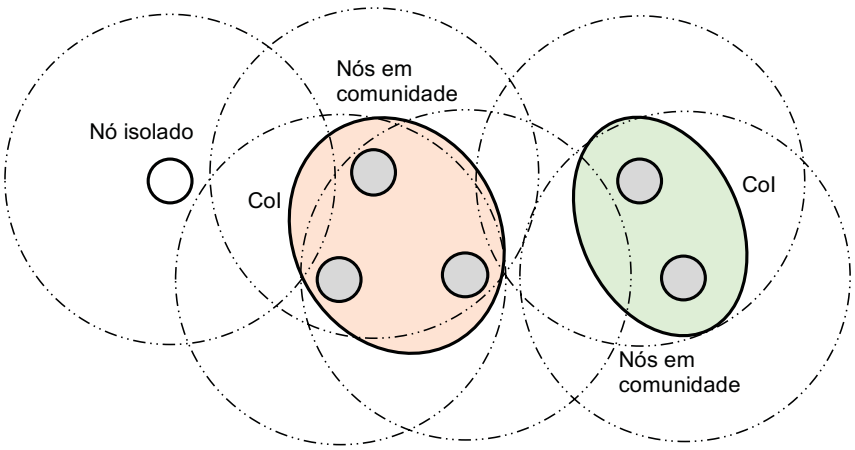


Figura 2.1: Comunidades de interesse

As relações construídas entre os dispositivos com interesses em comum durarão enquanto eles estiverem conectados entre si. Isso acontece enquanto a rede estiver ativa ou em frações desse tempo. A mobilidade dos dispositivos e as mudanças de interesses dos seus proprietários tornarão essas comunidades dinâmicas, sendo formadas e modificadas ao longo do tempo. Observar a evolução da rede, da sua ativação até o momento que ela deixa de funcionar, permite monitorar o comportamento dos dispositivos e de suas relações. As interações ocorridas representam uma espécie de memória ou histórico do funcionamento da rede, que é incorporada, em alguma medida, à avaliação dessas relações, auxiliando na segurança dos dados disseminados.

As comunidades que se estabelecem no mundo real são de diversos tipos: disjuntas ou não sobrepostas, sobrepostas, hierárquicas e locais (Chakraborty et al., 2017). Essa classificação varia conforme a interação entre os dispositivos e as comunidades estabelecidas. As Figuras 2.2 a 2.5, elaboradas baseadas no trabalho de Chakraborty et al. (2017), ilustram as características principais de cada tipo. As comunidades disjuntas ou não sobrepostas são isoladas umas das outras, ou seja, os nós pertencem a apenas uma comunidade (Fortunato, 2010), como se observa na Figura 2.2. As comunidades C_1 e C_2 são distintas, pois cada uma possui um conjunto de nós diferente. Um exemplo desse tipo de comunidade são alunos que participam de diferentes disciplinas em uma escola. Por outro lado, nas comunidades sobrepostas a situação é distinta, pois os nós podem pertencer à diferentes comunidades simultaneamente. A Figura 2.3 representa essa situação, onde o nó 3 pertence às comunidades C_1 e C_2. Uma pessoa que participa de diferentes grupos sociais em uma rede social é um exemplo desse tipo de comunidade (Chakraborty et al., 2017) (Chakraborty et al., 2012) (Xie et al., 2013).

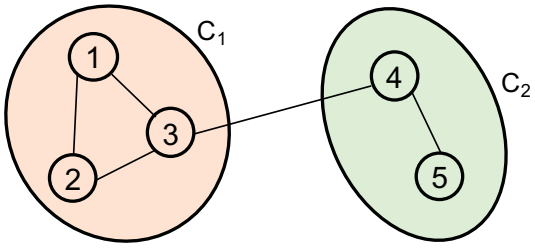


Figura 2.2: Comunidades disjuntas ou não sobrepostas (Chakraborty et al., 2017)

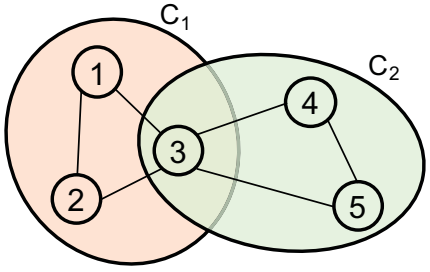


Figura 2.3: Comunidades sobrepostas (Chakraborty et al., 2017)

As comunidades hierárquicas são estruturas cujos grafos são vistos em múltiplos níveis, quando é escolhida uma estrutura de comunidade em particular (Balcan e Liang, 2013). Esse procedimento depende da aplicação em uso. A Figura 2.4 apresenta duas grandes comunidades em níveis distintos, que possuem duas comunidades cada uma. A comunidade C_1 possui as comunidades $C_{1.1}$ e $C_{1.2}$, enquanto a comunidade C_2, as comunidades $C_{2.1}$ e $C_{2.2}$. As células do corpo humano são exemplos desse tipo de comunidade, pois formam tecidos, que formam outros órgãos e assim por diante. As comunidades locais não apresentam qualquer estrutura quando vistas globalmente, mas possuem diferentes estruturas sob uma perspectiva local (Reichardt e Bornholdt, 2004), como ilustra a Figura 2.5. Observa-se localmente a existência da comunidade C_1 formada pelos nós 1, 2 e 3. Contudo, conforme as necessidades locais, ela se forma por outros nós dentre aqueles existentes, como por exemplo, 3, 4 e 5. Uma pessoa que mantém relações desiguais com certos membros de uma rede social configura uma comunidade local.

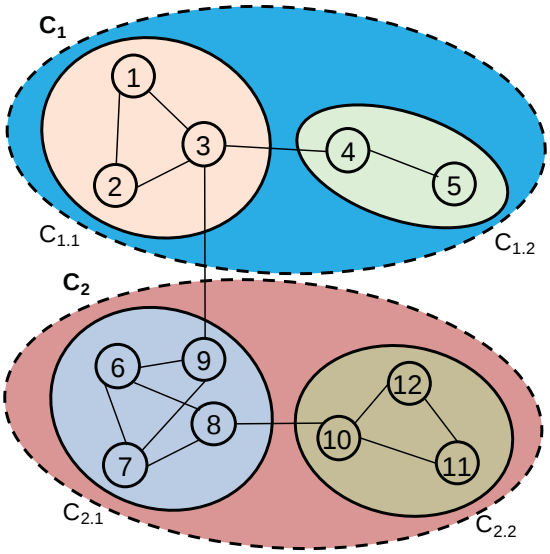


Figura 2.4: Comunidades hierárquicas (Chakraborty et al., 2017)

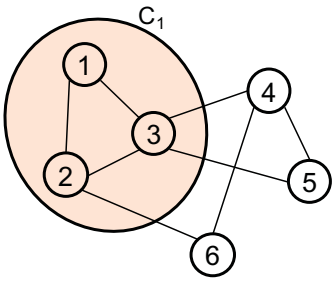


Figura 2.5: Comunidades locais (Chakraborty et al., 2017)

2.2 SAÚDE MÓVEL

Os serviços de saúde vêm passando por diversas mudanças na forma como interagem com os profissionais de saúde e, principalmente, com os pacientes. Eles estão evoluindo a partir de uma perspectiva centrada nos hospitais e clínicas para se centrarem nos pacientes (Farahani et al., 2017). Como as redes trazem para esse ambiente diversas características inerentes ao seu contexto, especialmente a mobilidade dos dispositivos e sua dinamicidade, elas contribuem para a evolução dos serviços prestados. Logo, a mobilidade dos dispositivos possibilita tratamento médico onde quer que as pessoas estejam, seja pelo monitoramento da sua saúde ou pela prestação de atendimentos de emergência, visto que os dados são acessados de maneira ubíqua. A interação entre dispositivos computacionais móveis e as pessoas tem sido intensificada e estabelecido redes locais temporárias, onde se trocam informações com diferentes propósitos e normalmente por um certo período de tempo. Dispositivos móveis, como *smartphones*, dada sua presença massiva, coletam vários tipos de dados (Ruiz-Ruiz et al., 2014) a fim de apoiar melhorias nos serviços de vigilância, transportes e saúde, entre outros. Particularmente nos serviços de saúde, os *smarphones* possibilitam interconectar dispositivos médicos das pessoas à Internet (Wood et al., 2017).

As informações relativas à uma pessoa no âmbito da saúde englobam dados de diversas características e origens. Além de identificar a pessoa, também representam suas condições de saúde ao longo da vida, a saúde de sua família, sua localização e outras situações relacionadas. Os equipamentos médicos, associados aos profissionais de saúde, pessoal técnico e administrativo que trabalham em instituições de saúde, geram um grande volume de informações. Há os sinais vitais, que incluem batimentos cardíacos, pressão arterial e nível de glicose (Farahani et al., 2017), os dados de identificação (Cole et al., 2017), (Zrelli et al., 2017), dados bancários e os dados de localização (Al-Hamadi e Chen, 2017), entre outros. Os sinais vitais permitem aos profissionais de saúde avaliarem as condições de saúde das pessoas e, se for o caso, prescrever tratamentos para o restabelecimento de sua saúde às condições normais. Esses sinais são sensíveis dada sua natureza e características. Além disso, devem estar disponíveis para uso no menor tempo possível, para que sua aplicação de maneira eficiente e eficaz em situações de emergência ocorra com sucesso. Por outro lado, eles não devem ser acessados por pessoas não autorizadas, pois comprometeria a sua segurança (Carminati et al., 2016) e a privacidade de seu proprietário.

2.3 CONTROLE DE DISSEMINAÇÃO

O compartilhamento de informações nos ambientes de redes envolve várias questões importantes. Dentre elas, segundo B e Sudhindra (2014) e Umarani e Sundaram (2013), as principais são a frequência de disseminação, o local da disseminação e o conteúdo disseminado. A frequência da disseminação é *proativa*, quando o compartilhamento da informação acontece em intervalos especificados, ou *reativa*, quando acontece a partir de algum evento específico. Quanto à localidade da disseminação, ela é *local*, se as informações são divulgadas aos nós vizinhos, ou *global*, quando as informações são propagadas para nós que estejam além do raio de comunicação do que nó que compartilha informações. Por fim, o conteúdo disseminado é uma informação *crua* ou *processada*. Em todos os casos, a disseminação dos dados ocorre por estruturas centralizadas ou distribuídas.

O controle da disseminação dos dados ocorre observando-se o contexto e as características sociais das pessoas envolvidas. Como os dispositivos geralmente são operados por pessoas, o emprego de modelos sociais, que descrevem seu comportamento de maneira mais adequada, permite disseminar dados às pessoas corretas (Bujari, 2012). Contudo, Wallgren et al. (2013) ressaltam que a disseminação de dados na IoT é sujeita à questões como links com perdas de dados, escutas não autorizadas (do inglês, *eavesdropping*) e mobilidade dos dispositivos. Assim, contramedidas devem ser adotadas para que os dados sejam disseminados corretamente e o uso de aspectos sociais das pessoas e de suas relações podem auxiliar nesse processo.

Segundo Bujari (2012), em cenários com grande mobilidade dos dispositivos de rede, o envio de dados a todos os clientes (*flooding*) é o único meio de comunicação. Estes esquema de disseminação de dados também é conhecido como epidêmico, cuja ideia por traz desse conceito é que os dados inundem (*flooding*) a rede, tal como como um vírus que se espalha em uma epidemia. Nesse caso, um nó copia sua mensagem para todos os nós com os quais entre em contato, desde que já não possuam uma cópia da mensagem. Diferente da inundação, alguns esquemas fazem uso do histórico de encontros anteriores para auxiliar na tomada de decisão durante a disseminação dos dados. Nesses casos, entende-se que um nó que encontra um outro nó várias vezes anteriormente tem uma grande probabilidade de encontrá-lo novamente no futuro.

Há diversos métodos para controlar a disseminação de dados para os usuários finais (Gharaibeh et al., 2017). Esses métodos estão relacionados à forma com que os dados são acessados. Os métodos mais comuns são os seguintes:

- *Acesso direto (Pull)*: Nesse método, os dados permanecem armazenados em bases de dados, a ser acessadas livremente ou mediante autenticação. Assim, aqueles usuários que têm interesse em algum dado, enviam uma requisição a um servidor e, posteriormente, recebem uma resposta com os dos disponíveis para a requisição realizada. Dentre os principais desafios deste método estão a autenticação de usuários, a busca por grandes volumes de dados e a garantia da corretude dos resultados;

- *Método Push*: No método *push*, os dados são enviados aos usuários sem qualquer requisição prévia de sua parte. Os usuários estão disponíveis para terem acesso aos dados, mas não têm noção se vão recebê-los ou quando isso vai acontecer. Trata-se de um método adequado para divulgação de eventos ou entrega de mensagens críticas em situações de emergências. Seu desafio é entregar os dados no tempo adequado;

- *Serviços de publicação / assinatura*: Neste método, as informações são publicadasem uma base de dados, mas sem a noção exata de quem irá acessá-las ou quando. Aquelas pessoas que são assinantes receberão os dados conforme seu interesse; e

- *Roteamento oportunístico*: Quem envia e quem recebe os dados não tem conhecimento um do outro. Isso ocorre por conta das topologias dinâmicas das redes e pelo emprego de tecnologias sem fio, que fazem com que os nós das redes não tenham noção de quem são os nós vizinhos. Esse roteamento entrega os dados nessas topologias, tomando decisões dinâmicas à medida que os dados são recebidos pelos nós intermediários.

A disseminação de dados nos ambientes de redes possui diversas características. Segundo Aksoy et al. (1998), elas descrevem os mecanismos de entrega dos dados, conforme seu funcionamento. Assim, pode-se analisar os métodos acima citados comparando-se algumas situações, que são apresentadas nos tópicos a seguir.

- *Pull do cliente vs. Push do servidor*: Enquanto no mecanismo *pull* os clientes requisitam os dados que desejam dos servidores, no *push* os dados são enviados pelo servidor de maneira antecipada ao cliente, sem qualquer requisição específica. O servidor inicia a transferência dos dados para o cliente. Logo, no mecanismo *pull* os clientes acessam os dados que desejam, enquanto no *push*, têm acesso a informações que desconhecem;

- *Periódica vs. Não periódica*: Em ambos os mecanismos *push* e *pull*, a disseminação ocorre de forma periódica ou não. A disseminação periódica ocorre mediante um agendamento prévio, conforme as necessidades do serviço oferecido, por exemplo. A disseminação não periódica é baseada em eventos, ou seja, os dados serão disseminados sempre que ocorrer um evento específico; e

- *Unicast vs. 1 para N*: No método *unicast*, os dados são enviados da sua origem diretamente a um outro dispositivo, enquanto no 1 para N, a entrega ocorre por difusão (do inglês, *broadcast*) ou para um grupo (do inglês, *multicast*). No *multicast*, os dados são enviados para um grupo específico de clientes, cujos endereços são previamente conhecidos. No *broadcast*, as informações são enviadas a um conjunto de clientes não especificado. Esses métodos atendem a escalabilidade da rede, caso vários clientes requisitem acesso às informações.

A disseminação dos dados é controlada empregando-se os mecanismos adequados às situações existentes. Assim, o envio de mensagens pelo método *push* de forma não periódica permite divulgar informações relativas à situações emergenciais diante de eventos críticos. Para

isso, os destinatários dessas mensagens devem ser previamente conhecidos, de forma que a disseminação ocorra de maneira adequada e eficaz.

2.4 SEGURANÇA EM REDES

A segurança em redes consiste em garantir seus atributos - confidencialidade, integridade e disponibilidade. Isso acontece de maneira plena, quando todos são garantidos, ou parcialmente, quando se busca garantir apenas alguns deles. O atendimento de maneira parcial cria brechas na segurança do serviço ou dispositivo como um todo (Avizienis et al., 2004). Quando a construção dos dispositivos ou serviços ocorre observando os atributos de segurança, dispositivos e serviços incorporam as melhores práticas. Isso torna-os inseguros em alguma medida, pois serão feitas adaptações em um produto pronto. No contexto da IoT, a segurança exerce um papel fundamental, especialmente no que tange à autenticação e confidencialidade dos dados. As contramedidas tradicionais de segurança não são aplicadas diretamente ao cenário da IoT, diante da diversidade de padrões de comunicação e de dispositivos (Sicari et al., 2015). Além disso, a grande quantidade de equipamentos interconectados impõe a questão da escalabilidade da rede, e exige uma infraestrutura apropriada para lidar com desafios em um ambiente dinâmico, como autenticação, controle de acesso, privacidade, entre outras (Conti et al., 2018). As MANETs também são vulneráveis a diversos tipos de ataques, devido ao meio de comunicação empregado e a limitação de recursos. A comunicação sem fio, por exemplo, é suscetível à interferências e interceptações (Lima et al., 2009).

A disseminação de dados por redes sem fio traz desafios à garantia da segurança. Ela propicia que as informações ao trafegar na rede estejam acessíveis a qualquer receptor próximo de um dispositivo transmissor (Ferreira, 2013). Nas redes cabeadas, as informações trafegam por cabos e não ficam expostas ao acesso não autorizado de modo tão explícito. Como as redes IoT baseiam-se em tecnologias sem fio, elas herdam seus problemas. Elas fazem uso do padrão IEEE 802.11, o que torna a garantia da segurança um desafio ainda maior (Sicari et al., 2015). Nas redes de sensores (do inglês, *Wireless Sensor Network*), por exemplo, há uma grande quantidade de nós, que possuem energia e capacidade de computação limitadas. Ela coleta e processa os dados, posteriormente enviando-os para processamento e avaliação por uma entidade externa através de um nó sink ou um gateway. Esse roteamento de dados é essencial (Figueiredo et al., 2005) e deve ser realizado de modo seguro.

Além disso, a disseminação de dados demanda garantir sua segurança para evitar a exposição não autorizada. O emprego de mecanismos de controle de acesso, bem como de controle da disseminação dos dados visa assegurar que o acesso a determinados dados disponíveis sejam feitos por usuários legítimos e devidamente autorizados. Isso garante a privacidade das informações trocadas, ou seja, quem disseminar a informação estará seguro de que ela estará acessível somente ao seu destinatário. Enquanto um controle de acesso se vale de políticas, papéis, confiança e outras características de quem solicita o acesso ao recurso, um controle da disseminação se vale de características dos usuários para verificar aquele a receber os dados.

2.4.1 Ameaças

As redes e seus dispositivos estão sujeitos a diversos tipos de ameaças, oriundas de falhas por mau funcionamento dos dispositivos ou da rede, falta de energia, entre outras. Essas falhas são intencionais, seja devido a um acesso ilegal, falhas de softwares e ataques de vírus, ou por falhas internas no design do seu *software* ou *firmware* (Cole et al., 2017), (Vasilomanolakis et al., 2017). As soluções presentes na literatura variam conforme a situação, compreendendo

desde a instalação de equipamentos redundantes até a replicação de dados em várias bases de dados distintas (Duarte e dos Santos, 2001). Particularmente no contexto da IoT, alguns ataques como fraude à eleição (Guo e Chen, 2015), autopromoção (Bao et al., 2013) e difamação (Bao e Chen, 2012b) visam comprometer as técnicas de confiança em uso, especialmente aquelas baseadas em reputação e recomendação.

Dentre essas ameaças, destaca-se o *Sybil*. Conhecido como ataque de personificação, ocorre quando um nó de rede assume diversas identidades de outros nós da rede, enquanto usa um único dispositivo físico. A obtenção das identidades assumidas acontece pela personificação de outros nós, a partir do momento que um nó de rede atacante acessa a rede a se passa por um outro nó, ou pelo uso de identidades falsas, furtadas ou falsificadas (Bannack et al., 2008). Em ambas as situações, o atacante torna-se um usuário autêntico e obtém acesso ao ambiente de rede. Após essa fase de autenticação, esse atacante empreende outros tipos de ataques.

Os ambientes dinâmicos oferecem diversos desafios para conter ou mitigar as ameaças à segurança dos dados disseminados nessas condições. A ausência de infraestrutura, possível de ocorrer nesses locais, associada à mobilidade das pessoas, inviabiliza a manutenção de mecanismos de controle de acesso tradicionais, comumente baseados na identificação dos usuários ou em políticas pré-estabelecidas. A participação intermitente das pessoas nas redes eventualmente estabelecidas em ambientes dinâmicos demanda a adoção de outras formas de identificação dos usuários ou, pelo menos, de avaliação de seu comportamento. Com isso, eles acessam determinados recursos disponíveis. Contudo, outras ameaças podem surgir, direcionadas às técnicas empregadas, distinguindo-se daquelas tradicionalmente encontradas na literatura.

2.5 CONFIANÇA

A confiança é estudada em várias áreas do conhecimento e usada como base para a tomada de decisão em diversos contextos. Cada disciplina a define de uma maneira diferente, mas todas possuem o objetivo comum de avaliá-la corretamente, de modo que seja robusta o suficiente para auxiliar nas tomadas de decisões (Cho et al., 2015). Se avaliada de forma inadequada, incorretamente, ela é depositada em alguém ou sobre um dispositivo não confiável, permitindo comportamentos imprevisíveis por parte dessa pessoa ou dispositivo. No entanto, a dificuldade na sua mensuração com total certeza implica algum risco às tomadas de decisões, que decorre da incerteza ou de alguma informação incompleta. Segundo Yamamoto (1990), a confiança exerce um papel crucial nas relações sociais, pois além de garantir um comportamento cooperativo, ela também maximiza os resultados nas relações entre duas entidades, levando a um círculo virtuoso de benefícios mútuos (Cho et al., 2015) (Gambetta et al., 2000).

A confiança é definida como a vontade de um avaliador de se arriscar, baseado numa crença subjetiva de que aquele em quem ele confia exibirá um comportamento confiável, a fim de maximizar o interesse do acreditador diante da incerteza de uma dada condição. Isso ocorre baseado na avaliação cognitiva de experiências passadas com o acreditado (Cho et al., 2015). Em outras palavras, um dispositivo, por exemplo, confiará em outro dispositivo se ele se comportar de maneira confiável. A avaliação dessa confiança leva em conta situações anteriores, ou seja, a existência de histórico de interações com o dispositivo que se busca avaliar.

O risco nas tomadas de decisão sempre existirá, sendo que quanto maior o risco, mais difícil será a tomada de decisão (Cho et al., 2015). Isso ocorre em razão dos prejuízos ao resultado esperado são maiores, o que afastaria o risco do objetivo final da tomada de decisão. Assim, as ambiguidades, incertezas e vulnerabilidades acerca da confiança devem ser bem avaliadas, a fim de minimizar o risco ao menor valor possível. Para tanto, diversos fatores que afetam o risco devem ser observados, tais como fé, medo, sentimento, poder, controle, cooperação, entre

outros. Nesses casos, como se tratam de fatores subjetivos, ficam sujeitos à avaliação individual e passíveis de variação de uma pessoa para outra. Outros fatores como normas, regulamentações, leis e contratos também impactam nas tomadas de decisão. Eles aumentam o risco e exigem atenção e conhecimento do agente responsável pela tomada de decisão.

A quantidade crescente de dispositivos conectados em rede exige procedimentos que envolvem o uso da confiança nesses ambientes. Isso reforça o entendimento de que os mecanismos de controle de acesso precisam ir além de somente verificar a autenticidade de um dispositivo ou usuário. Segundo Gligor e Wing (2011), a confiança nos ambientes que envolvem redes de seres humanos e de computadores deve ser construída sobre dois pilares: confiança comportamental, relacionada ao comportamento humano, e a computacional, derivada dos dispositivos. Nesse cenário, tanto o comportamento dos indivíduos, como o aspecto social das suas relações, mantidas com o suporte de redes computacionais, suscitam vários estudos. Para que a confiança possa ser usada, ela precisa ser especificada e, posteriormente, mensurada de alguma maneira. Para isso, técnicas como reputação, recomendação, confiança social, entre outras, vêm sendo empregadas.

2.5.1 Medição da Confiança

A confiança é medida de duas formas distintas: contínua ou escalar (Cho et al., 2015). Não há um padrão ou uma unidade de medida específica para essa finalidade, fazendo com que os autores busquem outras formas de mensuração. Esse procedimento vai além da simples avaliação da confiança, pois também permite comparar a conduta dos dispositivos de rede e classificá-los de alguma maneira. As formas de medição da confiança são apresentadas a seguir e permitem ao leitor compreender seus objetivos, benefícios e identificar possíveis casos de uso.

- *Confiança contínua*: Nessa forma de mensuração, a confiança varia na faixa [-1,+1], como ilustra a Figura 2.6 (Marsh e Briggs, 2009) (Cho et al., 2015). O valor 0 indica ignorância acerca da confiança, ou seja, que não se confia e nem se desconfia da outra parte. O valor -1 indica que não há confiança, enquanto que +1 indica confiança total. Há um limite entre a desconfiança e a confiança, que os autores chamam de nível de cooperação. A partir desse ponto ainda existe a possibilidade de alguma cooperação, apesar ainda não haver confiança total. Os valores entre -1 e 0 representam não confiança e há um limite de perdão entre eles. Até esse limite, ainda que não haja confiança, as entidades envolvidas aceitam a manutenção da relação entre elas.

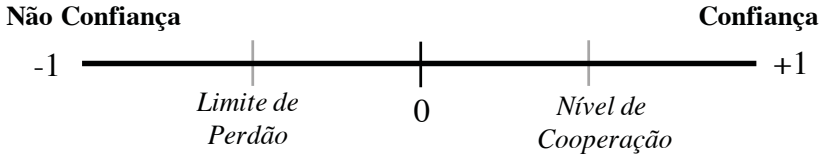


Figura 2.6: Mensuração da confiança de forma contínua (Cho et al., 2015)

- *Confiança escalar*: Diversos autores propuseram tipos de escalas diferentes para essa forma de medição (Cho et al., 2015). Dentre elas, há as escalas binárias, discretas, nominais e de valores contínuos, ilustradas pela Tabela 2.1, elaborada baseada no trabalho de Cho et al. (2015) e Marsh (1994). Observa-se que a escala binária incorpora uma perda na resolução dos níveis de confiança, pois há apenas dois valores para representá-la, 0 ou 1. Ela simplifica o processo de verificar a confiabilidade de uma entidade. Por outro lado, o uso de números, seja uma escala contínua ou discreta,

flexibiliza normalizações ou ressalta valores muito distintos. A escala nominal, como o próprio nome já indica, representa os níveis de confiança por adjetivos, que leva à avaliações diferentes de situações idênticas, visto que são subjetivos.

Tabela 2.1: Escalas para medida de confiança (Cho et al., 2015)

Escalas	**Níveis**											
Nominal	Falta de confiança						Confiança					
	Completa	Muito alta	Alta	Média alta	Média baixa	Baixa	Baixa	Média baixa	Média alta	Alta	Muito alta	Completa
Binária	0						1					
Discreta	-6	-5	-4	-3	-2	-1	1	2	3	4	5	6
Contínua	-1					0						+1

2.5.2 Construção da Confiança

A confiança possui uma subjetividade natural e sua avaliação depende do contexto e dos objetivos. A avaliação ocorre a partir de características individuais e relacionais (Cho et al., 2015). As características ou atributos individuais derivam do próprio indivíduo, enquanto que os relacionais, referem-se às dimensões de confiança oriundas das relações entre indivíduos, como acontece com a confiança social. Segundo Cho et al. (2015), os atributos individuais são lógicos, baseados em processos de cognição lógicos de evidências ou observações por parte de uma entidade, e atributos emocionais, que envolvem o senso emocional do indivíduo tais como sentimento, propensão, experiência e competência, entre outros

A Figura 2.7, baseada no trabalho de Cho et al. (2015), apresenta a classificação dos fatores que afetam a construção da confiança. O seu emprego ocorre de diversas formas para que se avalie a confiança de um dispositivo dentro do ambiente de rede. Um dispositivo que necessite que outro dispositivo execute alguma tarefa de seu interesse observará sua reputação para a execução de tarefas semelhantes. Deve-se verificar se o dispositivo de rede desejado executa as tarefas de forma correta e confiável ou solicitar a um outro dispositivo que informe se conhece aquele dispositivo e o quanto confia nele. Esse processo é conhecido como recomendação.

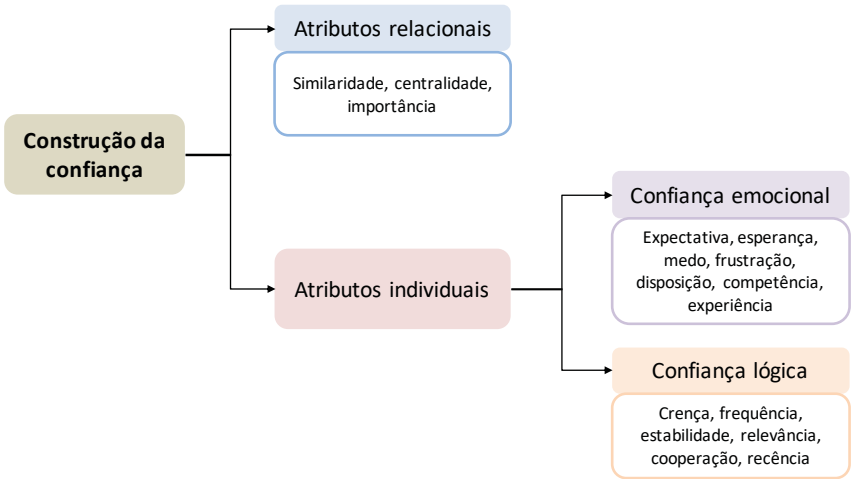


Figura 2.7: Classificação dos fatores que afetam a construção da confiança

A confiança é construída de várias maneiras, a fim de assegurar a sua correta avaliação. Dentre as diversas formas existentes, as mais comuns são a confiança social, reputação e

recomendação. Elas serão apresentadas a seguir, possibilitando ao leitor compreender o seu funcionamento e características principais, além de identificar possibilidades de uso.

- **Confiança social**: A confiança social provém das relações entre os seres humanos no ambiente das redes sociais. Essas redes são estruturas que consistem de indivíduos ou organizações formadas por laços entre si (Cho et al., 2015). Trata-se da confiança oriunda das relações sociais mantidas entre os proprietários dos dispositivos. Sua mensuração demanda o uso de diversas características ou atributos, tais como intimidade, honestidade, privacidade, centralidade e conectividade, entre outros. A avaliação da confiança de um dispositivo não deve se restringir à sua capacidade para execução de uma determinada tarefa. Pelo contrário, deve levar em conta, também, sua confiança social, que representa seu compromisso e boa vontade para executar um serviço solicitado (Guo et al., 2017).

  O exame do histórico de interações entre dois indivíduos propicia obter sua confiança social, seja a partir da similaridade das preferências e *background*, da reputação ou recomendações, ou de outras características inerentes às relações sociais. Com a expansão do seu uso, os dados dessas aplicações têm sido usados para investigar as relações de confiança entre as pessoas e os fatores críticos que afetam suas relações. Porém, as relações construídas nas redes sociais geralmente mostram-se diferentes daquelas existentes no mundo real. Isso se deve ao fato de que as relações online são mantidas por conveniência e generosidade, inexistindo no mundo real (Golbeck, 2009).

- **Reputação**: Um dispositivo que precise avaliar a confiança de um outro dispositivo usa as informações relativas às suas experiências diretas com esse dispositivo e aquelas oriundas de dispositivos conhecidos, que também teriam interagido com o dispositivo avaliado. Essas são experiências indiretas, que representam a reputação de um dispositivo de rede (Gwak et al., 2017). Constata-se que este modelo de avaliação adapta-se às situações onde há um histórico de interações, ou seja, os dispositivos já se encontraram e interagiram anteriormente. Caso contrário, torna-se inviável obter a reputação de um dispositivo, especialmente em ambientes dinâmicos como nas redes *ad hoc*.

- **Recomendação**: Ocorre quando um dispositivo informa a um outro dispositivo que ele confia em um terceiro dispositivo para a execução de uma determinada tarefa. O dispositivo que avalia a confiança não possui informações sobre o dispositivo desejado, ou seja, não possui um histórico de interações anteriores com ele. Portanto, ele se vale de recomendações de outros dispositivos acerca do dispositivo desejado. Ela permite avaliar a reputação de um dispositivo. Ambientes dinâmicos e de grande mobilidade dos nós dificultam a criação e manutenção de históricos de interação, como acontece com redes dinâmicas, onde a mobilidade dos dispositivos acontece com frequência.

2.6 RESUMO

Este capítulo apresentou conceitos de agrupamentos de dispositivos em comunidades dinâmicas mediante interesses em comum, as chamadas comunidades de interesse, apontando a viabilidade do seu uso em ambientes dinâmicos, como ocorre na IoT. A importância da 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 em situações de emergência. Por fim, constatou-se que a confiança torna-se uma alternativa na composição de mecanismos para disseminação de informações, agregando as relações sociais das pessoas ao ambiente de redes.

3 ABORDAGENS E TÉCNICAS DE CONFIANÇA EM REDES NÃO ESTRUTURADAS

Este capítulo apresenta uma revisão dos principais trabalhos publicados sobre o uso de mecanismos de confiança em redes não estruturadas. A Seção 3.1 apresenta uma visão geral do uso da confiança em redes em trabalhos que agregam formas diversas de confiança aos seus protocolos e mecanismos. A Seção 3.2 aborda os trabalhos que fazem uso da confiança nas redes *ad hoc* móveis e nas redes Par-a-Par. A Seção 3.3 apresenta os trabalhos que aplicaram técnicas de confiança nas redes IoT. A Seção 3.4 sintetiza o estado-da-arte apresentado, bem com discute os pontos de relevância nos trabalhos pesquisados, oportunizando a verificação das possibilidades existentes para solução do problema de pesquisa.

3.1 CLASSIFICAÇÃO

A proliferação de dispositivos móveis de comunicação pelo uso de redes sem fio traz diversas oportunidades de interação entre pessoas e entre pessoas e sistemas, assim como impõe alguns desafios. Nessas situações, a IoT destaca-se por oferecer uma plataforma para conectá-los, enriquecendo e tornando a vida dos cidadãos mais fácil (Farahani et al., 2017). Entretanto, oferecer um serviço de disseminação de dados sensíveis com elevada disponibilidade, restringindo o acesso a esses dados a indivíduos ou sistemas autenticados e autorizados, é um desafio de elevada complexidade.

Informações que, por sua natureza e características, são sensíveis e não devem ser expostas à pessoas não autorizadas, precisam ter sua segurança garantida. Um dos atributos de segurança destaca-se - disponibilidade -, para que a disseminação dessas informações aconteça de forma segura, no momento oportuno e no menor tempo possível. Atualmente, há diversas plataformas online para interação social das pessoas, onde aspectos das suas relações são observados e empregados no controle das trocas de dados. Muitas delas potencializam a distribuição de informações, causam vazamentos de dados e comprometem sua segurança (Silverstein, 2019). Assim, um serviço com segurança (*safety*) na disseminação de dados em redes entrega os dados às pessoas corretas e evita vazamentos. No caso de *e-health*, os dados dos pacientes são sensíveis e acessos não autorizados comprometem tratamentos, que impactam diretamente na sua saúde. Observa-se que a garantia da confidencialidade das informações prepondera sobre a sua disponibilidade aos usuários. Logo, são empregados mecanismos de autenticação e de validação dos usuários, que devem estar sempre atualizados (Farahani et al., 2017). Diversos trabalhos existem com soluções para garantir a segurança dos dados. Para ambientes não estruturados, mecanismos para validação dos usuários são adicionados. Dentre eles, destacam-se aqueles que empregam aspectos sociais relacionados à confiança. Eles permitem validar um usuário e conceder-lhe acesso a outros mecanismos de segurança existentes.

A confiança está presente nas relações sociais e auxilia nas tomadas de decisões. Porém, como as pessoas também mantém relações na falta de confiança, isso acarreta decisões incertas, incompletas e conflitantes. Por ser um componente essencial nas relações sociais, quando presente, faz com que os indivíduos trabalhem para manter interações futuras positivas, ao invés de trabalharem somente por interesse próprio. A confiança motiva a manutenção de relações duradouras baseadas na cooperação e colaboração. Conforme o domínio de aplicação, diferentes aspectos da confiança são usados no auxílio às tomadas de decisões tais como a confiança emocional, lógica e a relacional (Cho et al., 2015). Diversos trabalhos incorporam o uso de técnicas de confiança ao funcionamento das redes, como ilustra a Figura 3.1.

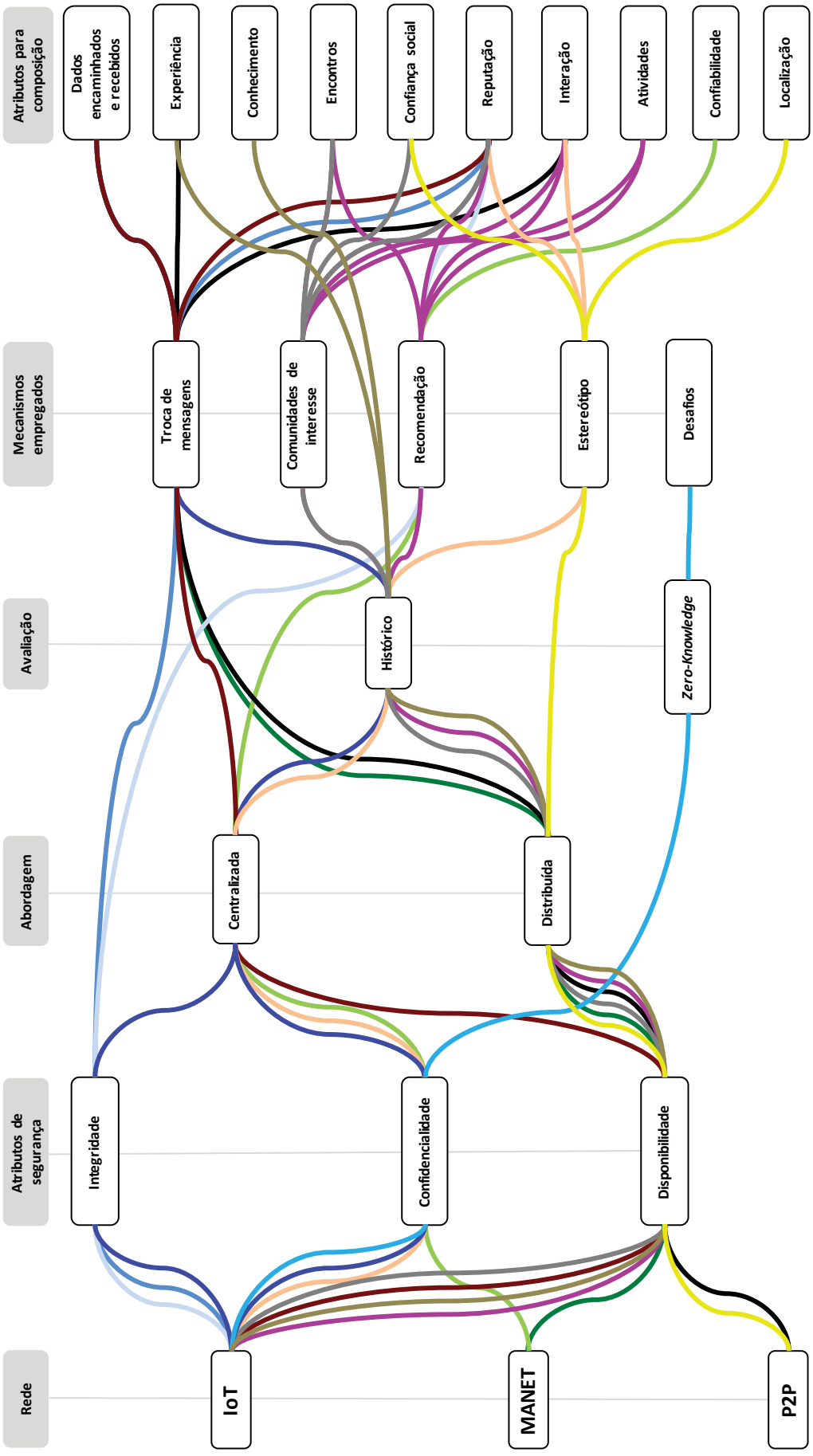


Figura 3.1: Taxonomia do estado-da-arte de confiança em redes não estruturadas

Dentre os tipos de redes existentes, trabalhos que abordam redes IoT, P2P (*Peer-to-Peer*) e MANETs (*Mobile Ad Hoc Networks*) foram pesquisados. Eles foram classificados conforme o tipo de rede que abordam e os atributos de segurança que buscam preservar. Os atributos mais comuns na composição da confiança foram identificados, bem como suas formas de avaliação e os mecanismos empregados. A Figura 3.1 apresenta uma taxonomia elaborada a partir dos trabalhos pesquisados na literatura. Pela taxonomia, constata-se que os autores comumente empregam o histórico de interações entre os dispositivos da rede para avaliar a confiança. As abordagens para ambientes dinâmicos, onde não há um registro das interações anteriores entre dispositivos - *Zero-Knowledge* (Feige et al., 1988), ainda são pouco empregadas. Além disso, a avaliação e a mensuração da confiança geralmente considera as trocas de mensagens e recomendações.

A composição e a avaliação da confiança nos trabalhos pesquisados possuem características em comum, como se observa na Figura 3.1. O uso da confiança ocorre em grande medida em redes IoT, onde as abordagens existentes geralmente são centralizadas. O emprego do histórico de interações prepondera, mas já há trabalhos que buscam atuar em ambientes *Zero-Knowledge*. Para composição da confiança, destacam-se o uso de mecanismos como a troca de mensagens, comunidades de interesse e recomendação. Nesses casos, constata-se que todos eles foram aplicados associados ao histórico de interações da rede, pois se adaptam a ambientes estruturados e centralizados. Dentre os atributos empregados para avaliação da confiança, tem-se a troca de mensagens, que envolve dados encaminhados e recebidos, a confiança social, os encontros, a reputação, a interação e as atividades. O agrupamento de dispositivos de rede em comunidades de interesse baseou-se em atributos como encontros, reputação e interação. Essas relações são detalhadas nos próximos tópicos desse capítulo.

O uso de redes para conectar dispositivos é uma realidade que tende a se ampliar no futuro com o uso da IoT. Para garantir a segurança na disseminação de dados sensíveis, torna-se crucial verificar a confiança dos dispositivos existentes nesse ambiente (Guo et al., 2017). Muitos dos trabalhos encontrados na literatura abordam a segurança dos dados parcialmente, ou seja, concentram-se em garantir alguns de seus atributos - disponibilidade, confidencialidade e integridade - e não a sua totalidade. Os autores geralmente recorreram ao histórico de interações entre os dispositivos para compor a confiança, o que torna os trabalhos inviáveis para ambientes de rede dinâmicos, onde há grande mobilidade dos nós e baixa frequência de interação.

A confiança é usada em diversos tipos de redes, como se observa nos trabalhos citados a seguir, que serão abordados mais detalhadamente ao longo deste capítulo. Nas MANETs, por exemplo, há os trabalhos de Mannes et al. (2012a), Mannes et al. (2012b) e Wang et al. (2017). Nas redes P2P, emprega-se confiança em trabalhos como os de Vasilomanolakis et al. (2017) e de Zuo e Iamnitchi (2016). Há outros trabalhos que não focam em um tipo de rede específico, como é o caso de Taylor et al. (2017).Seus autores propuseram o uso de estereótipo, que é o perfil de um dispositivo de rede obtido a partir de informações oriundas de outros dispositivos. O estereotipo é usado na construção da confiança, de modo que certas características dos dispositivos são usadas como indicadores de seu comportamento durante as interações. Porém, o uso dos estereótipos é apropriado em ambientes de rede sem dinamicidade ou mobilidade dos nós, uma vez que sua composição depende de uma maior frequência de interação dos dispositivos. Além disso, como as observações obtidas sobre os nós possuem um forte componente de subjetividade, elas carecem de confiabilidade e isso compromete sua eficácia.

Nguyen et al. (2016) apresentaram uma abordagem centralizada para IoT, onde avaliaram a confiança dos nós em um cenário sem histórico de interações, valendo-se de mecanismos distintos dos tradicionalmente empregados para seu cálculo. Para isso, aplicaram a técnica de desafios e respostas. Um determinada tarefa, que os autores denominaram desafio, é enviada para um dispositivo. Somente após ele enviar a resposta correta, será visto como confiável e terá

acesso ao serviço requisitado. Essa proposta direciona-se a ambientes distribuídos, sendo passível de ajustes nos desafios enviados, de forma a tornar o mecanismo mais seguro. Contudo, elaborar desafios consiste numa tarefa complexa para dispositivos com pouca capacidade de memória e processamento, tais como aqueles existentes no âmbito da IoT. Ao responder corretamente um desafio, o dispositivo indica que possui capacidade para resolvê-lo e responder ao solicitante da maneira correta e no tempo oportuno. Porém, essa ação não indica o quanto ele é confiável.

3.2 CONFIANÇA EM MANETS E EM REDES P2P

A confiança foi empregada em MANETs por Mannes et al. (2012a) e Mannes et al. (2012b). Eles propuseram um esquema chamado de sistema de quórum, quórum de sensoreamento (do inglês, *quorum systems, quorum sensing* - QS^2), inspirado em um mecanismo biológico de sensoreamento em quórum e de seleção por parentesco, ambos presentes em bactérias. Trata-se de um sistema em quórum tolerante à má-conduta de nós, resiliente a ataques *wormhole* e *blackhole* (Bannack et al., 2008). Seu objetivo era oferecer serviços de operações em MANETs que garantam a confiabilidade e a disponibilidade diante da mobilidade dos dispositivos e de sua restrição de recursos. Para isso, ele cria quóruns de escrita e de leitura com participantes colaborativos, negando a participação de nós de má conduta nas operações de um sistema de quórum na camada de gerência de dados.

O QS^2 funciona como ilustrado na Figura 3.2. O nó *e* inicia a operação de escrita no sistema de quórum a fim de enviar uma informação ao nó *c*. Ele anexa ao dado seu identificador, criando uma rota de identificação do caminho percorrido. Na medida em que o dado é disseminado, os nós *a* e *b* acrescentam seus próprios identificadores ao caminho percorrido pelo dado. O sistema compara a quantidade de escritas e de encaminhamentos. Se estiverem dentro dos limites previstos, assume-se que é um nó confiável. Logo, um nó será classificado como confiável, egoísta ou malicioso, conforme seu comportamento ao disseminar os dados.

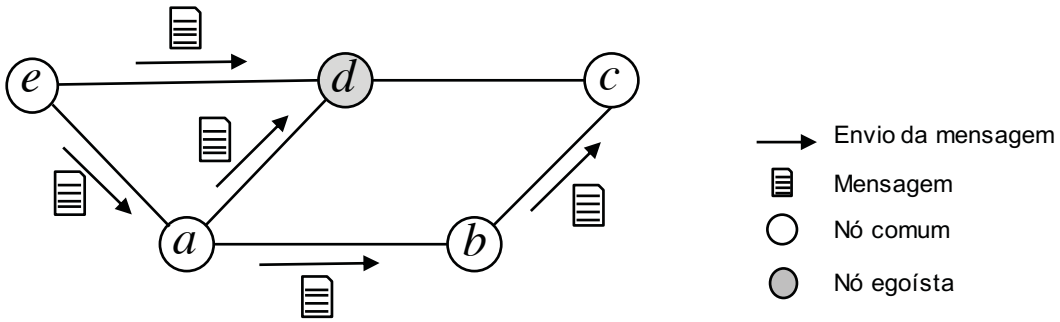


Figura 3.2: Funcionamento do mecanismo QS^2

O encaminhamento dos dados pode não ocorrer, como ilustrado na Figura 3.2, conforme se observa pelo comportamento do nó *d*. Ele recebe dados, mas não os encaminha, o que indica que ele é um nó egoísta. Um nó que encaminha os dados, mas altera a informação, será visto como confiável, apesar de não sê-lo. Essa ação maliciosa impactará no funcionamento do sistema proposto. O QS^2 detecta ataques *Sinkhole* e avalia a confiança dos nós em modo diferente dos modelos tradicionais, pois avalia parcialmente seu o comportamento. Isto ocorre porque ele computa a quantidade de dados de escrita e de leitura, sem avaliar propriamente o comportamento dos nós. Entretanto, ela oferece uma possibilidade de se constatar se um nó está ou não exercendo seu papel dentro da rede. Além disso, essa métrica avalia se as escritas estão ocorrendo, mas não indica se há alteração nos dados por parte de um nó qualquer, o que expõe o sistema a ataques de injeção de dados (Yang et al., 2017).

Um protocolo voltado para MANETS foi proposto por Wang et al. (2017), a fim de realizar o gerenciamento da confiança para MANETs, contra ataques de difamação (Bao e Chen, 2012b), de fraude à eleição (Guo e Chen, 2015), de serviços oportunísticos e de autopromoção. A confiança baseia-se nas recomendações dos nós e, para isso, tarefas são atribuídas aos nós baseadas em sua confiança, que provem da sua confiabilidade para executar esse tipo de serviço, da variância do seu uso e do atraso que leva para concluí-las. Além disso, o protocolo aplica os parâmetros conforme as mudanças no ambiente de rede, o que amplia os cenários para seu emprego. A construção da confiança depende da colaboração entre os nós, pois alguns deles exercem papéis mais relevantes, atuando como provedores de serviços para outros nós. Isso demanda de alguns nós maior robustez em termos de recursos computacionais, impedindo o uso desse protocolo em ambientes onde os dispositivos sejam homogêneos e possuam recursos computacionais restritos.

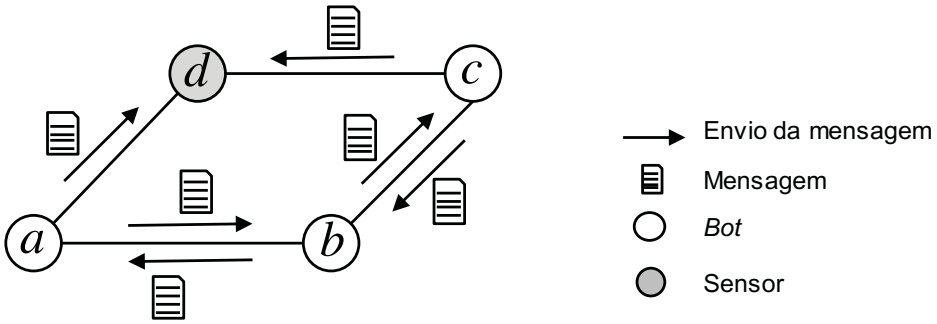


Figura 3.3: Funcionamento do mecanismos para uso em *botnets*

A confiança também é empregada nas redes P2P, onde Vasilomanolakis et al. (2017) propuseram um mecanismo baseado em confiança computacional, obtida pelo envio de mensagens especiais. A Figura 3.3 ilustra o funcionamento do mecanismo, onde cada dispositivo (*bot*) da rede (*botnet*) mantém uma lista de vizinhos. Isso propicia que a rede continue funcionando, inclusive do comportamento *churn* dos dispositivos. Regularmente, os *bots* enviam mensagens aos seus vizinhos para verificar sua presença na rede. Se um dos vizinhos da lista não estiver disponível, ele será isolado da rede. Como o mecanismo busca evitar que nós sensores identifiquem a *botnet*, há uma mensagem especial na qual os dispositivos enviam sua identificação. Os demais *bots* responderão normalmente a esta mensagem, enquanto os nós sensores não o farão, pois restrições legais os impedem de participar de atividades criminosas. Essa mensagem auxilia na avaliação da confiança dos demais *bots*. As decisões para isolar um dispositivo da rede serão baseadas em confiança, diante de modelos construídos sobre evidências e experiências anteriores.

A Figura 3.4 (Vasilomanolakis et al., 2017) ilustra a convergência do funcionamento do mecanismo após testes realizados pelos autores. Observa-se que os nós sensores foram isolados da rede em grande medida após 14 dias. Apesar do sucesso nessa ação, o tempo de convergência do mecanismo é considerado demasiado longo caso seja empregado em ambientes que precisam de respostas imediatas, seja por conta dos tipos de dados trafegados ou por conta das tomadas de decisão. Esse tempo é demasiado longo diante das demandas atuais para disponibilizar informações praticamente em tempo real (Farahani et al., 2017). Outro fator que influencia no uso desse mecanismo é a necessidade de manutenção de um histórico de interações e de experiências anteriores, cuja obtenção as vezes é inviável em ambientes dinâmicos.

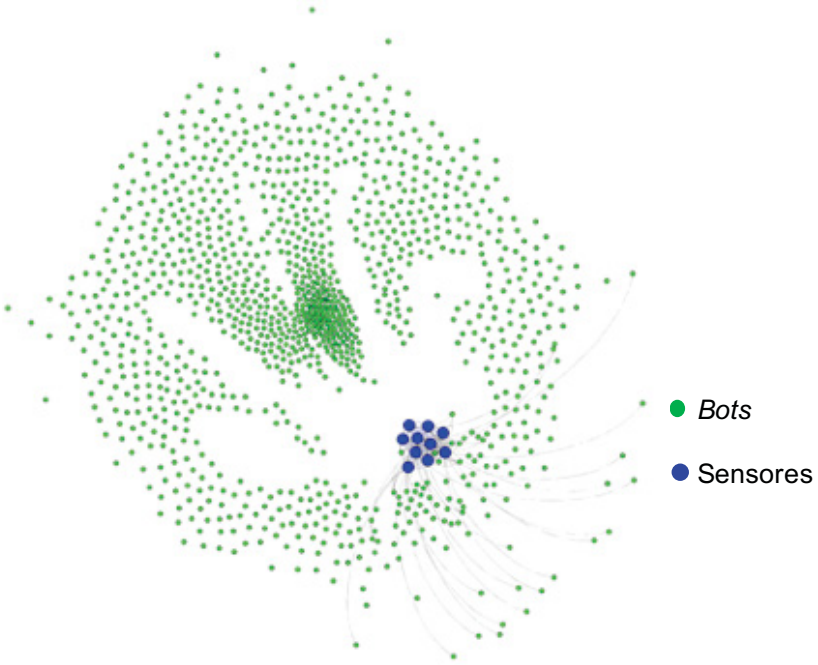


Figura 3.4: Convergência do mecanismo de confiança (Vasilomanolakis et al., 2017)

O uso das relações sociais dos proprietários dos dispositivos no funcionamento das redes P2P foi analisado por Zuo e Iamnitchi (2016), de forma a criar técnicas efetivas para melhorar sua performance. Informações como perfis, localização ou interesses, por exemplo, estão sujeitas à análise e uso. A arquitetura P2P oferece diversos benefícios para seu uso, tais como a inexistência de uma entidade central controladora, que elimina a possibilidade de se ter um ponto único de falha dentro da rede. Por outro lado, o efeito *churn*, por exemplo, afeta a disponibilidade de recursos e dificulta sua localização dentro da rede. Isso impõe desafios ao desenvolvimento de aplicações para esse tipo de ambiente. Os autores propuseram o aproveitamento das relações de confiança oriundas das redes sociais - *Facebook*, *Linkedin* e *Foursquare*, por exemplo - nas relações entre os pares, restringindo o acesso às informações somente aos pares confiáveis. Contudo, observa-se que as relações existentes nas redes sociais nem sempre correspondem àquelas existentes no mundo real (Golbeck, 2009). Os usuários não controlam totalmente as interações que mantêm nessas redes, o que impacta na disponibilidade desses dados quando disseminados sem qualquer controle, impactando na sua segurança.

3.3 CONFIANÇA NA IOT

A IoT possibilita a interconexão de dispositivos diversos, permitindo a disseminação de dados e o monitoramento de eventos variados. Logo, a confiança dos seus dispositivos precisa ser avaliada (Guo et al., 2017). Dentre as formas de avaliação disponíveis, destacam-se a reputação, recomendação e comunidades de interesse. A IoT possui características como mobilidade dos nós e dinamicidade da rede, que quando desconsideradas durante a avaliação da confiança, acarretam uma disseminação de dados ineficaz. Os trabalhos pesquisados serão analisados a seguir.

3.3.1 Reputação

A reputação é a técnica mais comumente empregada na literatura para avaliar a confiança de um dispositivo no âmbito da IoT. Há dois tipos de abordagens distintas encontradas

na literatura: centralizada, que é verificada nos trabalhos de Al-Hamadi e Chen (2017), Cervantes et al. (2018), Cervantes et al. (2015) e de Son et al. (2017)); e a distribuída, abordada nos trabalhos de Bao e Chen (2012a), Bao e Chen (2012b), Bao et al. (2013), Nguyen et al. (2016), Oh et al. (2018) e de Truong et al. (2017). A abordagem distribuída se adapta melhor à IoT. Em geral, a reputação associa-se à outras técnicas de confiança, como recomendação, agregando eficiência e eficácia no seu uso. A seguir, serão apresentados e comentados os trabalhos conforme a sua abordagem. Isso permitirá ao leitor conhecer os trabalhos que fazem uso da confiança na IoT, as vantagens e desvantagens dessas abordagens e identificar possíveis casos de uso.

3.3.1.1 Abordagens centralizadas

Uma Abordagem centralizada empregando reputação foi proposta por Cervantes et al. (2015) através de um sistema de detecção de intrusão (do inglês, *Intrusion Detection System* – IDS) de ataques Sinkhole em 6LoWPAN para IoT (do inglês, ***I**ntrusion detection for Si**N**khole attacks over 6LoWPAN for Interne**T** of Th**I**ngs* - INTI). Ele detecta ataque *sinkhole* (Cervantes et al., 2015) no roteamento de mensagens e visa prevenir, identificar e isolar os efeitos desse tipo de ataque. O INTI atua em ambientes onde alguns nós possuam restrições de capacidade de processamento, ao prover mecanismos de auto-organização e autorreparo no ambiente de rede. Para isso, ele combina *watchdog*, reputação e estratégias de confiança para analisar o comportamento dos dispositivos e detectar os atacantes. Os nós exercem três papéis distintos na rede: nós livres, nós membros e nós líderes. A avaliação dos nós leva em conta seus comportamentos anteriores. O sistema estima a quantidade de transmissões de dados de chegada e de saída. Quando essas quantidades são iguais, o nó é considerado bom. A Figura 3.5 ilustra o funcionamento do INTI, onde os nós livres enviam dados à estação base através de seus líderes, que os repassam ao líder do agrupamento vizinho por um nó associado.

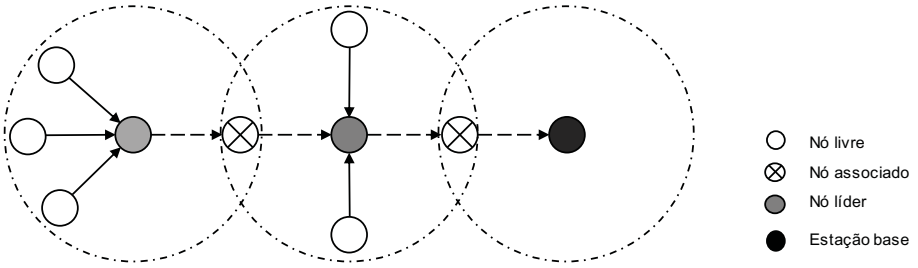


Figura 3.5: Funcionamento do INTI

As interações são verificadas por observações diretas, que ocorrem dentro do agrupamento, ou indiretas, que acontece entre agrupamentos. O INTI calcula a incerteza, crença e descrença para representar a reputação do nó. Para isso, cada nó propaga seu status nas mensagens transmitidas. Por fim, calcula-se a confiança baseado na quantidade de interações entre o nó que avalia e o nó avaliado, concluindo com a aplicação da distribuição β. Observa-se que as métricas empregadas geram falsos positivos ou falsos negativos, visto que não avaliam a confiança dos nós, mas o seu funcionamento. Esse processo fica comprometido se um nó atrasar o encaminhamento de dados recebidos, ainda que não intencionalmente, quando será considerado malicioso. Além disso, esse tipo de nó modifica os dados que recebe antes de encaminhá-los, como ilustra a Figura 3.6, promovendo ataques de injeção de dados. A avaliação da reputação dos nós depende da cooperação entre eles, que será comprometida por nós que não desejam cooperar.

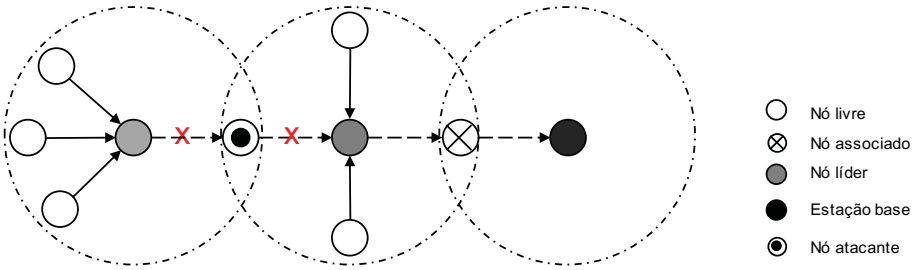


Figura 3.6: Exemplo de ataque ao INTI

Os papéis que os nós exercem no INTI demandam recursos computacionais diferenciados, especialmente para os nós líderes e associados. Esses últimos são aqueles nós membros que pertencem a vários agrupamentos simultaneamente e respondem pelo encaminhamento de mensagens entre agrupamentos. Nessas condições, a energia é um fator preponderante ao funcionamento do sistema, especialmente para o encaminhamento das mensagens. Além disso, a necessidade de experiências e interações anteriores inviabiliza sua aplicação em ambientes dinâmicos, onde os nós têm grande mobilidade e participam da rede de forma intermitente.

Em 2018, Cervantes et al. (2018) propuseram um outro IDS, chamado Thatachi, contudo, para garantir a confidencialidade e integridade dos dados disseminados. Ele cria agrupamentos para lidar com a densidade e a mobilidade dos nós, combinando estratégias de *watchdog*, reputação e confiança. Ele detecta alguns tipos de ataques, especialmente *sinkhole* (Cervantes et al., 2015) e *selective forwarding* (Arış et al., 2018), além de contribuir para redução do consumo de energia. A reputação de um nó é calculada a partir das quantidades de transmissões de dados recebidos e de saída. Se esses valores forem iguais, o nó será classificado como normal. Cada nó propaga sua reputação, a fim de que os demais nós possam calcular a confiança nele. Entretanto, o cômputo da confiança baseado na quantidade de dados recebidos e transmitidos fica comprometida diante da execução de ataques de injeção de dados (Yang et al., 2017). O IDS proposto não é apropriado às redes IoT e P2P, pois funciona de maneira centralizada.

Um protocolo para tomada de decisões em serviços de saúde, baseado em confiança e no compartilhamento de informações, foi proposto por Al-Hamadi e Chen (2017). Nesse trabalho, os nós compartilham informações acerca dos locais onde se encontram, tais como temperatura, umidade, horário, entre outras. Ele permite a construção de uma base de dados coletiva, empregada na avaliação das condições de um determinado ambiente em um dado instante. Isso auxilia na tomada de decisão para que pacientes acessem ou não esses locais. Ele usa a informação relativa ao horário da coleta dos dados como um fator de compensação, tal que as recomendações mais recentes sejam mais valorizadas que as mais antigas. Isso garante que a tomada de decisão baseie-se em informações atualizadas. O cômputo da reputação dos nós baseia-se nas suas recomendações sobre um local e diante das observações diretas que outros nós fazem sobre esse local. Assim, esse protocolo demanda a manutenção de históricos de interações, viabilizando o emprego de recomendações entre os nós. Essa condição inviabiliza seu uso em ambientes esparsos, nos quais ocorram poucas interações entre os nós da rede.

A confiança pessoal, obtida a partir do histórico de interações, e a reputação não pessoal, oriunda do estereótipo fornecido por outros dispositivos, foram combinadas por Son et al. (2017), a fim de garantir a segurança dos dados disseminados nas redes IoT. Os históricos de dispositivos semelhantes também auxiliam na composição da confiança, além de empregar informações relacionadas ao comportamento dos proprietários dos dispositivos, tais como localização, permanência em determinados locais, entre outras. Contudo, o cômputo da confiança exige dispositivos com capacidade de processamento para lidar com a quantidade de informações, o que nem sempre é possível no âmbito da IoT, onde alguns dispositivos possuem baixa capacidade

de processamento. Essa proposta não é compatível com ambientes distribuídos e com grande mobilidade dos dispositivos, especialmente com dispositivos com recursos limitados.

3.3.1.2 Abordagens distribuídas

Diversos trabalhos propuseram protocolos para ambientes distribuídos e voltados para avaliação da confiança dos nós baseado nos interesses em comum que possuem no âmbito das redes IoT (Bao e Chen, 2012a,b; Bao et al., 2013). Neles, as relações sociais mantidas entre os proprietários dos dispositivos são analisadas, contribuindo para que seus encontros e atividades venham a ser computados e usados no cálculo da reputação de cada nó. Assim, o cômputo da confiança é viabilizados e ela é atualizada sempre que os nós se encontrarem ou interagirem.

O protocolo proposto por Bao e Chen (2012a) realiza o gerenciamento de confiança dinâmica, que lida com nós que se comportam mal e alteram seu status ao longo do tempo. Ele garante a segurança pela disponibilidade do serviço mesmo em ambientes dinâmicos. Esse protocolo visa mitigar ataques de autopromoção, de difamação e aqueles destinados a melhorar a reputação de outros nós. Para isso, como ilustrado na Figura 3.7, os dispositivos computacionais agrupam-se conforme os interesses de seus proprietários, independente das suas relações de propriedade. As interações entre os dispositivos nesses ambientes restritos será mais intensa, enquanto que entre as comunidades, o tráfego de dados se reduz. A partir desse momento, cada nó avalia a confiança de outros nós dentro das comunidades de interesse onde se encontra, diante de características comuns como honestidade e cooperação. Isso ocorre a partir de suas observações diretas e de recomendações provenientes de outros nós. Além disso, os encontros entre eles provocam a atualização das observações que cada um detém sobre o outro.

Figura 3.7: Agrupamentos por comunidades de interesse

O protocolo emprega um parâmetro α, que atua como um peso nas observações diretas e os valores de confiança antigos. Assim, ele possibilita controlar o quanto as informações antigas influenciam no cálculo atual da confiança. Um parâmetro β pesa a influência das recomendações no cálculo da confiança. O trabalho avalia a influência de α e β no cômputo da confiança das propriedades de honestidade e cooperatividade diante da presença de nós maliciosos e honestos. Além disso, avalia também a influência desses parâmetros no cômputo da confiança das propriedades de honestidade e cooperatividade, bem como na composição do serviço no âmbito das redes IoT. Os resultados demonstram que o uso de novas observações diretas em detrimento das mais antigas aumenta a acuracidade no cálculo da confiança e a velocidade de convergência dos valores de confiança. Além disso, o uso de recomendações em detrimento de informações mais antigas contribui para velocidade de convergência da confiança. Porém, na presença de nós maliciosos emitindo recomendações falsas, a acuracidade diminui.

A avaliação da cooperação e das comunidades de interesse depende, respectivamente, da quantidade de amigos que cada nó possui e da quantidade de comunidades que participam. Em ambos os casos, observa-se a importância das interações no cômputo da confiança, que fica claro com o cálculo da recomendação, quando são usadas observações indiretas, que guardam relação com o histórico de observações. Os resultados demonstram que o uso tanto das observações diretas, como do histórico de observações melhoram com o aumento do peso atribuído a eles. Essa conclusão indica os benefícios do uso desse protocolo em ambientes onde os nós de rede interagem com frequência, pois propicia a criação do histórico de observações. Da mesma maneira, as interações frequentes também aumentam a probabilidade de um nó avaliar diretamente outros nós. Contudo, cenários dinâmicos, especialmente aqueles onde a participação dos nós é intermitente, não são indicados para o uso desse protocolo, tendo em vista as dificuldades para criação e manutenção de históricos de interações entre os dispositivos.

O gerenciamento da confiança através de um protocolo distribuído empregando as propriedades de honestidade, cooperatividade e comunidade de interesse foi proposto por Bao e Chen (2012b). Um nó avalia a confiança de outro nó quando ocorre um encontro social ou uma interação entre eles. São usadas observações diretas e indiretas (recomendações). O agrupamento dos dispositivos em comunidades de interesse permite enfrentar a escalabilidade da rede, na medida em que os dispositivos interagem com outros dispositivos que possuem interesses iguais. Os autores avaliaram o processo de composição do serviço diante da presença de nós maliciosos, que emitem recomendações falsas e impactam no cômputo da confiança por ameaças como autopromoção, difamação e promoção de outros nós. Ele garante a segurança pela manutenção da disponibilidade do serviço na presença desses tipos de ataques.

O protocolo apresentado emprega dois parâmetros distintos, sendo um parâmetro α, que atua como um peso nas observações diretas e os valores de confiança antigos. Assim, ele possibilita controlar o quanto as informações antigas influenciam no cálculo atual da confiança. Um parâmetro β atua como um peso na influência das recomendações no cálculo da confiança. Foi avaliada a influência de α e β no cômputo da confiança das propriedades de honestidade e cooperatividade diante da presença de nós maliciosos e honestos. Além disso, avaliam também a influência desses parâmetros no cômputo da confiança das propriedades de honestidade e cooperatividade, bem como na composição do serviço no âmbito das redes IoT.

Os resultados demonstraram que o uso de observações diretas recentes em detrimento das mais antigas aumenta a acuracidade no cálculo da confiança e a velocidade de convergência dos seus valores. Além disso, o uso de recomendações em detrimento de informações mais antigas contribui para o aumento da velocidade de convergência da confiança. Porém, na presença de nós maliciosos emitindo recomendações falsas, a acuracidade diminui. Este protocolo aplica-se aos ambientes com baixa mobilidade dos dispositivos e suas interações frequentes. Isso permite manter um histórico de interações, que auxilia no cômputo da confiança. Contudo, seu uso fica comprometido diante de interações eventuais entre os dispositivos de rede ou que sua mobilidade seja elevada, visto que informações passadas, diretas ou indiretas, serão escassas ou inexistentes.

O uso da reputação combinada com a experiência e o conhecimento, foi objeto do trabalho de Truong et al. (2017). Eles apresentaram uma abordagem distribuída para avaliação de confiança chamado REK (do inglês, *Reputation, Experience, Knowledge*). Ela compreende o uso de três indicadores de confiança: reputação - opinião pública acerca de quem é avaliado; experiência - oriunda das interações prévias com o avaliado; e conhecimento - corresponde aos entendimentos a respeito do avaliado. Essa abordagem compõe a confiança de maneira indireta, ou seja, a partir de situações e características distintas dos parâmetros tradicionais encontrados na literatura. Os autores propuseram modelos de avaliação desses indicadores, mas não apresentaram resultados. Essa abordagem é adequada às redes IoT, pois atua de maneira distribuída. O uso

de reputação permite distinguir certos nós para executar tarefas mais importantes. Porém, ela demanda conhecimento das interações dos nós ao longo do tempo. Adicionalmente, obter indicadores subjetivos como conhecimento e experiência é um grande desafio, assim como sua mensuração é complexa Cho et al. (2015).

A predição da confiança dos nós de uma rede levando em conta informações explícitas e implícitas foi proposta por Oh et al. (2018), motivados pela ideia de propagação de crença (Chau et al., 2006) (Kim e Hovy, 2006) (Yedidia et al., 2003), que permite a integração tanto das informações de confiança explícitas, como das avaliações das classificações, finalizando com a predição da probabilidade da confiança. Eles apresentaram um *framework* no qual a predição baseia-se na troca de mensagens entre os nós de uma rede. Essas informações são explícitas, quando a avaliação é feita diretamente pelo próprio nó, e implícitas, quando são inferidas de outras relações de avaliação. Essa solução propicia a avaliação da confiança em ambientes esparsos, com poucas interações entre os nós. Os autores abordaram as formas de propagação da confiança para a construção de novas relações de confiança: propagação direta, confiança transposta, propagação da confiança global e co-citações.

A propagação direta da confiança, como ilustra a Figura 3.8, ocorre quando o nó a confia no c, T_{ac}, e o c confia no nó b, T_{cb}. Infere-se que a probabilidade do nó a confiar no nó b, T_{ab}, aumenta na medida da confiança do nó c. Apesar disso, essa confiança depende da cooperação entre os nós envolvidos. Se o nó c, por exemplo, for mal intencionado e promover ataques de difamação, influenciará a confiança de a em b, T_{ab}. Isso também ocorre nos ataques de fraude à eleição, onde o nó c repassaria uma confiança falsa para o nó a.

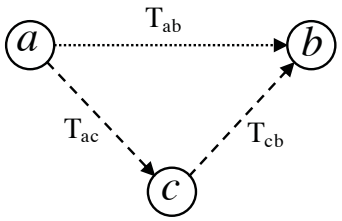


Figura 3.8: Propagação de confiança direta

A confiança transposta ocorre quando dois nós de uma rede confiam em um terceiro nó, mas não confiam um no outro. A Figura 3.9 ilustra essa situação. Os nós a e b confiam em um terceiro, c, mas não possuem registros ou históricos de confiança entre si. Como ambos confiam em um nó em comum, os autores entendem que somente se essa confiança no nó em comum for superior a 50%, a confiança será transposta para a relação dos nós a e b. Nesse caso, o nó em comum auxiliaria na composição da confiança entre nós que confiam nele. Contudo, essa confiança também depende da colaboração entre os nós e dos históricos de interações, que nem sempre se obtém em redes dinâmicas. Um outro desafio é saber quanto da confiança sobre o nó em comum influencia na avaliação da confiança entre os nós envolvidos. A confiança transposta serve como um indicador para composição da confiança final, dependendo de outros indicadores para possibilitar uma mensuração mais eficaz da confiança.

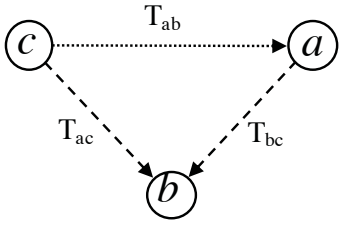


Figura 3.9: Propagação de confiança transposta

No modelo de propagação da confiança global, um nó é visto como confiável por vários outros nós, como ilustrado na Figura 3.10. Em função dessa situação, outros nós confiam nele também. Esse processo é conhecido como reputação, com largo emprego na avaliação de confiança em ambientes de rede. A reputação permite que um nó crie relações com outros nós com os quais não tenha interagido anteriormente. Todavia, os nós atuam em conluio e indicar que um nó qualquer como confiável. Isso induziria outros nós a estabelecerem relações com ele e o selecionarem para tarefas importantes dentro da rede, o que configura um ataque de fraude à eleição. Esse modelo é útil para obtenção de indicadores de confiança a serem empregados na composição da confiança, associado a indicadores de outros tipos.

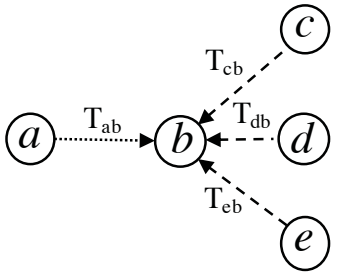


Figura 3.10: Propagação de confiança global

3.3.2 Recomendação

A recomendação também é empregada para construção da confiança, como ocorre no trabalho de Bao et al. (2013). Os autores propuseram um protocolo de gerenciamento da confiança escalável, adaptativo e sobrevivente para redes IoT em ambientes dinâmicos. Ele opera de forma distribuída e emprega múltiplas propriedades de confiança, tais como honestidade, cooperatividade e comunidade de interesse. Assim, garantem a disponibilidade do serviço. Cada nó avalia a confiança de outro nó quando ocorre um encontro social ou uma interação entre eles. São usadas observações diretas e indiretas (recomendações). A escalabilidade da rede é atendida através de uma estratégia de armazenamento dos valores de confiança mais elevados e mais recentes, criando um histórico de interações reduzido e adequado aos recursos de armazenamento limitados dos dispositivos IoT. A adaptabilidade do protocolo é demonstrada pela sua convergente acuracidade e comportamento na medida em que novos nós se conectam à rede. A sobrevivência está relacionada à resiliência do protocolo quando a confiança de um nó converge na direção da confiança verdadeira na presença de nós maliciosos executando ataques relacionados à confiança. Para isso, ele emprega um parâmetro β para pesar na influência das recomendações no cálculo da confiança e avalia seu efeito na confiança subjetiva computada. Devido as recomendações dependerem do histórico de interações entre dispositivos, isso inviabiliza o uso do protocolo em ambientes onde as interações sejam eventuais. Contudo, as CoI restringem em alguma medida

a comunicação aos seus dispositivos, atendem à escalabilidade da rede e limitam o acesso aos dados que trafegam na rede aos nós de uma mesma comunidade.

A tomada de decisões em serviços de saúde por meio de recomendações foi abordada por Al-Hamadi e Chen (2017), através de um protocolo baseado em confiança e no compartilhamento de informações. Os nós compartilham informações acerca dos locais onde se encontram, tais como temperatura, umidade, horário, entre outras. Avalia-se ambientes frequentados pelos proprietários dos dispositivos em um dado momento e local específicos por meio de recomendações, a fim de se construir uma base de dados coletiva desses ambientes. Isso auxilia nas tomadas de decisões para que outros pacientes possam acessar ou não tais locais. O horário da coleta dos dados é empregado como um fator de compensação, tornando as recomendações recentes mais valorizadas do que as mais antigas. Isso garante que as tomadas de decisões baseiem-se em informações atualizadas. Além disso, as recomendações de um nó são comparadas às de outros, permitindo avaliar se um nó está inserindo informações falsas na rede. O armazenamento e o processamento dos dados estão localizados na *cloud*, o que permite o uso desse protocolo com dispositivos que possuam recursos computacionais limitados. As recomendações incorporam características das relações sociais dos proprietárias dos dispositivos às tomadas de decisão nos ambientes. No entanto, exigem interações frequentes entre os dispositivos, às vezes eventuais em ambientes de rede dinâmicos e insuficientes para a construção da base de dados.

3.3.3 Comunidades de Interesse

As comunidades de interesse foram empregadas por Bao e Chen (2012a), Bao e Chen (2012b) e Bao et al. (2013), quando apresentaram protocolos para avaliação da confiança dos nós no âmbito das redes IoT. Em todos esses protocolos, o comportamento das comunidades ocorreu da mesma forma, onde os nós da rede agruparam-se mediante interesses sociais dos proprietários dos respectivos dispositivos. Porém, sua avaliação ocorreu somente no trabalho de Bao et al. (2013), onde os autores propuseram um protocolo de gerenciamento da confiança escalável, adaptativo e sobrevivente para redes IoT em ambientes dinâmicos. O protocolo é distribuído e emprega múltiplas propriedades de confiança, tais como honestidade, cooperatividade e comunidade de interesse. Cada nó avalia a confiança de outro nó quando ocorre um encontro social ou uma interação entre eles. São usadas observações diretas e indiretas Como ilustra a Figura 3.11, as comunidades de interesse são baseadas em IoT social, onde os nós se agrupam em comunidades conforme um interesse comum. Observa-se que as interações entre dispositivos dentro das comunidades de interesse tornam-se mais frequentes que aquelas entre comunidades.

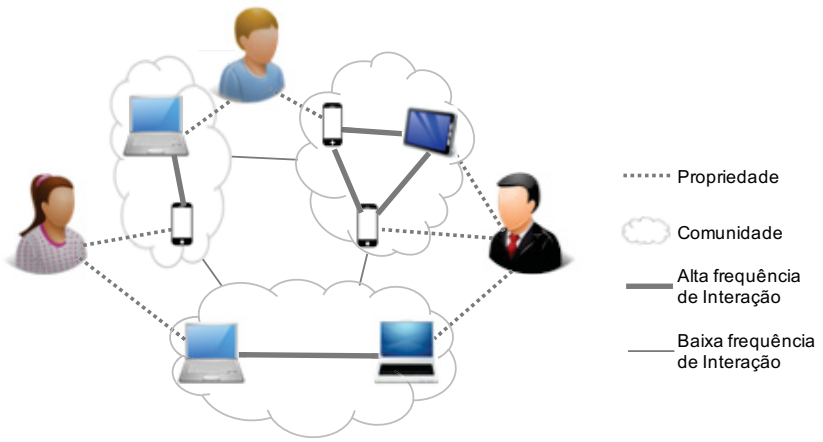


Figura 3.11: Emprego de comunidades de interesse

O agrupamento dos dispositivos em comunidades de interesse permite enfrentar a escalabilidade da rede, na medida em que os dispositivos interagem com outros dispositivos que possuem os mesmos interesses. O protocolo busca selecionar os melhores parâmetros na presença de nós maliciosos para responder às mudanças nas comunidades de interesse. A escalabilidade é atendida através de uma estratégia de armazenamento dos valores de confiança mais elevados e mais recentes dos nós com os quais ocorre os encontros, criando um histórico de interações reduzido e adequado aos recursos de armazenamento limitados dos dispositivos IoT. A adaptabilidade do protocolo é demonstrada pela sua convergente acuracidade e comportamento na medida em que novos nós se conectam à rede. A sobrevivência do protocolo está relacionada à sua resiliência quando a confiança de um nó converge na direção da confiança verdadeira na presença de nós maliciosos executando ataques relacionados à confiança.

O protocolo emprega dois parâmetros distintos, sendo um parâmetro α, que atua como um peso nas observações diretas e os valores de confiança antigos. Isso possibilita controlar o quanto as informações antigas influenciam no cálculo atual da confiança. Um parâmetro β pesa a influência das recomendações no cálculo da confiança. Os efeitos de α e β na confiança subjetiva foram avaliados, onde se verificou a confiança inter e intra comunidades. Avaliou-se, também, o efeito de β na confiança de novos nós que se conectam à rede, bem como o efeito de α na confiança relacionada ao espaço limitado de armazenamento da confiança, onde também se verificou a confiança inter e intra CoI. Por fim, os autores avaliaram a efetividade da estratégia de armazenamento diante da taxa de acerto de nós selecionados aleatoriamente. Este protocolo é direcionado a ambientes dinâmicos, onde os nós participam de forma intermitente. Para isso, ele mantém um histórico de interações registrando os valores de confiança de alguns poucos nós mais confiáveis, o que auxilia no cômputo da confiança. Contudo, o emprego desse protocolo em ambientes com interações esparsas entre os nós não permite a manutenção de históricos, visto que informações passadas, diretas ou indiretas, também serão escassas ou não existirão.

3.4 DISCUSSÃO

Esta seção apresenta uma discussão do estado-da-arte sobre o uso de abordagens de confiança em redes não estruturadas. Os trabalhos investigados foram analisados e, posteriormente, classificados conforme certas características e requisitos de interesse, que estão sumarizados na Tabela 3.1. Diante do objetivo dessa pesquisa, a classificação envolveu os tipos de redes não estruturadas onde comumente o emprego da confiança acontece: IoT, MANET e P2P. Os atributos de segurança de cada trabalho foram identificados, tendo como foco a avaliação da confiança, a fim de se verificar os mecanismos de confiança comumente empregados para atingi-los. Por fim, esses trabalhos foram analisados diante dos seguintes critérios: abordagens empregadas, atributos usados para composição da confiança e formas de avaliação.

A pesquisa bibliográfica demonstrou que os autores buscam prover segurança aos dados pela garantia das suas propriedades de integridade, confidencialidade e disponibilidade. Contudo, isso ocorre de forma parcial, ou seja, esses atributos não são garantidos de maneira concorrente. A maioria dos trabalhos procuram garantir a disponibilidade. Conforme o atributo de segurança almejado, as soluções oferecidas guardam alguma semelhança no seu funcionamento, como constata-se na Tabela 3.1 e foi observado na Figura 3.1. Os trabalhos pesquisados orientam-se, majoritariamente, para as redes IoT, havendo abordagens centralizados e distribuídas. Outra questão que se destaca é quanto à forma de verificação da confiança. O histórico de observações, ou seja, das experiências anteriores registradas, foi amplamente verificado. Por outro lado, somente um trabalho atuou em uma condição *Zero-Knowledge*, ou seja, empregando apenas as informações existentes quando da avaliação da confiança e não levando em conta informações

passadas. Apesar da prevalência no uso do histórico de observações, as abordagens - *centralizadas ou distribuídas* - são distintas, havendo um equilíbrio no seu uso.

Quanto aos mecanismos aplicados para o cômputo da confiança, observa-se pela Tabela 3.1 que eles se distribuíram entre vários tipos, destacando-se o uso das comunidades de interesse e a troca de mensagens. Entretanto, esse último não é considerado propriamente um mecanismo para avaliação de confiança, visto que a troca de mensagens indica o comportamento dos nós, mas não necessariamente se existe uma relação de confiança entre eles. O uso das comunidades de interesse guarda relação direta com as interações sociais que ocorrem entre os proprietários dos dispositivos. Seus interesses em comum propiciam que os respectivos nós de rede se agrupem, formando um ambiente restrito para troca de dados. Observa-se que as comunidades de interesse contribuem para a garantia da segurança dos dados disseminados entre os nós agrupados, na medida em que se vale de atributos de confiança oriundos das relações sociais dos proprietários dos dispositivos para criar e manter os agrupamentos, atuando como um mecanismo de auxílio no controle de disseminação de dados.

A composição da confiança ocorre a partir de diversos atributos, onde se verificou a predominância do uso da reputação, seguida de interações, confiança social e encontros. As interações e os encontros são atributos quantitativos, ou seja, quanto maior a interação entre os nós em um ambiente de rede, maior a quantidade de encontros. Essas quantidades servem como indicadores para construção da confiança em si, não sendo conclusivos acerca da confiança de um nó de rede. Constata-se que mais de 50% dos trabalhos fizeram uso desses atributos, indo ao encontro das características de mobilidade e dinamicidade da rede. O uso majoritário da reputação está relacionado ao emprego dos históricos de observações. A Tabela 3.1 mostra que sempre que um trabalho se valeu do histórico de observações para o cômputo da confiança, ele também empregou reputação. Isso se deve ao fato de que a reputação é construída ao longo do tempo, daí a necessidade de se ter um histórico de observações. Portanto, ela não é apropriado para ambientes de redes dinâmicos e com grande mobilidade dos nós, que inviabilizam a manutenção desses históricos. A confiança social ainda é pouco empregada nos trabalhos, mas demonstra um potencial de crescimento, principalmente diante da expansão do uso das redes sociais e de sua integração com outros serviços de rede. Além disso, embora a maioria dos trabalhos que a empregaram buscassem prover a segurança no acesso aos dados pela garantia da sua confidencialidade, há vários trabalhos que abordam a disponibilidade. Isso indica a importância do uso das informações oriundas das relações sociais das pessoas no contexto das redes.

A análise do estado-da-arte sobre o uso de abordagens de confiança em redes não estruturadas demonstrou que o cenário atual, no qual a dinamicidade das redes e a mobilidade dos dispositivos se destacam, demanda soluções distintas daquelas tradicionalmente empregadas nas redes existentes para garantir a segurança na disseminação dos dados. Segundo Roman et al. (2011), as abordagens tradicionais para gerenciamento da segurança, confiança e privacidade encontram dificuldades quando aplicadas à IoT, devido à escalabilidade e à grande variedade de relações entre as entidades existentes nesse ambiente. Assim, há necessidade de soluções apropriadas aos ambientes dinâmicos, não estruturados, especialmente onde não há uma memória anterior do funcionamento da rede e que atuem de forma distribuída. Logo, atende-se à questão de escalabilidade da rede, pois funcionam em frações dessa rede, sem qualquer controle centralizado. Nesse contexto, o uso das comunidades de interesse mostra-se promissor, pois segrega uma rede em agrupamentos distintos, confinando parte do tráfego de dados ao seu interior. Elas são estabelecidas e mantidas pelo uso de informações oriundas dos proprietários dos dispositivos e de suas relações sociais, adaptando-se ao local e momento das relações.

Tabela 3.1: Síntese do estado-da-arte do uso de confiança em redes não estruturadas

Tipos de redes		**-**	**MANET**			**P2P**		**IoT**											**IoT**
Referências		Taylor et al. (2017)	Wang et al. (2017)	Mannes et al. (2012a)	Mannes et al. (2012b)	Vasilomanolakis et al. (2017)	Zuo e Iamnitchi (2016)	Al-Hamadi e Chen (2017)	Cervantes et al. (2018)	Cervantes et al. (2015)	Son et al. (2017)	Bao e Chen (2012a)	Bao e Chen (2012b)	Bao et al. (2013)	Nguyen et al. (2016)	Oh et al. (2018)	Truong et al. (2017)	**Proposta**
Atributos de Segurança	Disponibilidade			✓	✓	✓	✓		✓			✓	✓	✓			✓	✔
	Confidencialidade		✓						✓		✓				✓			
	Integridade							✓	✓	✓								
Abordagens	Centralizada		✓					✓	✓	✓	✓							
	Distribuída	✓		✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✔
Avaliação	*Zero-Knowledge*														✓			✔
	Histórico	✓							✓		✓	✓	✓	✓		✓	✓	
Mecanismos	Troca de mensagens			✓	✓	✓			✓	✓						✓		
	Desafios														✓			
	Recomendação		✓					✓						✓				
	Comunidades de interesse											✓	✓	✓				✔
	Estereótipos	✓					✓				✓							
Atributos para Composição da Confiança	Reputação							✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Interação					✓					✓	✓	✓	✓		✓		
	Confiança social						✓					✓	✓	✓			✓	✔
	Experiência					✓											✓	
	Conhecimento																✓	
	Confiabilidade		✓															
	Atividades		✓											✓				
	Dados recebidos e encaminhados			✓	✓				✓	✓								
	Encontros											✓	✓	✓				
	Localização						✓											

3.5 RESUMO

Ao longo desse capítulo observou-se que a literatura oferece diversas abordagens de confiança para garantir segurança na disseminação de dados em redes não estruturadas. O uso de técnicas como reputação, recomendação e, mais recentemente, comunidades de interesse prevalece entre os autores. Essa última demonstra ser promissora para uso em ambientes não estruturados, especialmente por permitir o emprego de informações sociais com critério para sua formação. Além disso, a criação e manutenção de históricos de observações mostram-se inviáveis nessas redes, tornando um desafio o desenvolvimento de soluções para garantir a segurança no acesso aos dados em ambientes sem memória. Ela demanda o emprego de várias técnicas ou a sua combinação de maneiras distintas das atualmente realizadas. Essa análise demonstrou que os trabalhos encontrados na literatura buscaram prover a segurança dos dados pela garantia de seus atributos - confidencialidade, disponibilidade e integridade. Todavia, observou-se que as soluções existentes nem sempre atendem a todos esses atributos de foma concorrente, atuando para garanti-los parcialmente, conforme o nível de segurança almejada.

4 STEALTH: UM MECANISMO PARA DISSEMINAÇÃO DE DADOS SENSÍVEIS BASEADO EM CONFIANÇA SOCIAL

Este capítulo apresenta um mecanismo para controle de disseminação dedados sensíveis baseado em confiança social, denominado STEALTH (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control*). Ele dissemina os dados sensíveis de uma pessoa em situação emergencial à uma pessoa adequada, baseado na sua competência e interesses. O STEALTH agrupa os nós da rede por aspectos oriundos das relações sociais das pessoas, que serão usados como critério para controlar a disseminação dos dados sensíveis de um pessoa em situação emergencial. A Seção 4.1 apresenta uma visão geral do mecanismo, aborda suas características, modelo de rede e de comunicação, além de sua forma de atuação. A Seção 4.2 descreve a arquitetura do mecanismo, detalha o processo de agrupamento dos nós da rede, a avaliação da confiança e o seu funcionamento. A Seção 4.3 apresenta um exemplo de funcionamento do mecanismo, e detalha sua operação para disseminação dos dados sensíveis de uma pessoa em situação emergencial.

4.1 VISÃO GERAL

O STEALTH atua entre as camadas de rede e de aplicação para garantir a disponibilidade da disseminação dos dados sensíveis das pessoas em situação emergencial. Ele se baseia em aspectos sociais dos proprietários dos dispositivos para criar redes locais ao longo do tempo, a fim de manter comunidades de interesses. Diante de eventos críticos, ele dissemina os dados sensíveis da pessoa em situação emergencial à uma pessoa adequada que esteja próxima. O objetivo do mecanismo é permitir o atendimento emergencial da pessoa necessitada, atuando de maneira complementar às estruturas hospitalares. Além da descrição dos componentes da arquitetura STEALTH e dos seus algoritmos, o seu funcionamento também é apresentado.

4.1.1 Modelo de Rede

O STEALTH executa sobre um conjunto de dispositivos portáveis (nós) interligados numa rede de comunicação sem fio denotados por $D = \{d_1, d_2, d_3, ..., d_j\}$, onde $d_j \in D$. Esses nós possuem capacidade de processamento e de comunicação para agrupar nós e disseminar dados, como ilustrado na Figura 4.1. Cada nó possui um identificador exclusivo (Id), que o identifica num dado instante de tempo. Assume-se que cada nó venha a ter atributos individuais de confiança. Trata-se de um conjunto de competências $S_n = \{s_1, s_2, s_3, ..., s_z\}$, tal que $|S_n| \neq 0$ e $S_n \subset S$, onde S é o conjunto de todas as competências. Uma competência representa uma habilidade, perícia ou conhecimento em uma determinada área de atuação, tal como médico, policial, enfermeiro, etc.

Assume-se, também, que cada nó venha a ter um conjunto de interesses $I_n = \{i_1, i_2, i_3, ..., i_z\}$, tal que $|I_n| \neq 0$ e $I_n \subset I$, onde I é o conjunto de todos os interesses. Um interesse é um *hobby*, gosto ou preferência, tal como música, saúde, entre outros. Os nós se agrupam por interesses em comum e formam comunidades por um dado período de tempo. Uma comunidade C é um conjunto de tuplas distintas ⟨nó, período, interesse⟩, onde $C = \{\langle d_1, P_l, i_z\rangle, \langle d_2, P_l, i_z\rangle, ..., \langle d_n, P_l, i_z\rangle\}$ e $P_l = ((t_{s0}, t_{e0}), (t_{s1}, t_{e1}), ..., (t_{sl}, t_{el}))$, com $t_{s*} \leq t_{e*}$. Definição adaptada do conceito de comunidades dinâmicas proposto por Coscia et al. (2011) e revisado por Rossetti e Cazabet (2018). Por simplicidade, assume-se que um nó desligado ou com

falhas não atua na rede. Assume-se, também, que todos os nós apresentam um comportamento não malicioso, sendo desconsiderada a ocorrência de ataques ao funcionamento do sistema.

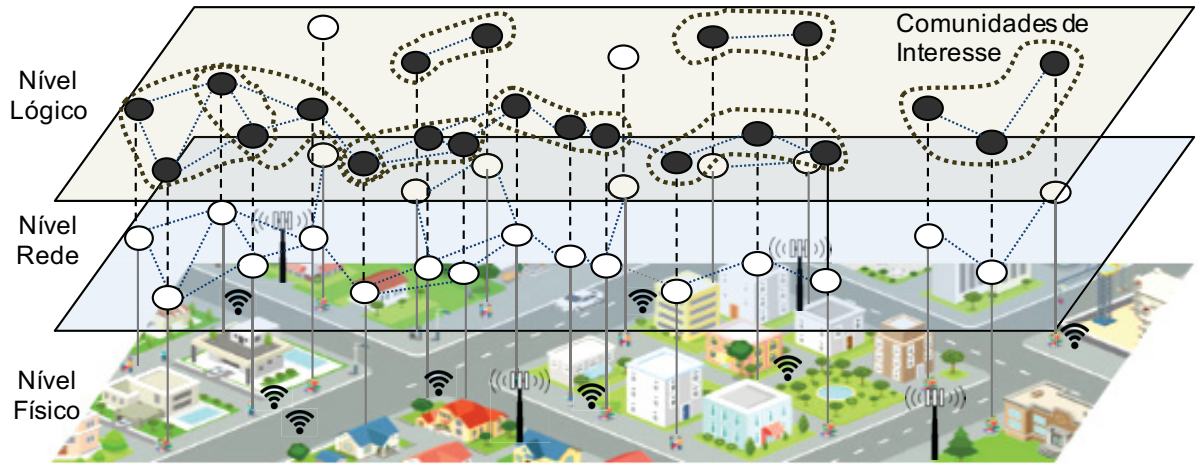


Figura 4.1: Modelo de rede e disseminação de dados sensíveis

As comunidades de interesse formam-se em função dos interesses em comum entre os nós da rede, sendo que a sua proximidade física permite a criação de conexões de rede entre eles. As comunidades estabelecidas pelo STEALTH foram sobrepostas (Chakraborty et al., 2017) (Chakraborty et al., 2012) (Xie et al., 2013), ou seja, um nó faz parte de diversas CoI simultaneamente e, conforme sua posição, haverá várias comunidades com um mesmo interesse, mas distantes fisicamente entre si. As CoI são estabelecidas ou modificadas na medida em que os nós se aproximam o suficiente para estabelecer uma conexão de rede *ad hoc* ou quando se afastam, interrompendo as conexões estabelecidas, respectivamente. Trata-se de uma adaptação do modelo usado por Bao e Chen (2012a), Bao e Chen (2012b) e Bao et al. (2013). A Figura 4.2 ilustra o tipo de rede *ad hoc* assumido, onde se observa diversos nós de rede conectados a um único nó, d_1. Quatro desses nós - d_1, d_2, d_3 e d_4 - formam um comunidade de interesse em saúde, cujo nó principal é d_1. Os nós - d_5 e d_6 - também estabelecem conexões com d_1, mas formam outras comunidades com ele, que não são representadas na figura.

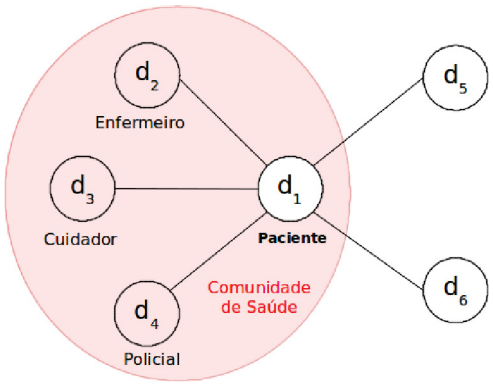


Figura 4.2: Modelo da rede *ad hoc* estabelecida

A mobilidade dos nós ao longo do tempo demanda a integração das dimensões espaciais e temporais relacionadas a eles dentro da rede. Essa rede é representada por grafos dinâmicos, também denominados grafos temporais (Sizemore e Bassett, 2017). Logo, uma rede é representada

por um grafo $G(V, E)$, onde os vértices V correspondem aos nós da rede, enquanto as arestas, $E : V \times V \Rightarrow \mathbb{R}$, correspondem às suas ligações. Essa representação destina-se às redes estáticas, nas quais não há mobilidade dos nós durante o seu tempo de funcionamento. A representação do modelo proposto distingue-se em razão do STEALTH criar redes locais dinâmicas, onde os nós se movimentam frequentemente ao longo do tempo. Nesses casos, a dimensão temporal agrega à representação a influência da mobilidade dos nós.Uma comunidade é representada por diversos grafos $G_0, G_1, ..., G_T$, um para cada momento $t = 0, 1, ..., T$, de operação da rede. Como exemplo, a Figura 4.3, baseada no trabalho de Sizemore e Bassett (2017), ilustra a evolução das conexões em uma rede ao longo do tempo. Essa rede possui 5 nós, sendo $V = \{1, 2, 3, 4, 5\}$. As arestas E variam, pois em cada tempo t há um grafo com ligações distintas. A Figura 4.4, adaptada de Sizemore e Bassett (2017), mostra o grafo G_1, relativo a $t = 1$, onde $E(G_1) = \{(1, 2), (2, 3), (2, 5), (3, 4)\}$. Para $t = 7$, o grafo G_7 possui as arestas $E(G_7) = \{(1, 3), (1, 5)\}$.

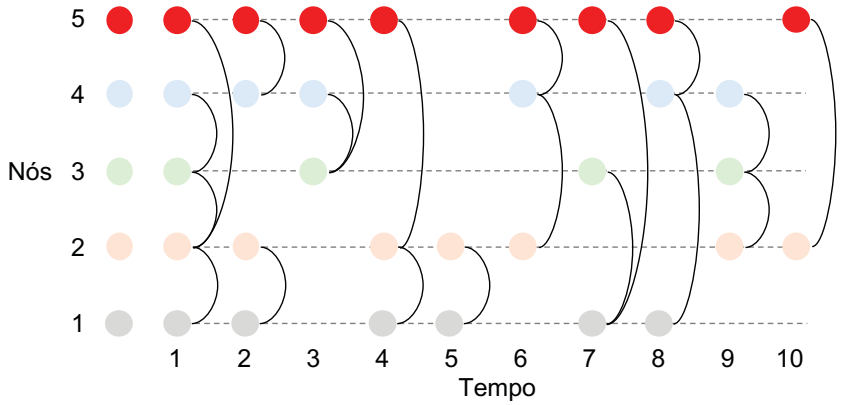


Figura 4.3: Evolução das conexões de rede ao longo do tempo

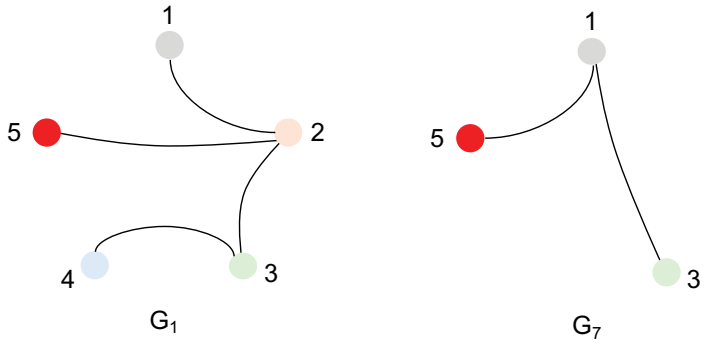


Figura 4.4: Grafos das conexões de rede em t_1 e t_7

As competências e interesses que cada nó possui permitirão medir sua confiança, que será usada com um critério para controlar a disseminação dos dados sensíveis de nós em situação emergencial. Dessa forma, os valores de confiança são vistos como pesos, que são associados aos vértices dos grafos. Portanto, a representação $G(V, E)$ deve incorporar essa informação de peso aos vértices. Cada grafo terá um conjunto de pesos W, denotado por $\{w_1, w_2, w_3, ..., w_y\}$, onde $w_y \in W$. A Equação 4.1 representa esse modelo de rede.

$$G(V, W, E) \tag{4.1}$$

A dinamicidade da rede e a mobilidade dos nós demandam que a dimensão temporal seja considerada para se verificar a evolução das ligações entre os nós ao longo do tempo. Assim, o grafo G é mostrado na Equação 4.2, onde T é um conjunto finito de instantes de tempo, V é um conjunto finito de vértices, N é um conjunto de nós (vértices) temporários, onde $N \subset T \times V$ e E é o conjunto de ligações $E \subset V \times V$, de modo que $(t, uv) \in E$, implicando $(t, u) \in E$ e $(t, v) \in E$. Esse conjunto de tempos T é discreto ou contínuo.

$$G(T, V, N, W, E) \tag{4.2}$$

Um nó cria suas comunidades incorporando nós vizinhos com os quais tem interesses em comum, que correspondem à sua vizinhança. A vizinhança N de um vértice v em um grafo $G(T, V, N, W, E)$ será dada por $N(v)$, sendo que $v \in V$ e $u \in V$, $N(v) = \{u, uv \in E\}$. O grau d de um vértice v, $d(v)$, equivale à quantidade de nós com os quais o nó relativo ao vértice v estabelece conexão em um dado momento e que pertencem às suas comunidades (Latapy et al., 2018).

4.1.2 Modelo de Comunicação

Os nós da rede iniciam seu funcionamento como nós isolados, agrupam-se por interesses em comum e formam comunidades de interesse (CoI). Um nó abandona uma CoI quando seu interesse difere dos demais nós da comunidade, sua mobilidade o afastar dos demais nós, interrompendo as conexões de rede estabelecidas, ou por decidir se desconectar da rede por interesse próprio. O ganho de escalabilidade é um dos benefícios dessa forma de agrupamento, pois comunidades possuem tamanhos variáveis, conforme a quantidade de nós que possuam, assim como restringem o tráfego de dados a esses nós. A transmissão dos dados entre os nós ocorre pelo meio sem fio, baseado no padrão IEEE 802.11, por um canal assíncrono. Esse padrão é empregado em trabalhos que verificam o comportamento de grupos pessoas ou multidões (Draghici e Steen, 2018). Dentre os comportamentos avaliados, verifica-se o fluxo de pedestres (Fukuzaki et al., 2014) (Fukuzaki et al., 2015) (Kalogianni et al., 2015), inclusive empregando-se *smartphones* (Kjærgaard et al., 2012) (Rachuri et al., 2013) (Ruiz-Ruiz et al., 2014). Os nós possuem raios de comunicação iguais e operam na mesma faixa de transmissão. As perdas de pacotes acontecem pela presença de ruído, mobilidade dos nós ou diante de outras falhas que venham a ocorrer com os dispositivos ao longo do seu funcionamento.

Na presença de eventos críticos, um nó em situação emergencial dissemina seus dados sensíveis a um outro nó pertencente à sua comunidade interesse (CoI) em saúde. Essa disseminação ocorre pelo emprego do método *push* (Gharaibeh et al., 2017). Para isso, durante a formação dessa CoI, a confiança nos vizinhos é medida a partir de seus interesses e competência. Sua confiança é usada como critério para controlar a disseminação dos dados sensíveis do nó em situação emergencial. Esses dados são disseminados apenas aos nós que possuírem determinadas características. Esses nós fisicamente próximos auxiliam nos primeiros atendimentos. A medição da confiança dos nós tem como referência a competência de médico e os interesses em comum que os nós avaliador e avaliado possuem. Quanto mais elevada a competência do nó avaliado, mais dados sensíveis ele acessa. Já os nós que não possuem habilidade na área de saúde receberão dados genéricos, tal como um contato de emergência, por exemplo.

4.2 ARQUITETURA STEALTH

Esta seção descreve os componentes do sistema STEALTH (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control*), bem como as suas interações e modo de funcionamento. A arquitetura do sistema STEALTH é composta de dois módulos, como ilustra a

Figura 4.5: o módulo **Gestão de Comunidades**, responsável por criar e atualizar as comunidades de interesse estabelecidas ao longo do tempo a partir da interação entre os dispositivos das pessoas portadoras; e o módulo **Gestão de Eventos Críticos**, responsável por verificar e disseminar os dados sensíveis da pessoa em situação emergencial ao dispositivo da pessoa adequada na presença de eventos críticos.

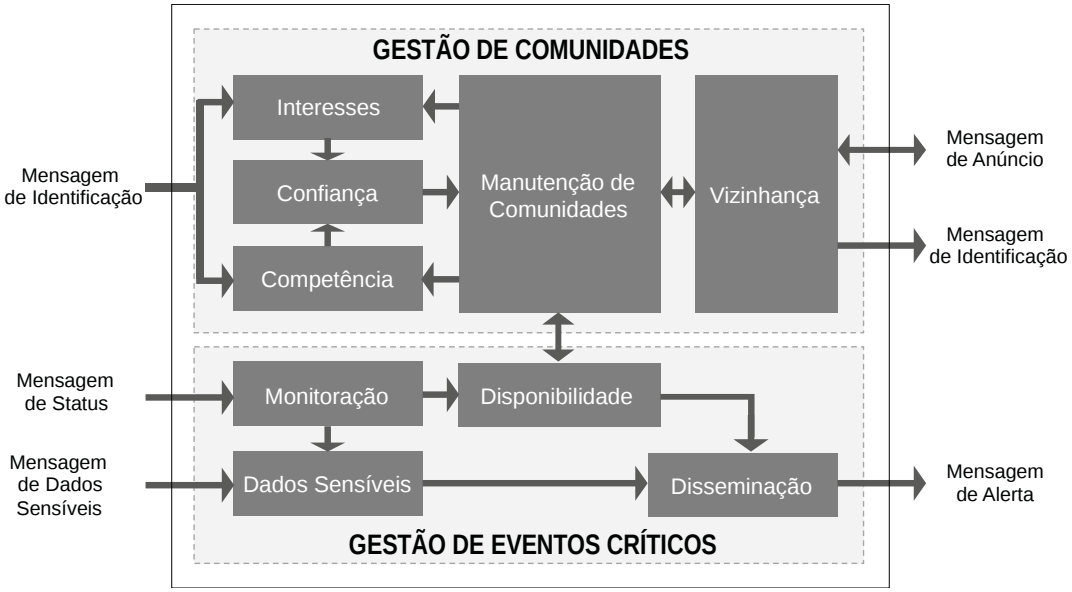


Figura 4.5: Arquitetura do STEALTH

4.2.1 Módulo Gestão de Comunidades

Este módulo mede a confiança dos dispositivos (nós) que estejam próximos e os inclui em uma comunidade ao receber sua mensagem de identificação, composta pelo seu *Id*, interesses e competência. Ele também é responsável por se identificar perante um nó que esteja em busca de nós vizinhos para formar suas próprias comunidades. Esse módulo é composto por cinco componentes: o componente *Vizinhança* busca por nós vizinhos e também encaminha uma mensagem de identificação a outros nós que também buscam por vizinhos, com o objetivo de identificar sua vizinhança; o componente *Interesses* verifica os interesses dos nós próximos ao recebê-los do nó vizinho, identifica interesses em comum para agrupar os nós e formar comunidades de interesse; o componente *Competência* trata da competência dos nós vizinhos ao receber suas informações de competência, a fim de saber o seu nível de competência em saúde; o componente *Confiança* mensura a confiança dos nós vizinhos ao receber seus interesses e competência, diante dos próprios interesses, a fim de verificar na sua comunidade de saúde o nó vizinho com a competência mais elevada em saúde; e o componente *Manutenção de Comunidades* coordena a criação, extinção e modificação das CoIs, a partir das informações de interação com os nós vizinhos. Assim, ele garante que as comunidades de interesse acompanhem a evolução das redes locais estabelecidas ao longo do tempo.

Os nós da rede iniciam sua operação de forma isolada. Na medida em que se movimentam, encontram outros nós e estabelecem comunidades de interesse. Esse processo é descrito no Algoritmo 1, que trata da gestão das comunidades de interesse. Periodicamente, cada nó limpa sua lista de vizinhos (*l*.3), anuncia sua presença por mensagens de anúncios em *broadcast* (*l*.4) à procura de nós vizinhos e aguarda um intervalo de tempo até um novo anúncio (*l*.5). Quando um nó vizinho percebe que um nó anuncia a sua presença (*l*.8), ele encaminha a este nó anunciador uma mensagem contendo sua identificação, competência e interesses (*l*.11). O nó anunciador, ao

Algoritmo 1: Gestão de Comunidades

```
1  procedure SearchNeighbors( )
2      while (true) do
3          NeighborList ← 0
4          SendAnnounce( )
5          WaitInterval( )
6      end while
7  end procedure
8  procedure ReceiveAnnounce( )
9      neighskill ← GetSkill( )
10     neighinterest ← GetInterests( )
11     AnswerAnnounce(id, neighskill, neighinterest)
12 end procedure
13 procedure ReceiveAnswer (id, neighskill, neighinterests)
14     if (HasCommonInterests( ) AND HasHealthInterest( ))
15         neightrust ← EvaluateNeighborTrust(neighskill, neighinterests)
16         NeighborList ← RegisterNeighbor(id, neighskill, neighinterests, neightrust)
17     end if
18 end procedure
19 procedure EvaluateNeighborTrust (neighskill, neighinterests)
20     skilltrust ← GetSkillTrust(skill, SkillsTaxonomy)
21     numcommoninterests ← GetNumCommonInterests(interests)
22     numnodeinterests ← GetNumNodeInterests( )
23     interesttrust ← numcommoninterests / numnodeinterests
24     return (skilltrust + interesttrust) / 2
25 end procedure
```

receber essa mensagem do nó vizinho, verifica a existência de interesse em comum em saúde entre eles (*l*.14). Quando há esse interesse em comum, ele mede a confiança do nó vizinho pela *EvaluateNeighborTrust* (*l*.15) e o insere na sua lista de vizinhos (*l*.16), dentro da sua comunidade de saúde. A medição da confiança do nó vizinho leva em conta a sua confiança acerca da sua competência (*l*.20) e dos interesses em comum que eles possuem (*l*.21-23).

4.2.1.1 Classificação de Competências

Dentre as características que as pessoas possuem, encontram-se as competências. Elas são profissões, habilidades ou *hobbies*, que lhes permitem executar as várias atividades do seu dia-a-dia. Essas competências estão distribuídas por diversas áreas. O STEALTH busca disseminar dados sensíveis com segurança às pessoas adequadas, ou seja, que detenham competência em saúde. Logo, algumas competências em saúde foram organizadas de forma hierárquica, usando o nível de conhecimento de cada profissão como critério. Essa organização deu origem à uma taxonomia, ilustrada na Figura 4.6, na qual as competências em saúde de cada profissão foram distribuídas por níveis, seguindo o modelo proposto por Carminati et al. (2016). Essa taxonomia é estendida com outras competências, conforme a necessidade existente.

O conhecimento em saúde é o critério principal da classificação realizada pelo STEALTH. Inicialmente, as pessoas são classificadas por possuírem ou não conhecimento em saúde. Aquelas que possuem são classificadas em duas áreas distintas - medicina e enfermagem. No ramo da medicina, encontram-se os médicos. Na ramo de enfermagem são incluídos os enfermeiros e diversos outros profissionais dessa área, além de uma classe de profissionais que possuem habilidades reduzidas em saúde, aqui denominados práticos. Nesse grupo incluem-se os cuidadores, policiais, bombeiros, entre tantos outros profissionais. Os práticos, por exemplo, são aquelas pessoas treinadas para prestar primeiros-socorros.

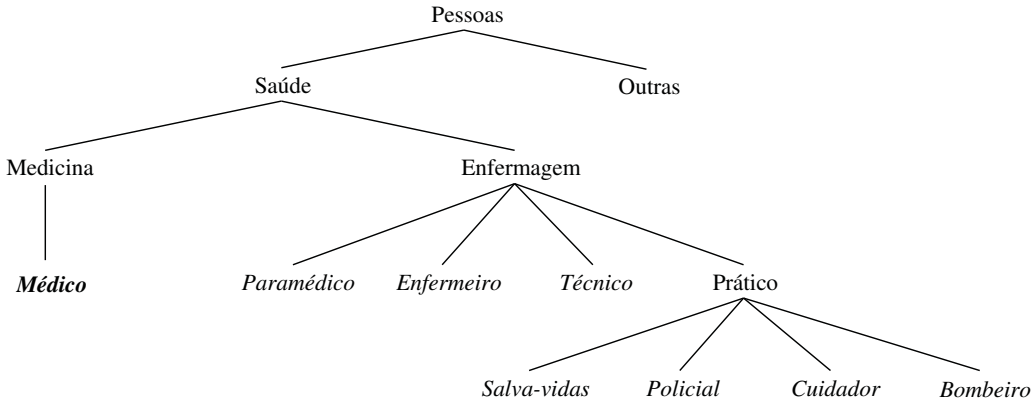


Figura 4.6: Taxonomia de competências em saúde

As competências que as pessoas possuem são avaliadas pela sua similaridade com aquelas incluídas nessa taxonomia. Esse processo é baseado nos trabalhos de Wu e Palmer (1994) e de Mohammad e Hirst (2012). Dada uma competência qualquer, verifica-se sua similaridade diante daquelas existentes na taxonomia, como ilustra a Figura 4.7. Neste trabalho, a competência de referência (s_{ref}) é o médico, visto ser a profissão com o nível mais elevado em conhecimento de saúde. O cálculo da Sim_s é realizado pela Equação 4.3, onde c_3 corresponde à quantidade de saltos entre entre o nível comum (l_{common}) mais próximo das competências avaliada e de referência até a raiz da taxonomia ($Raiz$). O c_2 equivale à quantidade de saltos entre a competência que se deseja verificar a similaridade (s_N) até a raiz da taxonomia ($Raiz$) e c_1 equivale à quantidade de níveis entre a competência de referência - médico - até a raiz da taxonomia ($Raiz$). Os valores de Sim_s variam na faixa $[0, 1]$ e se encontram na Equação 4.4.

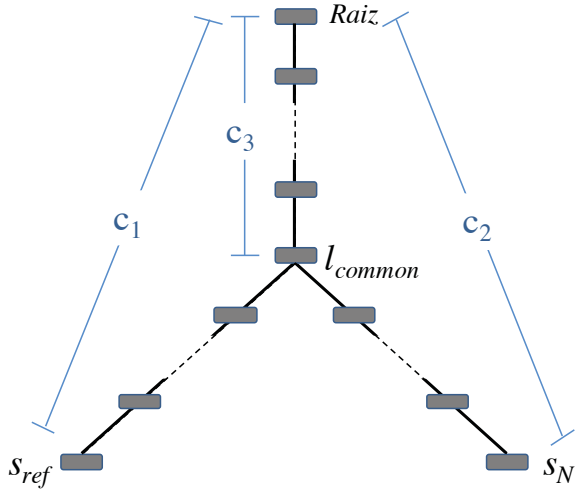


Figura 4.7: Medida da similaridade entre competências

$$Sim_s = \frac{2 \times c_3}{c_1 + c_2} \tag{4.3}$$

$$Sim_s = \begin{cases} 0, & se\ s\ \in \{outras\} \\ ]0, 1[, & se\ s\ \notin \{outras, médico\} \\ 1, & se\ s\ \in \{médico\} \end{cases} \tag{4.4}$$

Supondo que se deseje avaliar a similaridade entre a competência de salva-vidas e a de médico, empregando-se a taxonomia disponível na Figura 4.6. Observa-se que a competência de médico dista até a raiz da taxonomia 3 níveis, o que corresponde ao valor de c_1. A competência de salva-vidas dista até a raiz da taxonomia 4 níveis e equivale a c_2. Por fim, obtém-se a distância da classe comum entre as competências observadas - saúde - até a raiz da taxonomia. Ela dista 1 nível da raiz e equivale a c_3. Aplicando-se a Equação 4.3, obtém-se o valor 0,4, que é a similaridade da competência de salva-vidas dentro da taxonomia das competências.

4.2.1.2 Medição da Confiança

A medição da confiança ocorre diante dos atributos de confiança do nó avaliado, sendo um individual - *Competência* - e um outro relacional - *Similaridade*. A Competência indica uma habilidade percebida em um determinado nó, seja ela formal ou não, que ele detém para a execução de uma determinada tarefa (Cho et al., 2015) (Marsh, 1994). Ela é uma profissão, hobby, habilidade ou outra característica afim. O valor da confiança será tanto mais alto, quanto maior a competência em saúde do nó avaliado. A similaridade refere-se aos interesses em comum que o nó avaliador e o avaliado possuem. Logo, o valor da confiança aumenta à medida que esses nós possuam mais interesses em comum. A medição da confiança ocorre somente se o nó avaliado possuir, pelo menos, o interesse em saúde. Portanto, inexiste valor de confiança menor ou igual a 0, pois esse interesse em comum implica uma confiança mínima maior que 0.

Um nó i que encontra um nó j mede sua confiança acerca dos interesses em comum que ambos possuem, T_{ij}^{I}. Essa confiança equivale à razão entre os interesses em comum que os nós i, I_i, e j, I_j, possuem e os interesses do próprio nó avaliador I_i. Assim, busca-se quantificar o quão similar são os interesses do nó avaliado e do nó avaliador, sendo o nó avaliador a referência de interesses. Ela é obtida pela Equação 4.5, que é baseada no trabalho de Bao e Chen (2012b). Os valores de T_{ij}^{I} variam na faixa]0, 1], visto que a medição da confiança dar-se-á apenas se o nó j possuir interesse em saúde. A Equação 4.6 apresenta os valores possíveis de T_{ij}^{I}.

$$T_{ij}^{I} = \frac{|I_i \cap I_j|}{|I_i|} \tag{4.5}$$

$$T_{ij}^{I} = \begin{cases}]0,1[, & se \;\; I_i \cap I_j \neq 0 \;\; e \;\; I_i \neq I_j \; e \; \{saúde\} \subset I_i \cap I_j \\ 1, & se \;\; I_i = I_j \;\; e \;\; \{saúde\} \subset I_i \cap I_j \end{cases} \tag{4.6}$$

A confiança sobre a competência do nó j, T_{ij}^{Skill}, equivale à similaridade da competência do nó j e a competência de médico dentro da taxonomia, visto que o STEALTH assume essa competência como a mais elevada em saúde. A Equação 4.7 representa essa situação, onde os valores de T_{ij}^{Skill} variam na faixa [0, 1] e foram detalhados na Equação 4.4.

$$T_{ij}^{Skill} = Sim_j \tag{4.7}$$

Por fim, a confiança do nó i sobre o nó j, T_{ij} corresponde à soma da confiança relacionada aos interesses em comum que ambos possuem, T_{ij}^{I}, com a confiança oriunda da competência que nó j possui, T_{ij}^{Skill}, conforme a Equação 4.8. Os valores de T_{ij}^{I} e T_{ij}^{Skill} são somados e normalizados para uma faixa de [0, 0,5]. Os valores de T_{ij} variam na faixa]0, 1]. Como $T_{ij}^{I} > 0$, isso implica haver uma confiança mínima nos membros participantes dessa comunidade, cujo

valor depende da quantidade de interesses em comum entre os nós i e j. Os valores de T_{ij} variam conforme os valores de T_{ij}^{I}, disponíveis na Equação 4.6, e T_{ij}^{Skill}, disponíveis na Equação 4.4.

$$T_{ij} = \frac{T_{ij}^{I} + T_{ij}^{Skill}}{2} \tag{4.8}$$

Considere que um nó i avalia a confiança sobre um nó j, T_{ij}, cuja competência atribuída é de *cuidador*, e que ambos possuem um único interesse - *saúde*. Empregando-se a taxonomia de competências constante na Figura 4.6 e o interesse descrito, o resultado da T_{ij}^{Skill} será equivalente à similaridade, Sim_s, da competência do nó j, s_j. Logo, $Sim_s(s_j)$, que corresponde a $Sim_s(cuidador)$, terá o valor $0,28$, ou seja, $T_{ij}^{Skill} = 0,28$. A T_{ij}^{I}, obtida pela Equação 4.5, terá o valor 1, visto que o nó avaliador e avaliado possuem apenas *saúde* como interesse comum, único interesse de ambos. Logo, aplicando a Equação 4.8, a $T_{ij} = 0,64$. No entanto, caso o nó j tenha a competência *outras*, $Sim_s = 0$. Isso indica que ele não possui qualquer competência em atividades de saúde, $T_{ij}^{Skill} = 0$. Como $T_{ij}^{I} = 1$, a confiança de i em j, T_{ij}, terá o valor 0,5.

4.2.2 Módulo Gestão de Eventos Críticos

Neste módulo, o componente *Monitoração* verifica a condição de saúde da pessoa ao receber seu status de saúde. As mensagens dos dispositivos instalados junto ao seu corpo permitem identificar o momento de um evento crítico. O componente *Dados Sensíveis* obtém os dados sensíveis da pessoa em situação emergencial e garante sua disseminação apenas nessas condições. O componente *Disponibilidade* verifica a pessoa adequada para se disseminar os dados sensíveis, a fim de garantir que seja aquela com a competência mais elevada em saúde. O componente *Disseminação* coordena a disseminação dos dados sensíveis ao receber esses dados e a identificação da pessoa adequada. Essa disseminação ocorre por meio de mensagens de alerta somente às pessoas que pertençam à comunidade de saúde do nó e na medida de sua competência em saúde.

Algoritmo 2: Gestão de Eventos Críticos

```
1  procedure HandleEmergencyEvent( )
2      neighid ← GetHigherScoreNeighbor( )
3      neighskill ← GetNeighborSkill (neighid)
4      criticaldata ← GetCriticalData (neighskill)
5      SendAlert(neighid, criticaldata)
6      SendStopAnnounce( )
7  end procedure
8  procedure ReceiveAlert (id, criticaldata)
9      SendAckAlert( )
10 end procedure
11 procedure ReceiveStopAnnouce (Id)
12     NeighborList ← RemoveNeighbor(Id)
13 end procedure
```

Os nós pertencentes às CoI formadas com interesse em saúde apoiam os nós que representam as pessoas em situação emergencial, como descrito no Algoritmo 2. Desta forma, ao ocorrer um evento crítico com um determinado nó, ele verifica o nó vizinho com a confiança mais elevada (l.2) e obtém o dado sensível apropriado (l.3-4). Em seguida, envia uma mensagem de alerta para o nó selecionado (l.5) com seu dado sensível. Além disso, ele anuncia por *broadcast*

a interrupção de sua operação ($l.6$). Ao receber uma mensagem de alerta, o nó confirma seu recebimento ($l.9$). Quando um nó percebe que outro nó anuncia a interrupção de sua operação, ele exclui esse nó da sua lista de vizinhos ($l.11$). Isso impede que um nó em situação emergencial venha a ser selecionado para receber dados sensíveis de outros nós.

4.3 FUNCIONAMENTO DO STEALTH

Esta seção ilustra o funcionamento do mecanismo STEALTH em um ambiente urbano, demonstrando sua contribuição na disseminação segura dos dados sensíveis de uma pessoa em situação emergencial para que ela possa receber um primeiro atendimento. Considere uma área urbana onde as pessoas deslocam-se a pé pelas ruas existentes. Cada uma dessas pessoas possui uma profissão ou habilidade, que lhe habilita executar determinadas tarefas no seu dia-a-dia. Há médicos, motoristas, policiais, professores ou executivos, entre várias outras profissões. Os médicos detém o maior conhecimento em atendimento de saúde, enquanto policiais, por exemplo, possuem condições de prestar primeiros socorros. Certas pessoas são pacientes em tratamento médico e, eventualmente, precisam de atendimento emergencial.

Dentre essas pessoas, cinco delas possuem profissões distintas, como ilustrado na Figura 4.8, cujos ícones indicam essas profissões, além de também haver um paciente. Elas possuem um único interesse em comum, saúde, e não mantêm quaisquer relações entre si. Enquanto o policial, o bombeiro, a enfermeira e o médico possuem interesse em saúde por conta da sua profissão, outras pessoas, como o executivo, por exemplo, possuem interesse em saúde para que possam ajudar uma pessoa qualquer quando necessário. Elas possuem dispositivos de rede, como *smartphones*, para se conectarem em redes. O STEALTH roda nesses *smartphones* e está configurado para operar normalmente. O paciente possui, também, um dispositivo junto ao seu corpo, que constantemente verifica sua pressão arterial e informa a um aplicativo instalado em seu *smartphone*. Esse aplicativo comunica-se com o STEALTH para informar os valores de pressão arterial medidos e se estão dentro da normalidade para esse paciente.

Figura 4.8: Pessoas utilizando o sistema STEALTH

As interações entre as pessoas vistas na Figura 4.8, resultantes da sua mobilidade, são ilustradas na Figura 4.9. Elas retratam a formação de redes *ad hoc* pelos dispositivos das pessoas fisicamente próximas, levando à criação de redes locais dinâmicas, cuja topologia varia ao longo do tempo. O STEALTH inicia sua operação em cada dispositivo ao buscar por vizinhos, quando anunciam sua presença por uma mensagem em *broadcast* e aguardam um intervalo de tempo para fazer um novo anúncio.

No instante t_1, ilustrado na Figura 4.9, os vizinhos próximos ao paciente – *executivo* e *enfermeira* - encaminham para ele sua identificação, interesses, e competência. Ao receber essas informações, o módulo de Gestão de Comunidades do STEALTH do paciente verifica os interesses em comum entre ele e seus vizinhos, e calcula a confiança acerca desses interesses, T^I, pela Equação 4.5. Visto que eles possuem um único interesse - saúde, que é comum a todos eles, o valor de T^I para esses vizinhos é igual 1. Em seguida, o STEALTH calcula a confiança sobre a competência de cada vizinho, T^{Skill}, pela Equação 4.7. A T^{Skill} para o executivo terá valor

0, porque ele não possui competência em saúde, enquanto a da enfermeira, 0, 33. Por fim, ele calcula o indicador de confiança, T, dos vizinhos pela Equação 4.8. O executivo obtém valor 0, 5 e a enfermeira, 0, 66. Na medida em que que esses valores são calculados para cada vizinho, são armazenados na lista de vizinhos do paciente, dentro da sua comunidade de interesse em saúde.

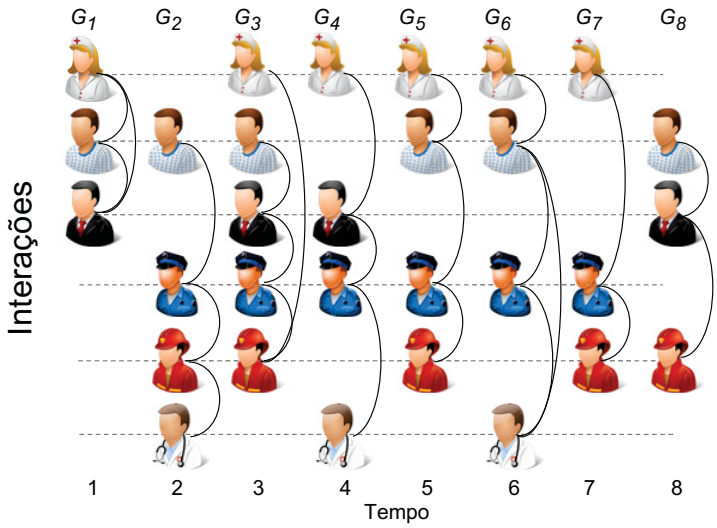


Figura 4.9: Pessoas interagindo ao longo do tempo

As interações entre as pessoas ao longo do tempo são representadas por grafos $G(V, E)$, onde as pessoas são seus vértices (V) e as interações, as arestas (E). O grafo G_1 representa a interação entre o paciente e seus vizinhos no instante t_1, sendo ilustrado na Figura 4.10. Nesse instante, o paciente, enfermeira e executivo estão próximos fisicamente, todos interagindo entre si, o que torna o grafo G_1 uma clique, pois para cada dois vértices em G_1, existe uma aresta que os conecta. Na medida em que o paciente se desloca pelas ruas, ele se afasta de algumas das pessoas e aproxima-se de outras. No instante t_1, ele está próximo da enfermeira e do executivo. No instante t_2, esses vizinhos se afastam e novos vizinhos surgem – policial, bombeiro e médico. Observa-se, potanto, que a mobilidade causa a evolução das suas vizinhanças ao longo do tempo. O STEALTH no *smartphone* do paciente acompanha as mudanças na sua vizinhança, modificando sua lista de vizinhos periodicamente, tal que a CoI em saúde do paciente se mantenha atualizada. Essas alterações na lista de vizinhos indicam as mudanças que ocorrem na topologia das redes locais estabelecidas ao longo do tempo e ressaltam sua dinamicidade.

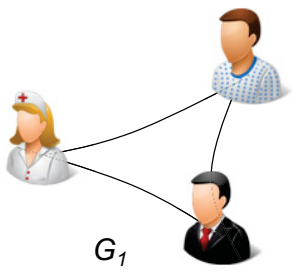


Figura 4.10: Grafo das interações em t_1

No instante t_6, os vizinhos próximos do paciente – *médico*, *policial* e *enfermeira* – encaminham sua identificação, interesses e competência a ele após perceberem que ele anuncia sua presença. Ao receber essas mensagens, como exibido na Figura 4.5, o módulo de Gestão de Comunidades do STEALTH do paciente verifica os interesses em comum que possuem e se

possuem interesse em saúde. Como possuem, ele calcula a confiança acerca desses interesses, T^I, pela Equação 4.5. Visto que elas possuem um único interesse em comum – saúde, o valor de T^I para os vizinhos é 1.A seguir, ele calcula a confiança sobre a competência que cada vizinho possui, T^{Skill}, pela Equação 4.7. A T^{Skill} do médico terá valor 1, enquanto a da enfermeira terá o valor $0,33$ e a do policial, $0,28$. Por fim, o indicador de confiança é calculado pela Equação 4.8. O médico obtém valor 1, a enfermeira, $0,66$, e o policial, $0,64$. Esses valores estão sumarizados na Tabela 4.1. Na medida em que os cálculos são feitos para cada vizinho, seus valores são mantidos na lista de vizinhos do paciente na sua comunidade de interesse em saúde.

Tabela 4.1: Valores obtidos para os indicadores de confiança

Usuário	**Competência**	T^{Skill}	T^I	T
	Médico	1	1	1
	Enfermeira	0,33	1	0,66
	Policial	0,28	1	0,64

O grafo G_6 representa as interações entre os nós e seus vizinhos no instante t_6, e é ilustrado na Figura 4.11. O STEALTH executa no dispositivo de rede de cada pessoa de maneira idêntica, fazendo com que cada um deles crie sua própria lista de vizinhos e comunidade de interesse em saúde. Isso ocorre porque todos possuem interesse em saúde. Logo, as interações no grafo G_6 possibilitam a formação de quatro comunidades de saúde distintas em t_6, ou seja, cada pessoa presente no grafo G_6 formará sua própria comunidade, que são retratadas na Figura 4.12.

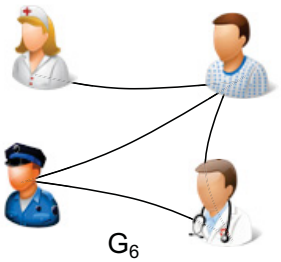


Figura 4.11: Grafo das interações em t_6

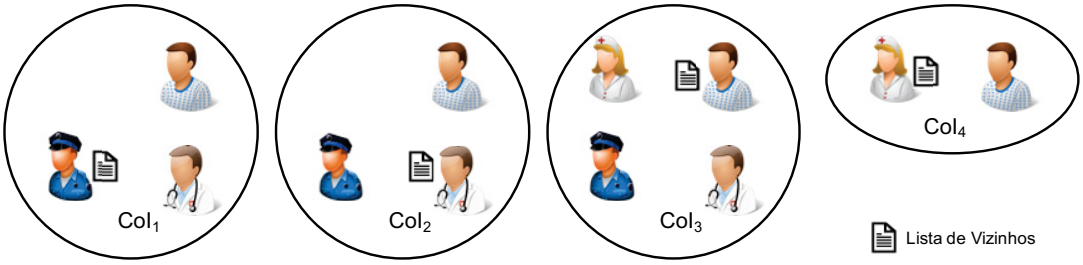


Figura 4.12: Comunidades de interesse formadas em t_6

Um evento crítico ocorre com o paciente no instante t_6, quando sua pressão arterial fica abaixo dos valores considerados normais para a sua condição de saúde. Nesse instante, como demonstrado na Figura 4.13, o paciente possui uma CoI em saúde formada, cujos membros

são o *médico*, a *enfermeira* e o *policial*. O módulo de gestão de eventos críticos do STEALTH instalado no seu *smartphone* identifica uma mudança no seu *status* de saúde, como mostrado na Figura 4.5. Portanto, ele busca na lista de vizinhos pelo membro da sua CoI em saúde com o indicador de confiança mais elevado. Ao verificar os indicadores de confiança, T, calculados quando a comunidade de interesse em saúde foi criada e sumarizados na Tabela 4.1, ele identifica um membro com indicador com valor 1, o mais elevado entre os vizinhos, que pertence ao médico. Então, o STEALTH do paciente coleta sua informação de pressão arterial e a encaminha ao STEALTH do médico. O médico, por sua vez, adota as providências que julgar necessárias para auxiliar o paciente, enquanto aguardam a chegada do atendimento especializado.

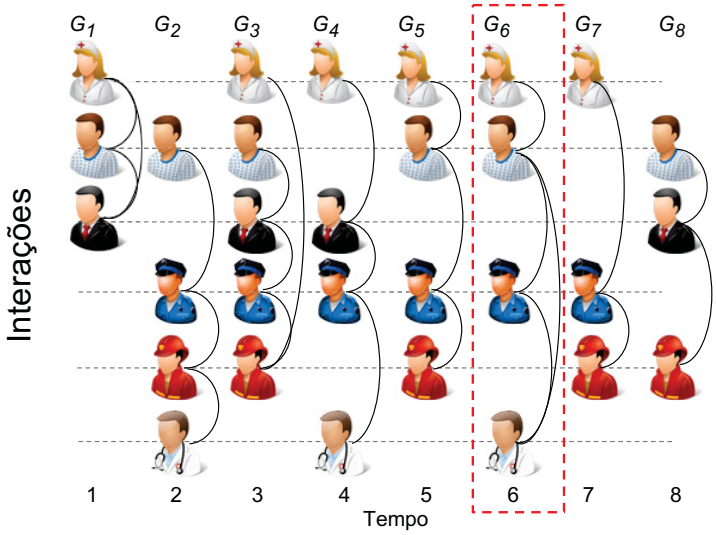


Figura 4.13: Evento crítico em t_6

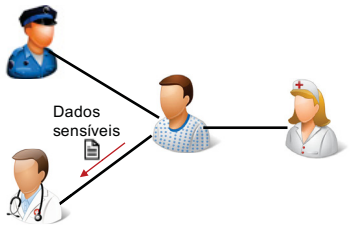


Figura 4.14: Disseminação dos dados do paciente em t_6

4.4 RESUMO

Este capítulo apresentou o mecanismo STEALTH, detalhou sua arquitetura e funcionamento. O emprego de grafos temporais para representar seu funcionamento demonstrou a relevância das dimensões temporais e espaciais no seu comportamento. A descrição do funcionamento destacou a a importância do agrupamento dos dispositivos por comunidades de interesse. O uso de aspectos sociais oriundos das relações sociais das pessoas – competência e interesses – ratificou que oferecem condições para garantir a disponibilidade do serviço de disseminação de dados sensíveis em situações emergenciais, impactando na sua segurança.

5 AVALIAÇÃO

O processo de avaliação do mecanismo STEALTH visou mensurar sua eficiência e eficácia para garantir a disseminação segura de dados sensíveis em situações emergenciais. Essa análise considera os resultados obtidos a partir do funcionamento do mecanismo em ambiente de simulação e diante de métricas previamente definidas especificamente para essa finalidade. As métricas aplicadas buscam evidenciar a eficácia do mecanismo STEALTH e o impacto do uso de comunidades de interesse e, especialmente, da confiança social, para garantia da segurança dos dados sensíveis disseminados. A Seção 5.1 descreve a implementação do mecanismo. A Seção 5.2 descreve os cenários avaliados e suas configurações. A Seção 5.3 apresenta as métricas selecionadas para avaliação do mecanismo. acompanhados das respectivas análises. Por fim, a Seção 5.5 discute os resultados alcançados.

5.1 IMPLEMENTAÇÃO

O STEALTH foi implementado e avaliado pelo simulador discreto de eventos NS-3 (*Network Simulator 3*) (Consortium, 2018), dado ao seu emprego no âmbito científico para o estudo de novas soluções para uso em redes. O NS-3 é uma ferramenta de código aberto, baseada nas linguagens C++ e Python, o que facilita o seu uso e acesso aos usuários. O código-fonte do NS-3 está disponível para alterações, o que permite que protocolos e eventos sejam modificados conforme a necessidade. Esse simulador permite a implementação redes, a coleta dos dados envolvidos no seu funcionamento e as métricas definidas para avaliação da solução implementada. O NS-3 suporta os principais protocolos de comunicação de redes, oferecendo condições de se avaliar soluções no contexto de vários tipos de redes, inclusive Internet das Coisas (IoT).

A versão do NS-3 utilizada foi a 3.28. Para isso, classe *node* foi modificada, para que incorporasse a lista de vizinhos dos nós, seus aspectos sociais - competência e interesses -, bem como armazenasse seus dados sensíveis e prioridade de atendimento. Os métodos e variáveis necessários foram adicionados à classe *node* sem interferir naqueles já existentes, a fim de alterar o comportamento das demais classes do simulador. Os códigos da aplicação, que incluem o STEALTH, a classe *node* modificada e os *traces* de mobilidade encontram-se no github[1]. Também está disponível nesse repositório as instruções para executar a aplicação.

A mobilidade dos nós empregada é oriunda do modelo realístico de Kouyoumdjieva et al. (2014) e representa o comportamento de movimentação de usuários em um ambiente urbano, o que permitiu observar as interações entre eles, especialmente seus encontros. Esse modelo foi adaptado para ser usado no mecanismo, pois dispunha de 3071 nós, quantidade muito além das necessidades da simulação desejada para o STEALTH. Além disso, o formato empregado para registro dos movimentos dos nós era distinto daquele usado pelo NS-3. Isso demandou sua conversão para o padrão exigido pela classe *Ns2MobilityHelper*. Do total de nós disponíveis no modelo, foram selecionados 100 nós dentre aqueles que apresentavam mobilidade por pelo menos um período de $900s$, que foi o tempo de simulação estabelecido.

Como previsto para o funcionamento do STEALTH, foram atribuídos interesses e competências aos nós, de modo que a formação de comunidades de interesse fosse viável. Além disso, essas informações também se aplicaram ao processo de cômputo da confiança realizada por alguns nós. Dentro do conjunto total de nós alocados para participarem da simulação, um subconjunto foi escolhido para ter seu comportamento controlado durante a simulação. Os nós

[1] https://github.com/agnaldosb/stealth

escolhidos entraram em situação emergencial num dado instante, quando se verificou como ocorriam as disseminações de dados sensíveis nesses momentos e as tomadas de decisão acerca dos atendimentos que aconteceram nos casos de emergências simultâneas.

5.2 CENÁRIOS AVALIADOS

As simulações foram realizadas com cenários distintos, permitindo observar o comportamento do STEALTH e suas ações em condições diversas. Alguns nós tiveram suas configurações pré-estabelecidas e fixas ao longo de todo esse processo, a fim de se comparar e avaliar os resultados obtidos entre as várias rodadas de simulação. Assume-se que todos os nós não apresentavam um comportamento malicioso para realizar ataques ao sistema e havia mecanismos de segurança para validação das suas identidades e proteção na transmissão dos dados. Por fim, diante dos resultados obtidos, os dados foram analisados e avaliados conforme métricas selecionadas especificamente para essa finalidade, empregando-se a ferramenta R (Foundation, 2018), versão 3.2.3, pelo aplicativo RStudio (RStudio, 2018), versão 1.1.463. Os resultados correspondem à média de 35 simulações e um intervalo de confiança de 95%.

O STEALTH foi avaliado diante três cenários distintos, a fim de analisar o seu funcionamento, verificar a disseminação dos dados sensíveis, além do impacto do emprego de comunidades de interesse e de aspectos sociais das relações das pessoas para controlar a disseminação esses dados. Os seguintes cenários forma empregados:

- *Cenário 1*: O STEALTH funciona normalmente e, diante de um evento crítico, um nó entra em situação emergencial. Nesse momento, ele verifica o vizinho de maior confiança em sua comunidade de saúde, dissemina seus dados sensíveis para esse vizinho, e interrompe a busca por novos vizinhos e o recebimento de mensagens. Não há confirmação do recebimento dos dados sensíveis. Este cenário representa uma situação urbana onde uma pessoa, diante de um evento crítico, entra em situação emergencial e há poucas pessoas próximas. Assim, a disseminação dos dados sensíveis para viabilizar o atendimento emergencial não demanda confirmação do recebimento desses dados.

- *Cenário 2*: O funcionamento do STEALTH ocorre como no Cenário 1, exceto que o nó para o qual os dados sensíveis foram disseminados deve confirmar seu recebimento. Enquanto essa confirmação não é recebida, o nó em situação emergencial continua a buscar por vizinhose mantém sua comunidade de saúde atualizada. Ao receber a confirmação de recebimento de seus dados sensíveis ou quando não houver outros vizinhos na sua comunidade de saúde, o nó deixa de buscar por novos vizinhos e de receber novas mensagens. Este cenário representa uma situação urbana comum em que uma pessoa sofre uma mal súbito, por exemplo, e necessita de atendimento emergencial.

- *Cenário 3*: Operação semelhante ao Cenário 2. Porém, os nós em situação emergencial disseminam, além dos dados sensíveis, um indicador de prioridade para atendimento. Ao receber dados sensíveis de vários nós simultaneamente, o STEALTH verifica os respectivos indicadores de prioridade dos nós em situação emergencial dos quais ele detém os dados sensíveis e confirma seu recebimento. Se as prioridades de atendimento dos nós forem diferentes, eles serão atendidos em ordem decrescente de prioridade, ou seja, da mais alta para a mais baixa. Se as prioridades forem iguais, o atendimento será na ordem de recebimento dos dados. Este cenário representa uma situação real onde várias pessoas entram em situação emergencial simultaneamente, como em acidentes de trânsito ou conflitos urbanos. Nesses casos, um único serviço de atendimento de

emergências atende às ocorrências. Porém, há necessidade de se tomar uma decisão acerca da ordem em que os atendimentos devem ocorrer, a fim de priorizar as situações mais urgentes ou aquelas onde a possibilidade de sobrevida do paciente é maior.

Esses cenários compartilham diversas configurações em comum. Contudo, dadas às distinções entre eles, o comportamento das simulações teve de ser modificado, a fim de atender aos objetivos de cada um. Para que fosse possível verificar o comportamento dos nós nos cenários, bem como comparar seu desempenho, foram selecionados alguns nós para possuírem atributos fixos em todas as rodadas de simulação para cada cenário específico. Isso permitiu demonstrar a eficiência e o desempenho do STEALTH. Aos demais nós presentes nas simulações, foram atribuídos randomicamente aspectos sociais distintos a cada simulação, criando um ambiente mais realístico. A seguir são descritas as configurações comuns aos três cenários simulados e aquelas específicas.

5.2.1 Configurações Comuns

Os cenários de simulação representaram situações realísticas, nas quais as pessoas se movimentavam em um ambiente urbano, a fim de se determinar a eficiência do uso de comunidades de interesse estabelecidas e verificar como ocorre a disseminação de dados sensíveis. Esse cenário baseou-se no modelo de mobilidade de Kouyoumdjieva et al. (2014) e usado por Helgason et al. (2014). Ele tem como base um trecho da Cidade de Estocolmo (Suécia), que traz à simulação características realísticas de um ambiente urbano de uma grande cidade. Trata-se de uma área de $400m$ x $430m$, onde os nós deslocam-se com velocidades entre 0,5m/s e 2,0m/s. Desse modelo, foram escolhidos 100 nós dentre aqueles disponíveis, cuja mobilidade se estende por um intervalo mínimo de $900s$, que foi a duração de cada rodada de simulação. Essa definição levou em conta que um nó ao deslocar-se na velocidade máxima prevista, 2,0m/s, durante $900s$, percorre 1800m. Essa distância corresponde a cerca de 65% das ruas existentes no modelo.

Tabela 5.1: Distribuição de profissionais de saúde

Profissional de Saúde	Médicos/ 1000 habitantes	Enfermeiros/ 1000 habitantes	Observações
Estocolmo (Suécia)	1,7	36,17	Existente em 2012 (population.city, 2015) (Socialstyrelsen, 2018)
Brasil	2	10	Existente em 2019 (de Medicina, 2019)(de Enfermagem, 2019) (de Geografia e Estatística, 2019)

O modelo de mobilidade citado foi incorporado ao ambiente de simulação e, a cada simulação, cada nó percorre sempre um mesmo caminho. O STEALTH aplica as competências e os interesses das pessoas nas tomadas de decisão para controlar a disseminação dos dados sensíveis. Elas são atribuídas aos nós logo no início de cada simulação. Cada nó recebeu uma única competência. Como o modelo de mobilidade refere-se à Cidade de Estocolmo, foram pesquisadas as distribuições de médicos e enfermeiros nessa cidade e também no Brasil, que se encontram relacionadas na Tabela 5.1. Os valores apontados nesta tabela não foram considerados nas atribuições das competências aos nós, a fim de permitir a realização das simulações com uma quantidade reduzida de nós, 100. As Tabelas 5.2 e 5.3 apresentam a distribuição das competências e interesses que foram efetivamente atribuídos aos nós em todas as simulações.

Os interesses foram atribuídos aos nós fazendo com que cada nó sempre tivesse, pelo menos, um interesse e no máximo cinco. A quantidade máxima está relacionada ao número

Tabela 5.2: Distribuição das competências atribuídos aos nós

Competência	Médico	Enfermeiro	Cuidador	Outras
Quantidade de Nós	10	15	20	55

de interesses disponíveis para atribuição vistos na Tabela 5.3. Os interesses e competências foram atribuídos aos nós de forma randômica, a cada rodada de simulação, nas quantidades relacionadas nas Tabelas 5.2 e 5.3. As competências previstas para distribuição na Tabela 5.2 foram classificadas e empregadas tendo como referência a taxonomia apresentada na Figura 4.6. Essa taxonomia possibilitou que cada nó medisse a confiança de outros nós pela Equação 4.7.

Tabela 5.3: Distribuição dos interesses atribuídos aos nós

Interesse	Saúde	Turismo	Música	Filmes	Livros
Quantidade de Nós	20	30	45	60	15

A comunicação entre os nós ocorreu utilizando a versão 4 do protocolo IP, sendo estabelecidas redes Ad-Hoc no padrão IEEE 802.11a e o protocolo de transporte UDP. O raio de transmissão foi de 50m, para permitir a formação comunidades de interesses ao redor dos nós e na medida em que se movimentam. Dessa forma, as pessoas selecionadas para receber os dados disseminados estariam próximas da pessoa em situação emergencial, facilitando o processo de atendimento emergencial.

5.2.2 Configurações Específicas

- ***Cenário 1***

  Três nós - 37, 52 e 70 - percorreram sempre o mesmo caminho cada um em todas as simulações. Eles foram selecionados porque se movimentam durante toda a duração da simulação e percorrem os caminhos mais longos no ambiente urbano selecionado. A esses nós fixos foi atribuída sempre a mesma competência em todas as rodadas - *outras* - e todos os interesses possíveis - *saúde, turismo, música, filmes* e *livros*. Foram selecionados dois instantes de tempo distintos para que ocorressem os eventos críticos e os nós entrassem em situação emergencial, 300s e 890s. Cada um deles representa o funcionamento do STEALTH, porém demonstrando comportamentos diferentes. Analisando-se o modelo de mobilidade empregado, no instante 300s os nós se movimentam de forma intensa. Assim, observou-se nesse instante diversas interações entre eles e a presença da vizinhança dos nós avaliados. Por outro lado, o instante 890s encontra-se no fim da simulação. Naquele instante, os nós se movimentam menos e as interações entre eles reduzem bastante, muitas vezes os não possuem quaisquer vizinhos. Além disso, como o evento crítico ocorre aos 890s, pode-se constatar a evolução das vizinhanças dos nós avaliados ao longo de toda a simulação. Foram rodadas 35 simulações com os nós entrando em situação emergencial no instante $300s$ e outras 35 simulações com esses nós entrando em situação emergencial em $890s$.

- ***Cenário 2***

  Semelhante ao Cenário 1, exceto que o nó que recebe os dados sensíveis disseminados por um nó em situação emergencial deve confirmar seu recebimento. Enquanto essa confirmação não é recebida, o nó em situação emergencial continua a buscar por

vizinhos e mantém sua comunidade de saúde atualizada. Ao receber a confirmação de recebimento de seus dados sensíveis ou quando não houver outros vizinhos na sua comunidade de saúde, o nó deixa de buscar por novos vizinhos e de receber novas mensagens. Como no Cenário 1, foram selecionados três nós - 37, 52 e 70 - e rodadas simulações com esses nós entrando em situação emergencial nos instantes 300s e 890s.

- ***Cenário 3***

  Esse cenário é semelhante ao Cenário 2. Todavia, os nós em situação emergencial disseminam seus dados sensíveis e, também, um indicador de prioridade de atendimento. Assim, quando vários nós entram em situação emergencial e disseminam seus dados sensíveis para um único nó, ele define a ordem em que confirmará o recebimento dos dados sensíveis usando os indicadores recebidos. Se esses indicadores forem diferentes, os nós serão atendidos em ordem decrescente de prioridade, ou seja, da mais alta para a mais baixa. Se forem iguais, o atendimento será pela ordem de recebimento dos dados.

  A definição da ordem de prioridade de atendimento na simulação somente é possível se vários nós enviarem seus dados sensíveis e o respectivo indicador de prioridade para um único nó simultaneamente ou em um intervalo de tempo próximo um do outro. Logo, foram selecionados três nós que atendessem à essa necessidade: 52, 69 e 70. Um quarto nó - 63 - foi escolhido para receber os dados dos nós citados. A escolha dos nós e do momento de interação entre eles considerou sua movimentação no modelo de mobilidade. Aos nós que entrariam em situação emergencial - 52, 69 e 70 - foi atribuída sempre a mesma competência - *outras* - e todos os interesses possíveis - *saúde, turismo, música, filmes* e *livros*. Para o nó - 63 - foram atribuídos esses mesmos interesses, mas a competência foi diferente - *médico*, tornando sua confiança a mais elevada dentro das comunidades de saúde dos nós que com ele viessem a interagir, aumentando suas chances de vir a ser selecionado para receber os dados sensíveis de outros nós. O instante escolhido para que os nós entrassem em situação emergencial foi aos 485s. Nesse momento, analisando-se o comportamento do modelo de mobilidade empregado, os nós 52, 69 e 70 se encontravam próximos o suficiente do nó 63 para que pudessem interagir e disseminar seus dados sensíveis a ele. Foram rodadas 35 simulações com os nós entrando em situação emergencial nesse instante.

A Tabela 5.4 sintetiza as configurações dos cenários avaliados, possibilitando ao leitor ter uma visão geral das situações que serão objeto de avaliação ao longo das simulações realizadas.

Tabela 5.4: Síntese das características dos cenários avaliados

Cenário	**UM**	**DOIS**	**TRÊS**
Disseminação	Dados sensíveis		Dados sensíveis e indicador de prioridade de atendimento
Confirmação do recebimento dos dados sensíveis	Não	Sim	
Encerramento da operação	Após disseminação dos dados sensíveis	Após receber a confirmação do recebimento dos dados sensíveis	
Nós com atributos fixos	37, 52 e 70		52, 63, 69 e 70
Ocorrência de eventos críticos	300s e 890s		485s

5.3 MÉTRICAS

A avaliação do desempenho do STEALTH ocorreu a partir da análise dos resultados obtidos em simulação, por métricas definidas previamente. Elas refletem o seu comportamento ao longo desse processo, inclusive caracterizando o modelo de mobilidade empregado. Para isso, foram definidos dois tipos de métricas distintas, sendo uma métrica de caracterização do modelo de mobilidade e cinco métricas de desempenho, que são apresentadas nas subseções a seguir.

5.3.1 Métrica de Caracterização

O modelo de mobilidade empregado possui características que precisam ser compreendidas, especialmente a forma como os nós se movimentam durante as simulações. Como cada um dos nós avaliados - 37, 52, 63, 69 e 70 - deslocam-se sempre pelos mesmos caminhos, eles estabelecem sempre as mesmas vizinhanças ao longo do tempo. Logo, há necessidade de se caracterizar esse comportamento. Essa caracterização permite verificar a influência do modelo de mobilidade nos resultados obtidos, especialmente na formação das comunidades de interesse.

A métrica *Número médio de vizinhos (N_N)* foi definida para representar a quantidade média de nós que pertencem às redes locais de um nó específico ao longo do tempo. Ela é empregada na avaliação de grafos (Latapy et al., 2018) e foi adaptada às necessidades deste trabalho. O N_N é obtido pelo somatório do somatório da razão entre o total de vizinhos de um nó, N, a cada intervalo de tempo, $j = t_s$, e a quantidade total de intervalos de tempo, t_s, onde essa vizinhança foi computada, multiplicado pelo total de simulações realizadas, N_S. Esse somatório será realizado para cada simulação, $i = N_S$. O N_N é computado pela Equação 5.1.

$$N_N = \sum_{i=1}^{N_S} \sum_{j=1}^{t_s} \frac{N_{ij}}{t_s \times N_S} \tag{5.1}$$

5.3.2 Métricas de Desempenho

A avaliação do desempenho do STEALTH ocorreu a partir da análise dos resultados obtidos em simulação, por métricas definidas previamente. Elas refletem o seu comportamento ao longo desse processo e tiveram como foco verificar sua robustez (do inglês, *dependability*) e sua segurança (do inglês, *safety*), na disseminação dos dados sensíveis. Além disso, as métricas demonstram o impacto dos aspectos sociais e comunidades de interesse na garantia da disponibilidade da disseminação desses dados. A análise da confiabilidade do serviço de disseminação dos dados é mensurada através das métricas **Taxa de Sucesso no Acesso aos Dados (**TS**)**, **Taxa de Dados Não Acessados (**TN_a**)**, **Tempo Médio de Acesso aos dados sensíveis (**MTA**)** e **Taxa de sucesso no acesso aos dados por competência** (TS_{Skill}). A análise da disponibilidade dos dados provida pelo STEALTH leva em conta a evolução das comunidades de interesse em saúde ao longo do tempo e a métrica **Número Médio de Comunidades de Interesse em Saúde** (N_C). Essas métricas são apresentadas a seguir.

- *Número médio de comunidades de interesse em saúde (N_C)*: Indica como os nós se agrupam em comunidades de interesse em saúde ao longo do tempo. Essa métrica é empregada para avaliar comunidades (Chakraborty et al., 2017) e os algorítimos de detecção de comunidades (Wagenseller et al., 2018). Ela representa a quantidade média de comunidades de interesse em saúde (N_C) formadas ao longo de todas as simulações. Equivale ao somatório do somatório da razão entre todas as comunidades de interesse

em saúde ($C_i j$) estabelecidas em cada simulação, $i = N_C$, e o total de intervalos de tempo, $j = t_s$, onde essas comunidades foram estabelecidas, multiplicados pelo total de simulações realizadas. O N_C é computado no intervalo que varia de 1 até t_s, que corresponde à quantidade de intervalos de tempo de simulação que um nó estabelece comunidades ao longo simulação. O N_C é obtido a partir da Equação 5.2.

$$N_C = \sum_{i=1}^{N_S} \sum_{j=1}^{t_s} \frac{C_{ij}}{t_s \times N_S} \tag{5.2}$$

- *Taxa de Sucesso no Acesso aos Dados* (TS): Indica a eficácia do mecanismo em garantir que dados sensíveis de um nó em situação emergencial disseminados a um nó adequado foram acessados com sucesso. Ela é computada pela razão entre a quantidade de vezes em que os dados foram disseminados e acessados com sucesso, A_{Sucess}, e a quantidade total de vezes que os dados sensíveis estiveram disponíveis para disseminação, A_{Disp}. O resultado é multiplicado por 100 para se obter o porcentual correspondente, conforme Equação 5.3. A A_{Disp} equivale ao total de simulações realizadas, N_S, pois os nós analisados entram em situação emergencial uma vez a cada rodada de simulação.

$$TS = \frac{A_{Success}}{A_{Disp}} \times 100 \tag{5.3}$$

- *Taxa de Dados Não Acessados* (TN_a): Indica ao porcentual de dados sensíveis de um determinado nó que não foram acessados ao longo das simulações, quando esse nó encontrava-se em situação emergencial, mas estavam disponíveis para disseminação. É o complemento da TS para atingir 100%, conforme a Equação 5.4.

$$TN_a = 100 - TS \tag{5.4}$$

- *Taxa de Sucesso no Acesso aos Dados por Competência* (TS_{Skill}): Indica o porcentual de dados sensíveis disseminados e acessados com sucesso para cada competência disponível atribuída os nós da rede. Ela corresponde à razão entre os dados sensíveis disseminados e acessados com sucesso pelos nós com uma determinada competência, A_{Skill}, e o total de acessos com sucesso, $A_{Success}$. Esse valor é multiplicado por 100 para obter o porcentual correspondente. A TS_{Skill} é obtida pela Equação 5.5 e observando-se a distribuição das competências atribuídas pela Tabela 5.2.

$$TS_{Skill} = \frac{A_{Skill}}{A_{Success}} \times 100 \tag{5.5}$$

- *Tempo Médio de Acesso aos Dados Sensíveis* (MTA): Indica o intervalo médio de tempo para acesso aos dados sensíveis de um nó em situação emergencial, a partir do momento de sua disseminação, para todas as simulações realizadas. Segundo Association et al. (2012), o tempo máximo aceitável para a entrega de dados médicos é de 125 milisegundos. Ela equivale ao somatório da razão dos intervalos de tempo entre o momento da disseminação dos dados sensíveis, td, e o momento do acesso pelo

nó selecionado, ta, de cada simulação realizada, $i = N_S$ e número total de simulações realizadas, N_S. A Equação 5.6 representa o cômputo dessa métrica.

$$MTA = \sum_{i=1}^{N_S} \frac{ta_i - td_i}{N_S} \tag{5.6}$$

5.4 RESULTADOS E ANÁLISE

Esta subseção apresenta os resultados obtidos ao longo das simulações realizadas para os três cenários avaliados e analisa suas contribuições para demonstrar a robustez - disponibilidade e a confiabilidade - e a segurança - disponibilidade - do STEALTH na garantia da disseminação dos dados sensíveis. Para efeito de completude, os resultados da simulações dos Cenários 1 e 2 referentes aos eventos críticos que ocorreram aos 890s, são apresentados no Apêndice A.

5.4.1 Caracterização do Modelo de Mobilidade

O modelo de mobilidade empregado (Kouyoumdjieva et al., 2014) possui características específicas, tais como a velocidade com que os nós se movimentam e os caminhos que percorrem ao longo do tempo. As velocidades são conhecidas e variam entre 0,5m/s e 2m/s. Os caminhos percorridos pelos nós são sempre os mesmos. Assim, considerando-se os cenários avaliados como especificado na Subseção 5.2.2, a métrica Número de Médio de Vizinhos (N_N) foi empregada para caracterizar o modelo, especialmente acerca dos nós previamente selecionados em cada cenário. As Figuras 5.1, 5.2 e 5.3 demonstram como se comportam as vizinhanças dos nós.

Nas Figuras 5.1(a), 5.2(a) e 5.3(a) constata-se que a vizinhança dos nós analisados - 37, 52 e 70 - tiveram um comportamento semelhante. Os nós 37 e 52 mantiveram um N_N semelhante nos cenário 1 e 2. A vizinhança do nó 70 destacou-se pela quantidade de nós. O cenário 3 apresentou resultados distintos dos demais, como demonstra a Figura 5.3(a). O comportamento do nó 69 destaca-se, visto que ele manteve uma vizinhança muito pequena, resultando no $N_V = 0$. Esses números correspondem à razão entre o total de nós que formaram as redes locais ao redor de cada nó avaliado e o total de simulações para cada cenário.

A métrica N_N é representativa para a avaliação dos resultados obtidos ao longo das simulações, pois caracteriza o modelo de mobilidade e indica a presença de vizinhança em torno dos nós avaliados. Contudo, ela não demonstra sua evolução ao longo do tempo. As Figuras 5.1(b), 5.2(b) e 5.3(b) apresentam a evolução da vizinhança em torno dos nós 37, 52, 69 e 70, conforme o cenário avaliado e em uma determinada rodada de simulação. A evolução da vizinhança é computada a partir de 25s do início de cada simulação, que é o tempo mínimo para que os 100 nós envolvidos na simulação estejam em condições de enviar e receber mensagens normalmente. A presença da vizinhança do nó 70 no cenário 1, por exemplo, ilustrada na Figura 5.1(b), indica que o STEALTH criou redes locais em torno desse nó durante 100% do tempo que ele esteve ativo na simulação. O oposto aconteceu com o nó 69 no cenário 3, Figura 5.3(b). Ele criou redes locais ao seu redor apenas a partir de $393s$ do início da simulação, ou seja, em $14,6\%$ do seu tempo funcionamento durante a simulação, vindo a interromper seu funcionamento aos $485s$, quando entrou em situação emergencial. Em ambas as situações, a vizinhança é uma característica própria do modelo de mobilidade empregado.

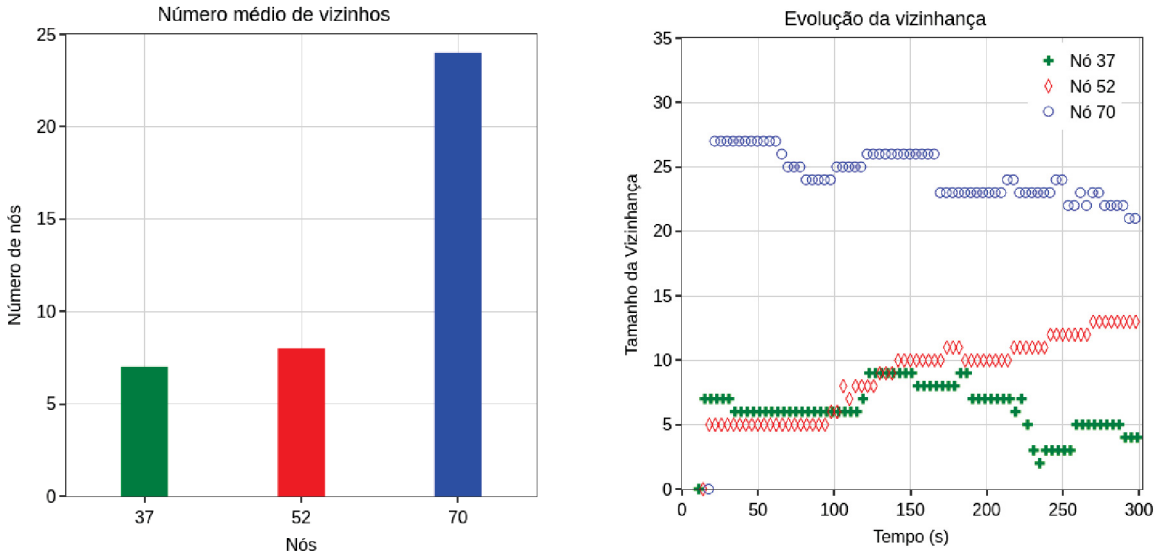


Figura 5.1: Dinamicidade e tamanho das redes locais ao longo do tempo
Cenário 1 - Evento crítico aos 300s da simulação

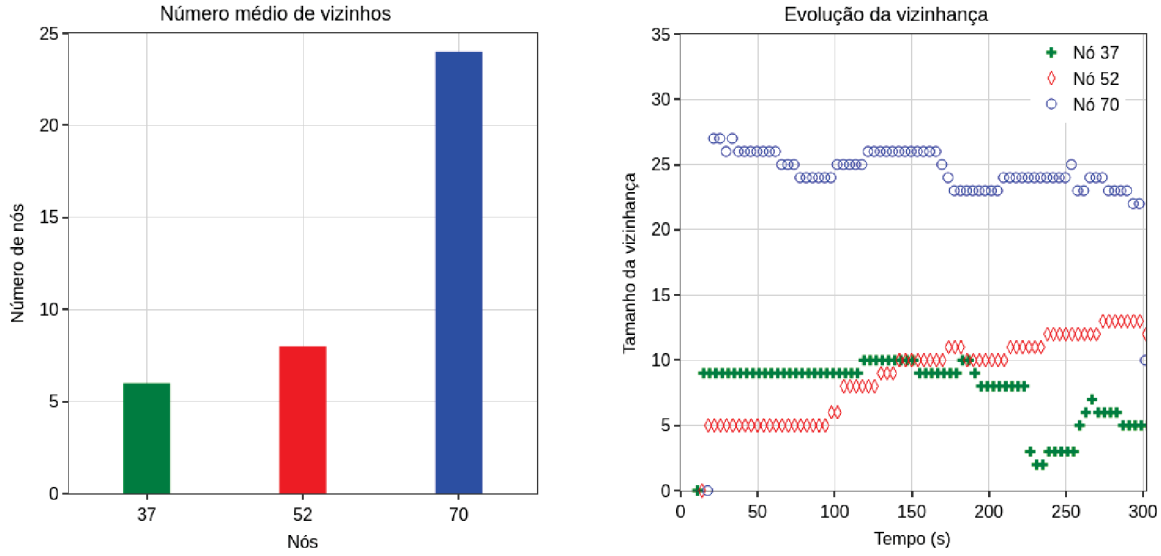


Figura 5.2: Dinamicidade e tamanho das redes locais ao longo do tempo
Cenário 2 - Evento crítico aos 300s da simulação

Os cenários 1 e 2 foram configurados para que os nós entrassem em situação emergencial aos 300s, enquanto no cenário 3, aos 485s. Esses instantes foram escolhidos por serem momentos de interações mais frequentes no modelo de mobilidade. Esse comportamento foi verificado previamente para definir essas configurações, o que se reflete no tamanho da vizinhança dos nós. O nó 70 tinha uma vizinhança com 22 nós no cenário aos 300s, como se constata pela Figura 5.1(b). Nesse momento, ele possuía diversos vizinhos para os quais disseminaria seus dados sensíveis nesse instante. Por outro lado, o nó 69 apresentou um comportamento distinto no cenário 3, que é retratado pela Figura 5.3(b). Em situação emergencial, ele possuía 3 vizinhos. Porém, em grande parte da simulação, sua mobilidade fez com que ficasse sem vizinhos.

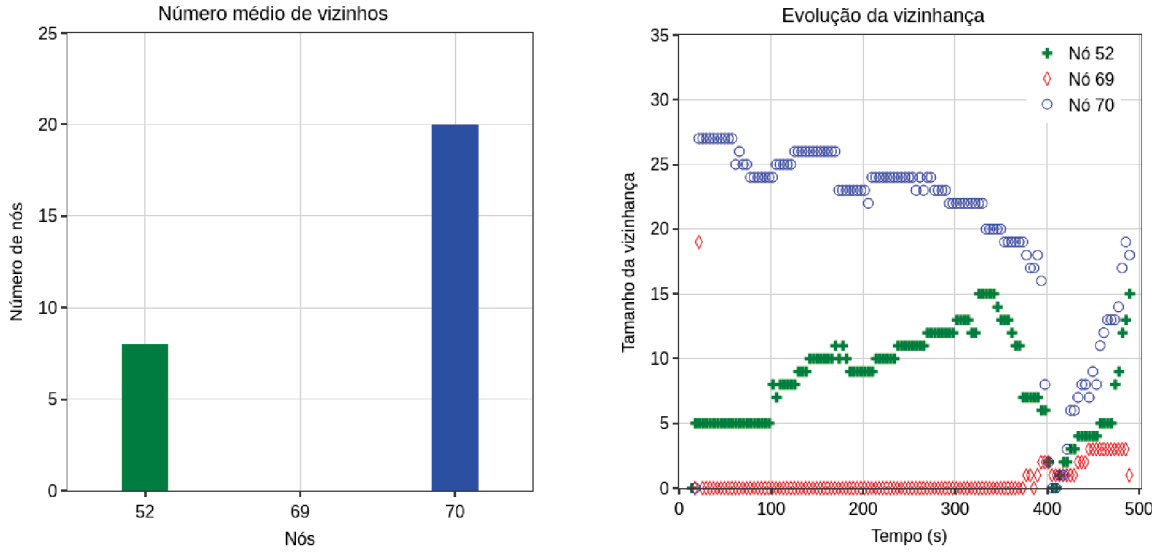


Figura 5.3: Dinamicidade e tamanho das redes locais ao longo do tempo
Cenário 3 - Evento crítico aos 485s da simulação

5.4.2 Disponibilidade

O Número Médio de Comunidades de Interesse em Saúde, N_C, estabelecidas por cada nó avaliado ao longo das respectivas simulações é distinto e é apresentado nas Figuras 5.4(a), 5.5(a) e 5.6(a). Os nós entraram em situação emergencial aos 300s, cenários 1 e 2, e aos 485s, cenário 3, próximos do instante central de cada rodada de simulação. Nesses momentos, a mobilidade dos nós implicou o estabelecimento de uma quantidade menor de comunidades do que nos cenários onde os eventos críticos ocorreram aos 890s. No cenário 1, conforme demonstra a Figura 5.4(b), o nó 37 estabeleceu um $N_C = 4$ para todas as simulações. No cenário 2, a quantidade de comunidades estabelecidas aumentou para 6, enquanto no cenário 3, o N_C ficou em 13. O nó 70 teve um comportamento semelhante nos três cenários, onde seu N_C3 aumentou desde o cenário 1 até o 3, quando atingiu 20, o que aumenta a disponibilidade para disseminação de seus dados em situações emergenciais. Isso caracteriza a dinamicidade das redes locais estabelecidas, especialmente da sua topologia. A mobilidade dos nós através de caminhos distintos, associada aos aspectos sociais - interesses - atribuídos a eles, impactou na formação dessas comunidades.

As Figuras 5.4(b) e 5.5(b) e 5.6(b) apresentam os gráficos da dinamicidade das comunidades de saúde dos nós 37, 52, 69 e 70 estabelecidas pelo STEALTH e seu tamanho ao longo do tempo em uma rodada específica de simulação. Os resultados mostram que o STEALTH acompanhou a dinamicidade das redes locais criadas, especialmente diante da mobilidade dos nós. Ele conseguiu verificar as mudanças nas vizinhanças dos nós e ajustou suas comunidades de interesse em saúde, a fim de mantê-las atualizadas. Nos cenários 1 e 2, conforme observa-se nas respectivas figuras, os nós 37, 52 e 70 mantiveram comunidades de saúde em 100% do tempo de simulação em que estiveram ativos. Durante esse período de tempo, o sistema esteve pronto para disseminar seus dados sensíveis, pois identificou nós que poderiam auxiliá-lo. Ao entrarem em situação emergencial, aos 300s, todos possuíam vizinhos ao seu redor e estabeleceram comunidade com alguns deles. Isso ocorreu por conta do modelo de mobilidade, que propiciou interações entre os nós até o instante em que entraram em situação emergencial. No cenário 3, a situação mostrou-se distinta, conforme se observa na Figura 5.6(b), quando foram avaliados os nós 52, 69 e 70. Constata-se que o nó 52 manteve comunidades de saúde em 93,39% do tempo de simulação em que esteve ativo. Durante esse período de tempo, o sistema esteve pronto para disseminar seus dados sensíveis, pois identificou nós que poderiam auxiliá-lo. Ao

entrar em situação emergencial, aos 485s, havia vizinhos ao seu redor e ele estabeleceu uma comunidade com alguns deles. Logo, ele disseminou seus dados sensíveis. O nó 69 manteve um comportamento distinto e estabeleceu comunidades apenas por 11,30% do tempo, até que entrou em situação emergencial. Por fim, constata-se que o nó 70 foi aquele que manteve comunidades de saúde por mais tempo, 98,26%. Esse comportamento é corroborado pela Figura 5.6(a), onde o nó 69 estabeleceu o menor N_C, 4, já o nó 70 apresentou o maior valor entre todos os nós, 20.

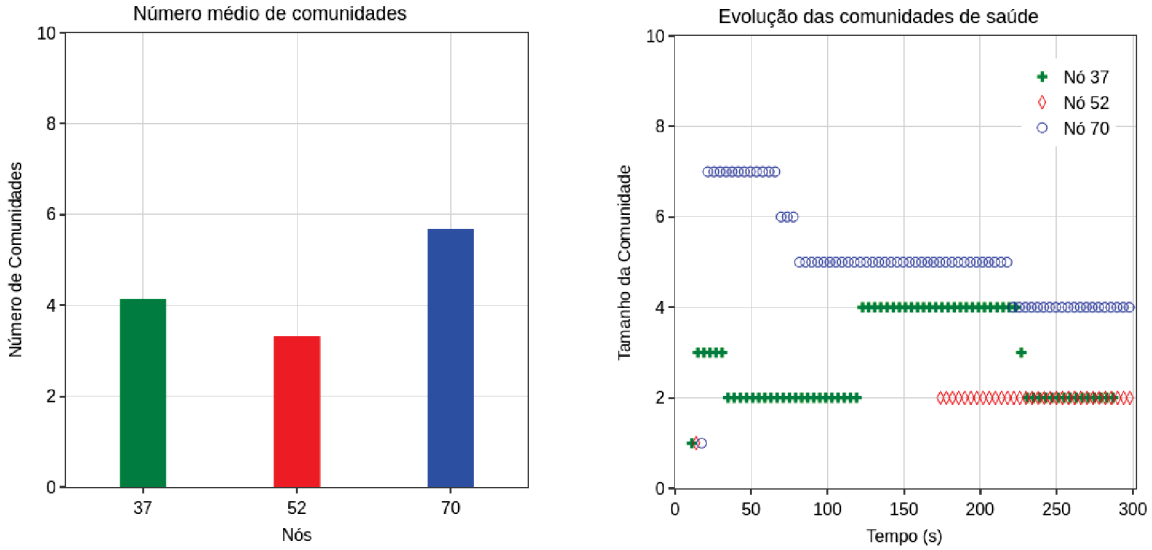


Figura 5.4: Disponibilidade de comunidades de saúde ao longo do tempo
Cenário 1 - Evento crítico aos 300s da simulação

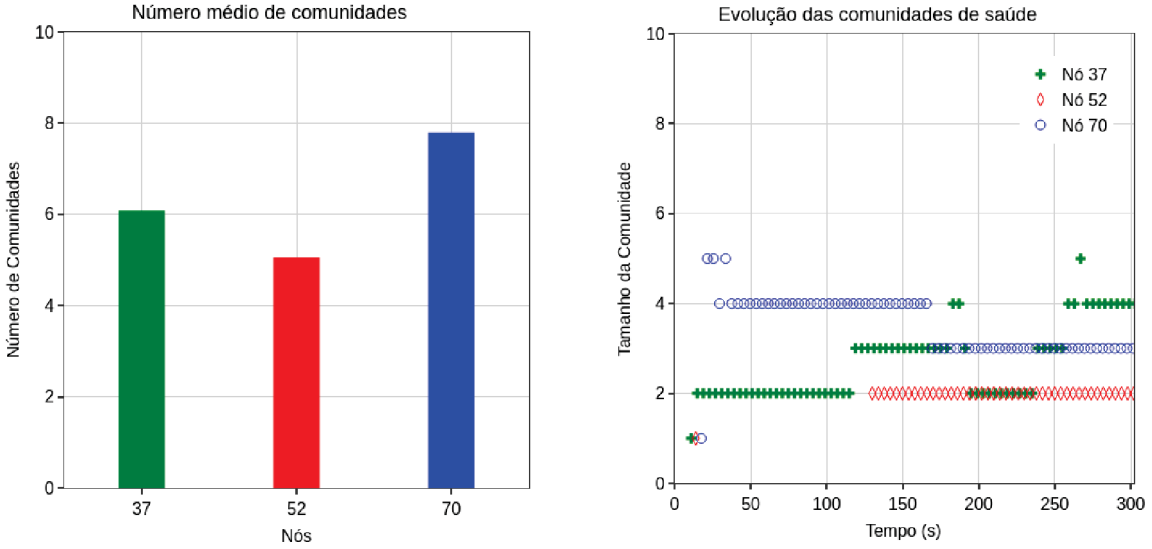


Figura 5.5: Disponibilidade de comunidades de saúde ao longo do tempo
Cenário 2 - Evento crítico aos 300s da simulação

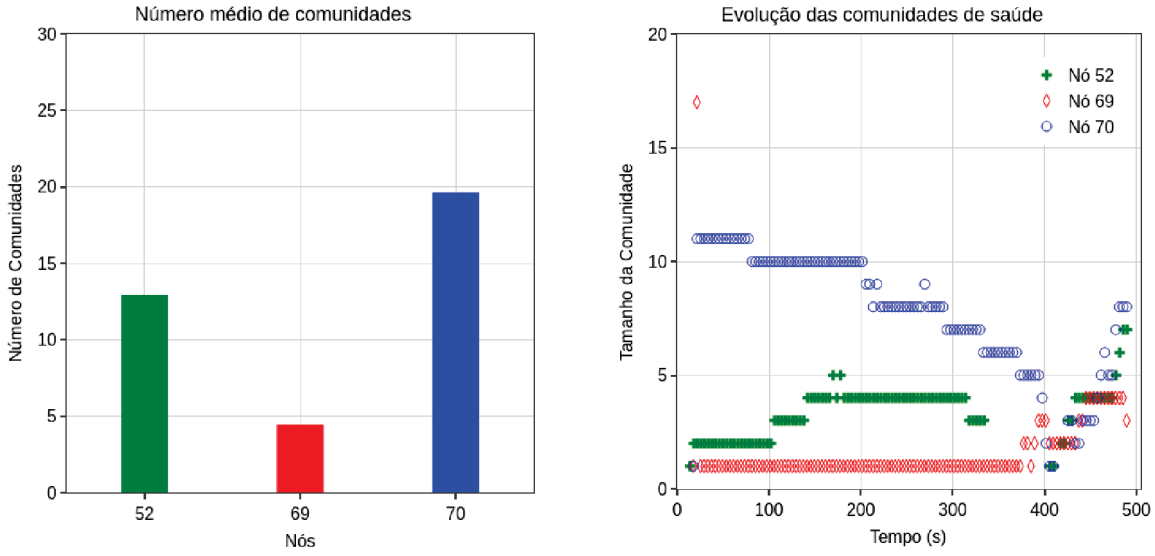


Figura 5.6: Disponibilidade de comunidades de saúde ao longo do tempo
Cenário 3 - Evento crítico aos 485s da simulação

As comunidades de saúde apresentam um comportamento com menor amplitude em seu tamanho, se comparado às vizinhanças. Isso ocorre por contemplarem somente aqueles vizinhos que possuem interesse em saúde. O tamanho das comunidades sempre será menor ou igual ao tamanho da vizinhança num mesmo instante de tempo, que é o comportamento esperado, vistos os atributos apresentados na Tabela 5.3. No mundo real, a possibilidade de haver vizinhos ao redor de uma pessoa que sejam profissionais de saúde é baixa, como demonstra a Tabela 5.1. As comunidades de interesse contemplam o próprio nó ao redor do qual foram estabelecidas e os seus respectivos vizinhos que possuem interesse em saúde e outros interesses em comum. O nó 69 esteve em uma condição crítica no cenário 3, como exibido na Figura 5.6(b), pois formou sua primeira comunidade de saúde apenas aos 393s após iniciada a simulação. Ele não teria condições de disseminar seus dados sensíveis a outros nós até esse instante.

5.4.3 Confiabilidade

A análise da confiabilidade verifica a capacidade do sistema em disseminar com sucesso e de maneira controlada os dados sensíveis das pessoas em situação emergencial. O comportamento dos nós selecionados - 37, 52, 69 e 70 - demonstra essa situação, conforme o cenário avaliado, que encontra-se demonstrada na Tabela 5.5. No cenário 1, o nó 70 foi bem-sucedido (TS) em 100% das situações emergenciais ao longo das simulações, quando seus dados disseminados foram acessados com sucesso. Os demais nós, 37 e 52, também foram bem-sucedidos, tendo sucesso em em mais de 94% das situações emergenciais. No cenário 2, que demanda a confirmação do acesso aos dados, o nó 70 foi bem-sucedido em 85,71% das situações emergenciais. Todos os nós do cenário 3 foram 100% bem-sucedidos na disseminação de seus dados. Contudo, esse resultado é o esperado, visto que o momento em que os nós entraram em situação emergencial foi selecionado previamente para garantir esse resultado. O agrupamento dos nós em comunidades de interesse impacta diretamente na TS, pois garante a disseminação dos dados sensíveis de um nó em situação emergencial apenas a um outro nó dentre aqueles que pertençam à sua comunidade de interesse em saúde. A importância do emprego das CoI para controlar a disseminação dos dados sensíveis dos nós é constatada pelos dados não acessados (TNa). No cenário 2, em 25,71% das situações emergenciais, os dados sensíveis do nó 37 não foram acessados por outros nós.

Isso ocorreu devido à falta de uma comunidade de saúde durante as situações emergenciais ou a sua conexão com os outros nós foi interrompida por conta da sua mobilidade.

Tabela 5.5: Disseminação dos dados

Cenário		**UM**		**DOIS**		**TRÊS**	
Métrica		$TS(\%)$	$TN_a(\%)$	$TS(\%)$	$TN_a(\%)$	$TS(\%)$	$TN_a(\%)$
Nó	37	97,14	2,86	74,29	**25,71**	-	-
	52	94,29	5,71	77,14	22,86	**100**	0
	69	-	-	-	-	**100**	0
	70	**100**	0	85,71	14,29	**100**	0

O tempo médio de acesso aos dados sensíveis (MTA) representa o custo em relação ao tempo para que os dados sensíveis disseminados por um nó em situação emergencial sejam acessados. Ele é impactado diretamente pela dinamicidade das redes locais estabelecidas, cuja topologia se modifica com a mobilidade dos nós. A Tabela 5.6 sumariza os resultados obtidos, onde é possível constatar que eles atendem em sua maioria à latência máxima de 125ms estabelecida pela IEEE para entrega de alertas médicos Association et al. (2012). Enquanto nos cenários 1 e 2, os dados sensíveis do nó 37 foram acessados imediatamente ($MTA = 0$), no cenário 2, os do nó 70 foram acessados, em média, após 170ms de sua disseminação. Nas demais situações, os dados foram acessados no máximo 27ms após sua disseminação. O emprego das comunidades de interesse contribui para o processo de tomada decisão de verificação do nó adequado e reduz o tempo de acesso aos dados disseminados.

Tabela 5.6: Latência no acesso aos dados disseminados

Métrica		MTA (ms)		
Cenário		**UM**	**DOIS**	**TRÊS**
Nó	37	**0**	**0**	-
	52	2,5	3	**4**
	69	-	-	0
	70	17	**170**	27

Os dados sensíveis dos nós em situação emergencial foram disseminados somente aos nós pertencentes às suas comunidades de saúde e diante das competências previstas na Tabela 5.2. O emprego de interesses e competências, associados à formação de comunidades de interesse, além de possibilitar avaliar a confiança dos nós, permite controlar a disseminação dos seus dados sensíveis. Isso ocorre em uma condição *Zero-Knowledge*, visto que as comunidades de saúde são recriadas periodicamente e desconsideram interações anteriores entre os nós da rede. O sucesso no acesso aos dados por competência (TS_{Skill}) indica a prevalência das competências nas comunidades estabelecidas, como se observa na Tabela 5.7. No cenário 1, os dados foram disseminados apenas aos nós com competência em saúde. No cenário 2 essa situação modificou-se e 76,92% do total de dados disseminados foram para nós com outras competências. 50% dos dados disseminados pelo nó 52 foram acessados por nós com competência de médico. Isso indica que em 50% das situações emergenciais, o STEALTH detectou a presença de pelo menos um médico na comunidade de saúde disponível. O sucesso observado no cenário 3, 100% dos dados disseminados a nós com competência de médico, é o esperado, visto que suas competências e o momento da situação emergencial foram definidos para que isso acontecesse dessa maneira.

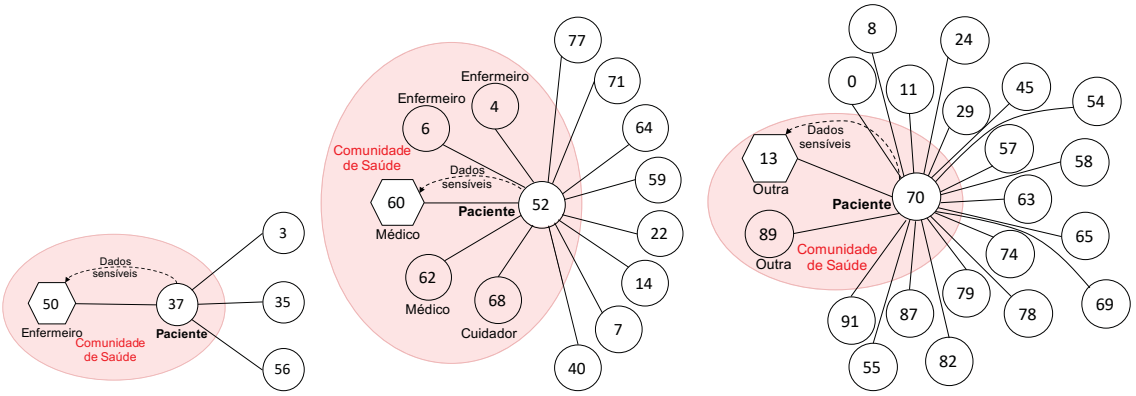
Tabela 5.7: Controle de disseminação

Métrica		Taxa de Acesso por competência (TS_{Skill}) (%)								
Cenário		**UM**			**DOIS**			**TRÊS**		
Nós		37	52	70	37	52	70	52	69	70
Competência	Médico	44,12	81,82	**91,43**	7,69	**50**	18,18	**100**	**100**	**100**
	Enfermeiro	32,35	18,18	8,57	7,69	30	13,63	0	0	0
	Cuidador	23,53	0	0	7,69	16,67	36,36	0	0	0
	Outras	0	0	0	76,92	3,33	31,81	0	0	0

O STEALTH cria redes locais dinâmicas ao longo do tempo, as quais influenciarão na disseminação dos dados sensíveis dos nós em situação emergencial. Essa dinamicidade está relacionada à mobilidade dos nós e à infraestrutura de rede, que é reconstruída ciclicamente. Portanto, inexiste um histórico de interações anteriores entre os nós, ou seja, tem-se um ambiente sem memória. Essas redes locais são estabelecidas na medida em que ocorrem os encontros entre os nós. As Figuras 5.7 a 5.10 exibem o estado das redes locais estabelecidas pelos nós avaliados e disponíveis quando entraram em situação emergencial.

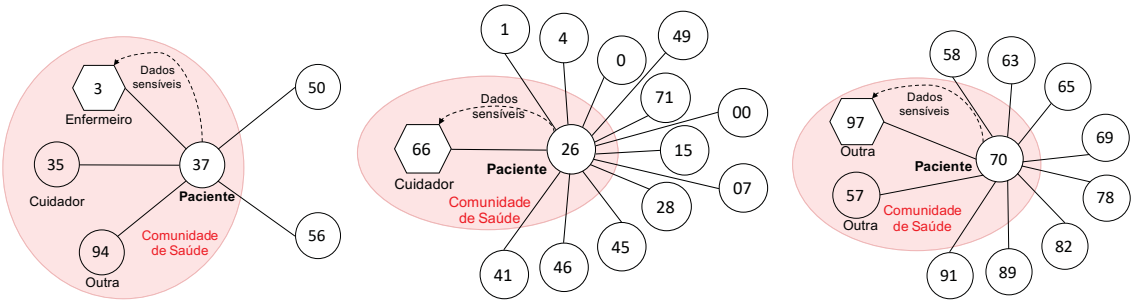
O momento da disseminação dos dados sensíveis dos nós avaliados no cenário 1 é visto na Figura 5.7. Nela observa-se os vizinhos em torno de cada nó avaliado e suas respectivas comunidades de saúde. O nó 37 possuía apenas um vizinho na sua comunidade de saúde, nó 50, que detinha a competência de Enfermeiro, como ilustra a Figura 5.7(a). Constata-se, também, o tipo de comunidade criada pelo STEALTH: sobreposta (Chakraborty et al., 2017) (Chakraborty et al., 2012) (Xie et al., 2013). O nó 37 mantém uma comunidade de saúde com o nó 50, da mesma maneira que mantém outras comunidades com os nós 3, 35 e 56. O nó 52, como ilustra a Figura 5.7(b), possuía uma quantidade maior de vizinhos, o que se refletiu na sua comunidade de saúde, que possuía membros com várias competências distintas. Observa-se dois médicos, nós 60 e 62, sendo que o nó 60 foi o nó adequado para o qual foram disseminados os dados sensíveis do nó 52. Isso se deve ao fato de que, apesar de ambos possuírem a mesma competência, seus interesses eram distintos. Como o nó 60 possuía mais interesses em comum com o nó 52 que o nó 62, isso implicou uma confiança maior no nó 60, que foi selecionado. Algo semelhante ocorreu com o nó 70, com ilFigura 5.7(c), que possuía uma quantidade de vizinhos ainda maior que os demais nós avaliados. Contudo, ainda assim sua comunidade de saúde possuía apenas dois vizinhos, nós 13 e 89, que detinham interesse em saúde, todavia não possuíam uma competência específica - *outras*. Com uma mesma competência, a tomada de decisão acerca da escolha do nó para disseminação dados sensíveis foi decidida em função da quantidade de interesses em comum que cada vizinho dessa comunidade mantinha com o nó 70. Nesse caso, o nó 13 foi escolhido.

As Figuras 5.8 a 5.10 apresentam as configurações de redes locais para os demais cenários, mas que implicaram um processo semelhante de tomada de decisão para escolha do nó para o qual seriam disseminados os dados sensíveis. O comportamento do nó 70 destaca-se pela quantidade de vizinhos que ele possuía em todos os cenários avaliados. Isso foi anteriormente observado pelo seu Número Médio de Vizinhos, N_V, pelas Figuras 5.1(a) a 5.3(a). Ele é seguido do nó 52 e dos nós 37 e 69 em menor escala. Ainda assim, observa-se, que para todos os cenários, os dados sensíveis foram disseminados de maneira controlada, ou seja, apenas às pessoas adequadas,não havendo a exposição dos dados à pessoas não autorizadas.



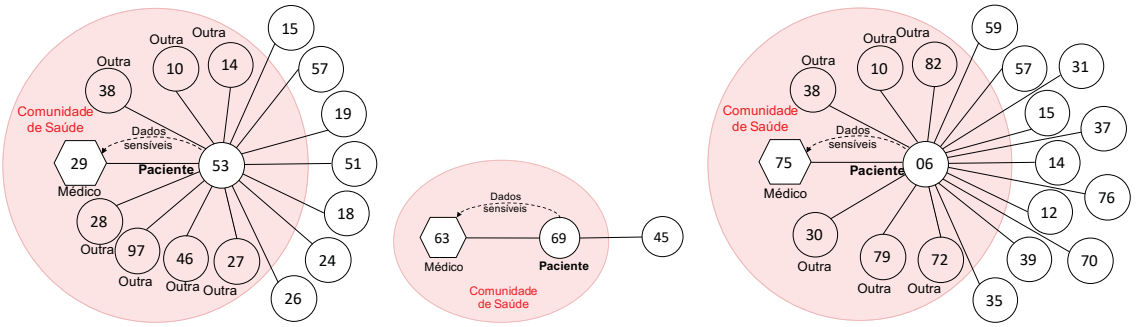
(a) (b) (c)

Figura 5.7: Comunidades de saúde dos nós 37, 52 e 70 durante situação emergencial
Cenário 1 - Evento crítico aos 300s da simulação



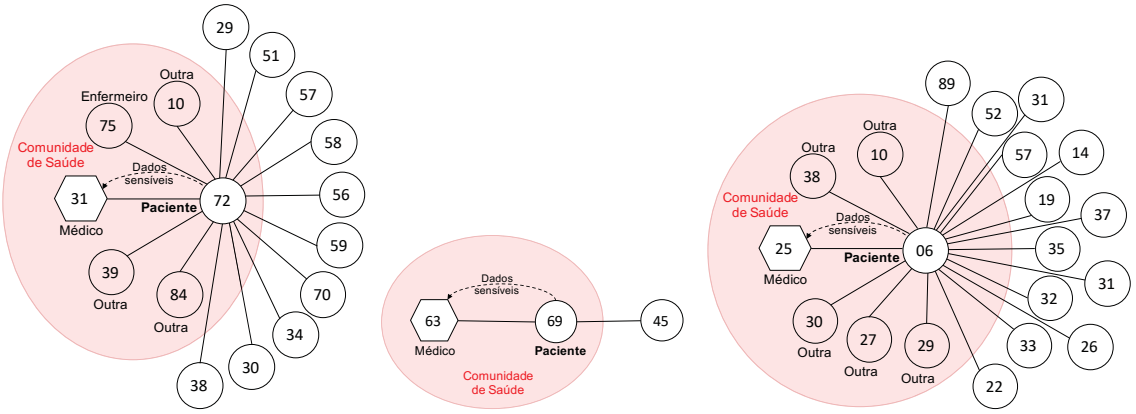
(a) (b) (c)

Figura 5.8: Comunidades de saúde dos nós 37, 52 e 70 durante situação emergencial
Cenário 2 - Evento crítico aos 300s da simulação



(a) (b) (c)

Figura 5.9: Comunidades de saúde dos nós 52, 69 e 70 durante situação emergencial
Cenário 3 - Evento crítico aos 485s da simulação - Prioridades de atendimento idênticas



(a) (b) (c)

Figura 5.10: Comunidades de saúde dos nós 52, 69 e 70 durante situação emergencial
Cenário 3 - Evento crítico aos 485s da simulação - Prioridades de atendimento distintas

5.5 DISCUSSÃO

Os resultados obtidos nas simulações realizadas demonstraram a robustez e a segurança do STEALTH, garantindo a confiabilidade do serviço de disseminação de dados sensíveis ao oferecer um serviço de maneira continuada e correta. Para isso, foram estabelecidos três cenários distintos, como descrito na Seção 5.2, sendo cada um com um objetivo distinto. Cada um desses cenários buscava retratar o comportamento do mecanismo em situações distintas. Em todas as simulações, observou-se que disseminação dos dados sensíveis dos nós em situação emergencial sempre ocorreu de maneira controlada, isto é, o STEALTH atuou para os dados fossem disseminados para pessoas adequadas. Para isso, os dados sensíveis foram disseminados a nós vizinhos com a confiança mais elevada, que pertenciam à comunidade de saúde dos nós em situação emergencial e na medida da sua competência em saúde.

Os nós avaliados entraram em situação emergencial nos cenários simulados em momentos previamente estabelecidos, como se houvesse acontecido um evento crítico e eles tivessem passado de uma condição normal de saúde para uma situação emergencial. Os cenários 1 e 2 foram simulados com os nós avaliados entrando em situação emergencial aos 300s e 890s da simulação. Esses tempos foram selecionados para representar situações específicas observadas na caracterização do modelo de mobilidade empregado (Helgason et al., 2014). Enquanto aos 300s de simulação observou-se um movimento intenso dos nós, provocando diversos encontros entre eles, aos 890s a configuração era completamente diferente. Especialmente próximo do final da simulação, 900s, o movimento dos nós era esparso, promovendo uma interação reduzida entre eles e impactando diretamente na disseminação dos dados sensíveis.

O cenário 3 teve uma configuração distinta dos demais para que os nós entrassem em situação emergencial, 485s. Esse instante foi escolhido a fim de fazer como alguns nós selecionados disseminassem seus dados a um único nó. Portanto, diante de situações emergenciais simultâneas e distintas, conforme a prioridade de atendimento requerida por cada nó, seria tomada uma decisão acerca da ordem de atendimento. Logo, todos os dados disseminados pelos nós avaliados foram acessados com sucesso, como se observa na Tabela 5.5, o que era esperado. Dada à proximidade existente entre os nós aos 485s, os tempos médios de acesso aos dados sensíveis, MTA, foram baixos, atingindo um valor máximo de 27ms para o nó 70. Esse comportamento atende aos requisitos previstos pela IEEE (Association et al., 2012), que estabelece uma latência mínima para entrega de alertas médicos de 125ms. Ao nó que acessaria

os dados dos demais, 63, foi atribuída a competência de médico. A disseminação dos dados por competência, T_{Skill}, constatados na Tabela 5.7, ocorreram como previsto antecipadamente.

A disponibilidade do serviço oferecido pelo STEALTH foi elevada nos cenários 1 e 2 simulados com o instante 300s pré-configurado. O acesso aos dados sensíveis disseminados pelos nós em situação emergencial atingiu 100% em alguns casos, como valores na Tabela 5.5. Esse resultado está intimamente associado à mobilidade dos nós avaliados. Aos 300s de simulação os nós se movimentavam como alta frequência e interagiam intensamente. À medida que a simulação se aproxima do final, a mobilidade dos nós se reduz claramente, o que aconteceu nos cenários simulados com o instante 890s pré-configurado. Os resultados obtidos demonstram situações esparsas, com poucos nós, a disseminação de dados é impactada em grande medida. Isso é constatado nos resultados sumarizados na Tabela A.1. O nó 70, por exemplo, não teve seus dados acessados durante todas as simulações realizadas para o cenário 1, $TN_a = 100\%$.

A evolução das redes locais em torno dos nós avaliados também demonstra a disponibilidade do serviço oferecido pelo STEALTH. Dentre as suas atividades, o mecanismo cria redes locais na medida em que os nós se encontram e, de forma cíclica, essas redes são descartadas, sendo estabelecidas outras novas. Com isto, a mobilidade dos nós é incorporada à topologia dessas redes, que se modifica ao longo do tempo. Essa característica é observada pelas Figuras 5.1(b) a 5.3(b), A.1(b) e A.2(b). A dinamicidade das redes locais estabelecidas fica caracterizada especialmente pelas mudanças que ocorrem na sua vizinhança.

O custo para acesso aos dados sensíveis disseminados mostrou-se muito baixo, como constatado pelo tempo médio entre o instante da sua disseminação e o instante que foram acessados, MTA. Os resultados obtidos foram relacionados nas Tabelas 5.6 e A.2. Os valores obtidos para as situações emergenciais ocorridas aos 300s são muito baixos, sendo que o pior resultado foi o do nó 70, MTA teve o valor 170ms, destacando-se dos demais. Esse valor mais elevado deve-se ao fato de que o caminho percorrido pelo nó 70 permitiu que tivesse diversas interações, possuindo vários vizinhos. Embora esse valor esteja além daquele previsto pela IEEE (Association et al., 2012), que é de 125ms, todos os demais valores obtidos ficaram bem abaixo desse limiar. Com isso, foram disseminados dados sensíveis de vários nós para ele, o que impactou no seu comportamento. Caso o nó que acessou os dados sensíveis disseminados pelo nó 70 se deslocasse na velocidade mais alta prevista, 2m/s, em 170ms ele se deslocaria menos de 1m, impactando minimamente no atendimento do nó em situação emergencial.

A mensuração da confiança dos nós é realizada na medida em que eles se encontram, quando são obtidos valores instantâneos. Somente aqueles nós que possuem interesse em saúde têm sua confiança avaliada. Diferentemente do trabalho de Bao et al. (2013), que avalia a convergência da confiança, seja entre comunidades e dentro das comunidades. O STEALTH não verifica a confiança de nós que não pertençam às comunidades de saúde. Além disso, por atuar em uma situação *Zero-Knowledge*, os valores de confiança obtidos pelo STEALTH não convergem ao longo do tempo. Os valores obtidos são instantâneos e representam as características do nó no momento da avaliação, visto que não são empregadas informações anteriores ao encontro dos nós oriundas de reputação e recomendações.

5.6 RESUMO

Este capítulo apresentou a metodologia de avaliação e verificação dos resultados apresentados pelo mecanismo STEALTH, a fim de mensurar sua eficiência e eficácia em garantir a segurança na disseminação de dados sensíveis em situações emergenciais. Os resultados obtidos diante de métricas definidas demonstram a robustez e segurança do mecanismo STEALTH, que garante a disponibilidade e a confiabilidade do serviço de disseminação dos dados sensíveis,

prestado corretamente e de maneira contínua. O impacto do uso de comunidades de interesse e da confiança social para controlar a disseminação dos dados foi verificado. Os cenários foram avaliados, de modo que o mecanismo pudesse representar situações reais de um ambiente urbano. Além disso, foram discutidos os resultados apresentados. O STEALTH mostrou-se robusto e eficaz para garantir a disseminação segura de dados sensíveis em situações emergenciais.

6 CONCLUSÕES

A expansão do uso da Internet entre as pessoas tem levado à disponibilização cada vez maior de serviços online. A área de saúde também se insere nesse movimento e, através de serviços de saúde em redes (*e-health*), destacam-se aqueles serviços orientados ao atendimento de situações emergenciais. Esses serviços possibilitam que profissionais de saúde acessem de maneira ubíqua às informações dos pacientes, independentemente de sua localização. Contudo, fora dos ambientes hospitalares surgem diversos desafios, como, por exemplo, prover os dados das pessoas com segurança para que recebam atendimento eficiente e eficaz. Os ambientes urbanos e esparsos podem não dispor de infraestrutura para tal, inclusive de redes. Além disso, suas características, especialmente a mobilidade dos dispositivos, podem inviabilizar a criação e manutenção de históricos de interações, caracterizando-se como ambientes sem memória.

A literatura apresenta diversas abordagens com o objetivo de garantir a segurança dos dados em ambientes de redes estruturados e com pouca ou nenhuma mobilidade dos nós. Todavia, ambientes não estruturados demandam soluções que levem em conta a dinamicidade da rede ao longo do tempo, sua escalabilidade, além de incorporar mecanismos de controle de disseminação dos dados que se valham de informações disponíveis no momento das interações. Essas soluções devem ser distintas das tradicionais, particularmente por conta desses ambientes possuírem um condição *Zero-Knowledge* (Feige et al., 1988) em relação às interações entre as pessoas. Dessa forma, os aspectos sociais das pessoas e de suas relações são candidatos promissores, diante da presença intensa das redes sociais na vida das pessoas atualmente. Esses aspectos possibilitam a mensuração da confiança das pessoas, que posteriormente é usada em apoio às tomadas de decisão para controlar a disseminação dos dados disponíveis às pessoas adequadas.

O mecanismo STEALTH (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control*) foi proposto com o objetivo de permitir o atendimento emergencial de uma pessoa que, diante de um evento crítico, não se encontra nas suas condições normais de saúde, atuando de maneira complementar às estruturas hospitalares. Para isso, agrupa os dispositivos de rede em comunidades de interesse, cujo critério de formação são os interesses que as pessoas mantêm. Ele aplica aspectos sociais das pessoas e de suas relações - interesses e competências - para medir sua confiança quando pertencerem à uma comunidade de saúde. Quando um nó da rede entra em situação emergencial, ele verifica os nós que pertencem à sua comunidade de saúde em busca do nó com a confiança mais elevada. Os dados sensíveis são disseminados ao nó selecionado.

A avaliação do STEALTH foi conduzida no simulador de rede NS-3, considerando um ambiente urbano e um modelo de mobilidade realístico. O desempenho do mecanismo verificou sua robustez (do inglês, *dependability*) e sua segurança (do inglês, *safety*), na disseminação dos dados sensíveis. O STEALTH obteve taxa de sucesso no acesso aos dados sensíveis disseminados pelos nós em situação emergencial de 100% em alguns casos. A disponibilidade do serviço atingiu 100% em algumas situações, indicando que os nós em situação emergencial sempre tiveram um nó próximo para auxiliá-lo. Nos momentos como o previsto para situações dessa natureza. Além disso, o mecanismo permitiu que os dados disseminados fossem acessados em intervalos de tempo reduzidos, geralmente abaixo de 170ms, e apenas pelos nós capacitados, comprovando a conveniência do emprego das comunidades de interesse e de aspectos sociais em ambientes não estruturados e dinâmicos. Em geral, os dados foram acessados com uma latência inferior ao previsto pela IEEE, que é de 125ms (Association et al., 2012).

Conclui-se que garantir uma disseminação segura de dados sensíveis em ambientes dinâmicos e não estruturados, a fim de apoiar as tomadas de decisão diante de situações

emergenciais de saúde, é possível. Esse objetivo foi alcançado pelo STEALTH, visto que ele controla a disseminação dos dados sensíveis das pessoas em situação emergencial, de maneira que apenas aquelas pessoas que atendam a determinados critérios possam recebê-los. Esse controle ocorreu na perspectiva de que os dados foram disseminados apenas às pessoas capacitadas, ou seja, as pessoas receberam os dados na medida de sua competência em saúde. O STEALTH se mostrou robusto ao oferecer um serviço com alta disponibilidade, funcionando continuamente de maneira correta e seguro ao longo de todas as simulações, disseminando dados sensíveis de forma controlada, apenas às pessoas adequadas e na medida de sua competência em saúde. Com isto, este trabalho contribuiu com um detalhamento do uso da confiança em ambientes não estruturados e com uma solução para apoiar a disseminação de dados sensíveis de pessoas em situação emergencial, em complemento aos serviços prestados nos ambientes hospitalares.

6.1 TRABALHOS FUTUROS

Embora o foco desse trabalho seja possibilitar que pessoas - pedestres - auxiliem outras pessoas próximas em situação emergencial nos momentos que precedem um atendimento médico, ele pode ser estendido em várias direções, possibilitando uma variada gama de trabalhos futuros. A robustez do mecanismo, através dos seus atributos de confiabilidade e a disponibilidade, é passível de aperfeiçoamento, possibilitando que ele ofereça um serviço ainda mais robusto aos usuários. Adicionalmente, os dados disseminados pelo mecanismo devem ter sua segurança assegurada frente à possíveis ameaças ao seu correto funcionamento. Finalmente, a solução proposta não tem seu uso limitado aos dados de saúde, podendo ser adaptada para outros domínios de aplicação. Nos tópicos a seguir são detalhados as possíveis direções para trabalhos futuros.

6.1.1 Ampliação da disponibilidade e confiabilidade

A robustez do STEALTH é impactada pelas mudanças nas dimensões temporais e espaciais nos ambientes onde é empregado. A mobilidade das pessoas - pedestres - influencia diretamente na sua vizinhança e na formação das comunidades de interesse. Dessa forma, a topologia das redes locais estabelecidas é dinâmica e evolui ao longo do tempo. Pessoas que se deslocam no ambiente urbano em veículos também podem estabelecer comunidades e auxiliar outras pessoas. Redes heterogêneas seriam estabelecidas, possibilitando um melhor aproveitamento dos recursos disponíveis (Melo et al., 2013). Nesses casos, a inclusão de nós em maior velocidade viabiliza atendimentos mais rápidos das pessoas em situação emergencial, visto que eleva a quantidade de conexões de rede e melhora a comunicação fim-a-fim (Melo et al., 2014), aumentando a disponibilidade do serviço oferecido. Por outro lado, comparando-se as velocidades dos pedestres com as dos veículos, surgem novos desafios, particularmente em relação à dimensão temporal.

O controle de disseminação dos dados realizado pelo mecanismo leva em conta aspectos sociais das pessoas e de suas relações - competência e similaridade - para incorporar o seu comportamento às tomadas de decisões quanto à disseminação dos dados sensíveis. Porém, diversos aspectos sociais são apresentados na literatura (Cho et al., 2015) e são passíveis de incorporação ao mecanismo mediante avaliação. Ampliar a quantidade de aspectos sociais empregados torna o processo de tomada de decisão mais robusto e expande as possibilidades de emprego do mecanismo, ampliando a confiabilidade do serviço.

O mecanismo considera que somente pacientes entrem em situação emergencial, o que acontece de forma indistinta no mundo real. A realidade impõe que qualquer pessoa pode ter sua condição de saúde alterada em algum momento, inclusive aquelas pessoas que detém

competência em saúde. Dessa forma, os processos de tomada de decisão podem ser aprimorados para que qualquer pessoa entre em situação de emergencial, garantindo maior confiabilidade ao serviço oferecido. Essas alterações impactam na forma de atendimento, que deverá levar em conta eventos simultâneos e buscar alternativas ao longo do tempo.

6.1.2 Integração de mecanismos de privacidade

O comportamento do STEALTH demonstrou sua robustez e a segurança do ponto de vista de (*safety*). Porém, ameaças do ponto de vista de *security* existem e devem ser consideradas no funcionamento do mecanismo, especialmente diante da infraestrutura de rede que o mecanismo provê. Nessas redes dinâmicas, os dados sensíveis dos pacientes são disseminados pelo STEALTH em texto puro e, na presença de um atacante, ficam vulneráveis. Assim, ao serem acessados sem autorização, comprometem a privacidade da pessoa em situação emergencial. A encriptação de dados é uma alternativa que pode ser avaliada, especialmente por auxiliar na garantia da privacidade das pessoas envolvidas. Porém, ela demanda recursos de processamento e memória dos dispositivos envolvidos na troca de dados.

A verificação da identidade dos nós da rede não é realizada, mas seus aspectos sociais, que são a base do controle da disseminação dos dados sensíveis. Logo, um nó pode se passar por vários vizinhos simultaneamente, caracterizando um ataque *Sybil*, também conhecido como ataque de personificação. Nesse tipo de ataque identidades são furtadas ou falsificadas (Evangelista et al., 2016a,b) (Bannack et al., 2008). Assim, um atacante torna-se usuário autêntico do mecanismo e pode receber dados sensíveis disseminados por outros nós, comprometendo sua privacidade. Adicionalmente, esses nós podem empreender ataques de autopromoção (do inglês, *self-promoting* (Bao et al., 2013)), manipulando seus aspectos sociais. Assim, ele influenciará no cômputo do seu indicador de confiança e poderá ser selecionado para receber dados de outros nós em situação emergencial. Dessa forma, o gerenciamento dos usuários e seus dispositivos deve ser aprimorado, o que pode acontecer, por exemplo, através de sistemas de gerenciamento de identidades (do inglês, *Identity Management*) (Macedo et al., 2016).

6.1.3 Extensão da Aplicação e Uso em Outros Contextos de Serviços

O foco do mecanismo é controlar a disseminação de dados, o que ocorre em diversas áreas distintas de saúde. Logo, pode ser estendido para uso em outros contextos. Na área de segurança pública, por exemplo, o STEALTH pode ampliar seu alcance, agilizando a divulgação de ocorrências e atendendo melhor a população. Nesse caso, pessoas em situação de risco ou próximas de algum evento dessa natureza podem informar algum agente de segurança próximo acerca do problema em curso. Conforme a situação e a competência dos agentes que se encontrem próximos geograficamente, aqueles com maior competência poderão atuar em apoio à resolução do problema. Adicionalmente, aspectos sociais mais específicos e voltados para essa área podem ser verificados e avaliados para uso nos processos de tomadas de decisões.

Uma outra área onde o mecanismo pode vir a ser empregado é no suporte ao gerenciamento de tráfego urbano. Quando os dispositivos de sinalização e controle de tráfego como câmeras, sensores e sinais de trânsito encontram-se defeituosos, caracterizam uma situação emergencial. Além disso, os aspectos sociais dos engenheiros e técnicos que estejam próximos são avaliados. Dessa forma, sua competência técnica seria avaliada para que contribuíssem para a solução dos problemas em equipamentos eletrônicos. Aquele profissional com maior competência nas proximidades do equipamento em pane seria notificado sobre a situação e adotaria alguma providência imediata.

REFERÊNCIAS

Abomhara, M. e Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. Em *PRISMS Privacy and Security in Mobile Systems*, páginas 1–8. IEEE.

Aksoy, D., Altinel, M., Bose, R., Cetintemel, U., Franklin, M., Wang, J. e Zdonik, S. (1998). Research in data broadcast and dissemination. Em *International Conference on Advanced Multimedia Content Processing*, páginas 194–207. Springer.

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

Arış, A., Oktuğ, S. F. e Voigt, T. (2018). Security of Internet of Things for a Reliable Internet of Services. Em *Autonomous Control for a Reliable Internet of Services*, páginas 337–370. Springer.

Association, I. S. et al. (2012). 802.15. 6-2012 IEEE Standards for Local and Metropolitan Area Networks–Part 15.6: Wireless Body Area Networks.

Atzori, L., Iera, A. e Morabito, G. (2010). The Internet of Things: A survey. *Computer networks*, 54(15):2787–2805.

Avizienis, A., Laprie, J.-C., Randell, B. e Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33.

B, V. R. e Sudhindra, K. R. (2014). Survey of trust models in wireless sensor networks. *International Journal of Advanced Information Science and Technology*, 31(31).

Balcan, M. F. e Liang, Y. (2013). Modeling and detecting community hierarchies. Em *International Workshop on Similarity-Based Pattern Recognition*, páginas 160–175. Springer.

Bandyopadhyay, D. e Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69.

Bannack, A., da Silva, E., Lima, M. N., dos Santos, A. L. e Albini, L. C. P. (2008). Segurança em redes ad hoc. *SBRT Simpósio Brasileiro de Telecomunicaçoes*, páginas 19–20.

Bao, F. e Chen, I.-R. (2012a). Dynamic trust management for Internet of Things applications. Em *International workshop on Self-aware Internet of Things*, páginas 1–6.

Bao, F. e Chen, R. (2012b). Trust management for the Internet of Things and its application to service composition. Em *World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, páginas 1–6.

Bao, F., Chen, R. e Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. Em *ISADS Autonomous Decentralized Systems*, páginas 1–7. IEEE.

Bernabe, J. B., Ramos, J. L. H. e Gomez, A. F. S. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Computing*, 20(5):1763–1779.

Bujari, A. (2012). A survey of opportunistic data gathering and dissemination techniques. Em *21st International Conference on Computer Communications and Networks (ICCCN)*, páginas 1–6. IEEE.

Carminati, B., Ferrari, E. e Guglielmi, M. (2013). Controlled information sharing for unspecified emergencies. Em *Risks and Security of Internet and Systems (CRiSIS)*, páginas 1–8. IEEE.

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

Carrero, M. A., da Silva, R. I., dos Santos, A. L. e Hara, C. S. (2015). An autonomic in-network query processing for urban sensor networks. Em *2015 IEEE Symposium on Computers and Communication (ISCC)*, páginas 968–973. IEEE.

Cavallari, R., Martelli, F., Rosini, R., Buratti, C. e Verdone, R. (2014). A survey on wireless body area networks: Technologies and design challenges. *IEEE Communications Surveys & Tutorials*, 16(3):1635–1657.

Cervantes, C., Nogueira, M. e Santos, A. (2018). Mitigação de ataques no roteamento em iot densa e móvel baseada em agrupamento e confiabilidade dos dispositivos. Em *Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. SBC.

Cervantes, C., Poplade, D., Nogueira, M. e Santos, A. (2015). Detection of sinkhole attacks for supporting secure routing on 6lowpan for Internet of Things. Em *IM Integrated Network Management*, páginas 606–611. IEEE.

Chakraborty, A., Ghosh, S. e Ganguly, N. (2012). Detecting overlapping communities in folksonomies. Em *Proceedings of the 23rd ACM conference on Hypertext and social media*, páginas 213–218. ACM.

Chakraborty, T., Dalmia, A., Mukherjee, A. e Ganguly, N. (2017). Metrics for community analysis: A survey. *ACM Computing Surveys (CSUR)*, 50(4):54.

Chau, D. H., Pandit, S. e Faloutsos, C. (2006). Detecting fraudulent personalities in networks of online auctioneers. Em *European Conference on Principles of Data Mining and Knowledge Discovery*, páginas 103–114. Springer.

Cho, J.-H., Chan, K. e Adali, S. (2015). A survey on trust modeling. *ACM Computing Surveys (CSUR)*, 48(2):28.

Cole, I., Sibamba, L., Hilowle, A. e Jallow, J. (2017). It risk assessment for group6 healthcare clinic report. *arXiv preprint arXiv:1712.04560*.

Consortium, N.-. (2018). NS-3 A Discrete-Event Network Simulator for Internet Systems. https://www.nsnam.org. [Online]. Acesso em: Maio 2018.

Conti, M., Dehghantanha, A., Franke, K. e Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.

Coscia, M., Giannotti, F. e Pedreschi, D. (2011). A classification for community discovery methods in complex networks. *Statistical Analysis and Data Mining*, 4(5):512–546.

Damiani, M. L., Bertino, E., Catania, B. e Perlasca, P. (2007). GEO-RBAC: a spatially aware RBAC. *Transactions on Information and System Security (TISSEC)*, 10(1):2.

de Enfermagem, C. F. (2019). Enfermagem em Números. http://www.cofen.gov.br/enfermagem-em-numeros. [Online]. Acesso em: Jan. 2019.

de Geografia e Estatística, I. B. (2019). Projeção da população do Brasil e das Unidades da Federação. https://www.ibge.gov.br/apps/populacao/projecao//index.html. [Online]. Acesso em: Jan. 2019.

de Medicina, C. F. (2019). Estatística. http://portal.cfm.org.br/?option=com_estatistica. [Online]. Acesso em: Jan. 2019.

Draghici, A. e Steen, M. V. (2018). A survey of techniques for automatically sensing the behavior of a crowd. *ACM Computing Surveys (CSUR)*, 51(1):21.

Duarte, E. e dos Santos, A. L. (2001). Semi-active replication of snmp objects in agent groups applied for fault management. Em *IEEE/IFIP International Symposium on Integrated Network Management*, páginas 565–578. IEEE.

Ericsson (2018). Internet of Things forecast. https://www.ericsson.com/en/mobility-report/internet-of-things-forecast. [Online]. Acesso em: Maio 2018.

Evangelista, D., da Silva, E., Nogueira, M. e Santos, A. (2016a). Um controle de associações resistente a ataques Sybil para a disseminação segura de conteúdo da IoT. Em *Anais do XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*. SBC.

Evangelista, D., Mezghani, F., Nogueira, M. e Santos, A. (2016b). Evaluation of Sybil attack detection approaches in the Internet of Things content dissemination. Em *2016 Wireless Days (WD)*, páginas 1–6. IEEE.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N. e Mankodiya, K. (2017). Towards fog-driven IoT ehealth: promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*.

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

Ferreira, J. L. M. (2013). Segurança em redes sem fio. Dissertação de Mestrado, Universidade Tecnológica Federal do Paraná, Curitiba - Brasil.

Figueiredo, C. M., dos Santos, A. L., Loureiro, A. A. e Nogueira, J. M. (2005). Policy-based adaptive routing in autonomous WSNs. Em *International Workshop on Distributed Systems: Operations and Management*, páginas 206–219. Springer.

Fortunato, S. (2010). Community detection in graphs. *Physics reports*, 486(3-5):75–174.

Foundation, T. R. (2018). The R Project for Statistical Computing. https://www.r-project.org/. [Online]. Acesso em: Nov. 2018.

Fukuzaki, Y., Mochizuki, M., Murao, K. e Nishio, N. (2014). A pedestrian flow analysis system using wi-fi packet sensors to a real environment. Em *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, páginas 721–730. ACM.

Fukuzaki, Y., Mochizuki, M., Murao, K. e Nishio, N. (2015). Statistical analysis of actual number of pedestrians for wi-fi packet-based pedestrian flow sensing. Em *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*, páginas 1519–1526. ACM.

Furlaneto, S. S., Dos Santos, A. L. e Hara, C. S. (2012). An efficient data acquisition model for urban sensor networks. Em *2012 IEEE Network Operations and Management Symposium*, páginas 113–120. IEEE.

Gambetta, D. et al. (2000). Can we trust trust? *Trust: Making and breaking cooperative relations*, 13:213–237.

Garyfalos, A. e Almeroth, K. C. (2008). Coupons: A multilevel incentive scheme for information dissemination in mobile networks. *IEEE Transactions on Mobile Computing*, 7(6):792–804.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M. e Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials*, 19(4):2456–2501.

Gielow, F., Jakllari, G., Nogueira, M. e Santos, A. (2015). Data similarity aware dynamic node clustering in wireless sensor networks. *Ad Hoc Networks*, 24:29–45.

Gligor, V. e Wing, J. M. (2011). Towards a theory of trust in networks of humans and computers. Em *International workshop on Security Protocols*, páginas 223–242. Springer.

Golbeck, J. (2009). Introduction to computing with social trust. Em *Computing with social trust*, páginas 1–5. Springer.

Guo, J. e Chen, R. (2015). A classification of trust computation models for service-orientedInternet of Things systems. Em *Services Computing (SCC)*, páginas 324–331. IEEE.

Guo, J., Chen, R. e Tsai, J. J. (2017). A survey of trust computation models for service management in Internet of Things systems. *Computer Communications*, 97:1–14.

Gwak, B., Son, H., Kang, J. e Lee, D. (2017). IoT trust estimation in an unknown place using the opinions of I-Sharing friends. Em *Trustcom/BigDataSE/ICESS*, páginas 602–609. IEEE.

Hansen, F. e Oleshchuk, V. (2003). Spatial role-based access control model for wireless networks. Em *Vehicular Technology Conference*, volume 3, páginas 2093–2097. IEEE.

Health Organization, W. (2015). Cardiovascular diseases (CVDs). http://www.who.int/mediacentre/factsheets/fs317/en/. [Online]. Acesso em: Mar. 2019.

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

INFSO, D. (2008). Networked enterprise & RFID infso g. 2 micro & nanosystems in cooperation with the working group RFID of the etp eposs,"Internet of Things in 2020: Roadmap for the future".

Innovation, E. (2016). Saensuk Smart City launches smart healthcare pilot. https://www.enterpriseinnovation.net/article/saensuk-smart-city-launches-smart-healthcare-pilot-1759874204. [Online]. Acesso em: Abr. 2019.

Kalogianni, E., Sileryte, R., Lam, M., Zhou, K., Van der Ham, M., Van der Spek, S. e Verbree, E. (2015). Passive wifi monitoring of the rhythm of the campus. Em *Proceedings of The 18th AGILE International Conference on Geographic Information Science*, páginas 1–4.

Khaliq, K. A., Chughtai, O., Qayyum, A. e Pannek, J. (2017). An emergency alert system for elderly/special people using vanet and wban. Em *Emerging Technologies (ICET), 2017 13th International Conference on*, páginas 1–6. IEEE.

Kim, S.-M. e Hovy, E. (2006). Automatic identification of pro and con reasons in online reviews. Em *Proceedings of the COLING/ACL on Main conference poster sessions*, páginas 483–490. Association for Computational Linguistics.

Kjærgaard, M. B., Wirz, M., Roggen, D. e Tröster, G. (2012). Detecting pedestrian flocks by fusion of multi-modal sensors in mobile phones. Em *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, páginas 240–249. ACM.

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

Labs, A. I. (2018). About us. https://autoidlabs.org/. [Online]. Acesso em: Maio 2018.

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

Latré, B., Braem, B., Moerman, I., Blondia, C. e Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks*, 17(1):1–18.

l'est Republicain (2018). Les pompiers recrutent des Bons Samaritains. https://www.estrepublicain.fr/edition-de-vesoul-haute-saone/2018/02/04/les-pompiers-recrutent-des-bons-samaritains. [Online]. Acesso em: Abr. 2018.

Li, S., Da Xu, L. e Zhao, S. (2015). The Internet of Things: a survey. *Information Systems Frontiers*, 17(2):243–259.

Li, S., Oikonomou, G., Tryfonas, T., Chen, T. M. e Da Xu, L. (2014). A distributed consensus algorithm for decision making in service-oriented Internet of Things. *Transactions on Industrial Informatics*, 10(2):1461–1468.

Lima, M. N., dos Santos, A. L. e Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 11(1):66–77.

Lin, G., Bie, Y. e Lei, M. (2013). Trust based access control policy in multi-domain of cloud computing. *JCP*, 8(5):1357–1365.

Macedo, R., Santos, A., Ghamri-Doudane, Y. e Nogueira, M. (2016). A scheme for DDoS attacks mitigation in IdM systems through reorganizations. Em *15th IEEE/IFIP Network Operations and Management Symposium (NOMS)*, páginas 298–305. IEEE.

Mahalle, P. N., Thakre, P. A., Prasad, N. R. e Prasad, R. (2013). A fuzzy approach to trust based access control in Internet of Things. Em *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, páginas 1–5. IEEE.

Mannes, E., Nogueira, M. e Santos, A. (2012a). A bio-inspired scheme on quorum systems for reliable services data management in MANETs. Em *2012 IEEE Network Operations and Management Symposium*, páginas 278–285. IEEE.

Mannes, E., Nogueira, M. e Santos, A. (2012b). Reliable operational services in MANETs by misbehavior-tolerant quorum systems. Em *Proceedings of the 8th International Conference on Network and Service Management*, páginas 343–349. International Federation for Information Processing.

Marsh, S. e Briggs, P. (2009). Examining trust, forgiveness and regret as computational concepts. Em *Computing with social trust*, páginas 9–43. Springer.

Marsh, S. P. (1994). *Formalising trust as a computational concept*. Tese de doutorado, University of Stirling, Stirling - UK. http://hdl.handle.net/1893/2010.

Melo, R., Nogueira, M. e Santos, A. (2014). Sistema indicador de resiliência na conectividade de redes heterogêneas sem fio. *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (XV SBSeg)*, páginas 139–152.

Melo, R., Santos, A., Nogueira, M. e Mehdi, D. (2013). Modelagem e projeto de redes sem fio heterogêneas resilientes e sobreviventes. *Minicursos do XXXI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos (SBRC)*, páginas 1–50.

Mohammad, S. M. e Hirst, G. (2012). Distributional measures of semantic distance: A survey. *arXiv preprint arXiv:1203.1858*.

Mosenia, A. (2017). Addressing Security and Privacy Challenges in Internet of Things. *CoRR*, abs/1807.06724.

Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D. e Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications surveys & tutorials*, 16(3):1658–1686.

Nguyen, T., Hoang, D. e Seneviratne, A. (2016). Challenge-response trust assessment model for personal space IoT. Em *PerCom Workshops Pervasive Computing and Communication Workshops*, páginas 1–6. IEEE.

Oh, H.-K., Kim, J.-W., Kim, S.-W. e Lee, K. (2018). A unified framework of trust prediction based on message passing. *Cluster Computing*, páginas 1–13.

Ouaddah, A., Mousannif, H., Elkalam, A. A. e Ouahman, A. A. (2017). Access control in the Internet of Things: big challenges and new opportunities. *Computer Networks*, 112:237–262.

Park, J. e Sandhu, R. (2002). Towards usage control models: beyond traditional access control. Em *Symposium on Access control models and technologies*, páginas 57–64. ACM.

Park, J. e Sandhu, R. (2004). The UCON ABC usage control model. *Transactions on Information and System Security (TISSEC)*, 7(1):128–174.

population.city (2015). Stockholm · population. [Online]. Acesso em: Dez. 2018.

Rachuri, K. K., Efstratiou, C., Leontiadis, I., Mascolo, C. e Rentfrow, P. J. (2013). Metis: Exploring mobile phone sensing offloading for efficiently supporting social sensing applications. Em *2013 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, páginas 85–93. IEEE.

Reichardt, J. e Bornholdt, S. (2004). Detecting fuzzy community structures in complex networks with a potts model. *Physical Review Letters*, 93(21):218701.

Roman, R., Najera, P. e Lopez, J. (2011). Securing the Internet of Things. *Computer*, 44(9):51–58.

Rossetti, G. e Cazabet, R. (2018). Community discovery in dynamic networks: a survey. *ACM Computing Surveys (CSUR)*, 51(2):35.

RStudio (2018). RStudio - Open Source and enterprise-ready professional software for R. https://www.rstudio.com/. [Online]. Acesso em: Nov. 2018.

Ruiz-Ruiz, A. J., Blunck, H., Prentow, T. S., Stisen, A. e Kjærgaard, M. B. (2014). Analysis methods for extracting knowledge from large-scale wifi monitoring to inform building facility planning. Em *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, páginas 130–138. IEEE.

Sandhu, R. e Park, J. (2003). Usage control: A vision for next generation access control. Em *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, páginas 17–31. Springer.

Security e Committee, P. (2004). Break-glass – An Approach to Granting Emergency Access to Healthcare Systems. Joint NEMA/COCIR/JIRA.

Sicari, S., Rizzardi, A., Grieco, L. A. e Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, 76:146–164.

Silverstein, J. (2019). Hundreds of millions of Facebook user records were exposed on Amazon cloud server. https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/. [Online]. Acessado em Abr. 2019.

Sizemore, A. E. e Bassett, D. S. (2017). Dynamic graph metrics: Tutorial, toolbox, and tale. *NeuroImage*.

Socialstyrelsen (2018). Health Care Practitioners. http://www.socialstyrelsen.se/english. [Online]. Acesso em: Dez. 2018.

Son, H., Kang, N., Gwak, B. e Lee, D. (2017). An adaptive IoT trust estimation scheme combining interaction history and stereotypical reputation. Em *CCNC Consumer Communications & Networking Conference*, páginas 349–352. IEEE.

Sriram, N. (2017). Survey on security of Internet of Things in eHealth and clouds. Em *International Journal of Innovative Computer Science & Engineering*, volume 4, páginas 22–28. IJICSE.

Taylor, P., Griffiths, N., Barakat, L. e Miles, S. (2017). Bootstrapping trust with partial and subjective observability. Em *Conference on Autonomous Agents and MultiAgent Systems*, páginas 1745–1747. IFAAMAS.

Truong, N. B., Lee, H., Askwith, B. e Lee, G. M. (2017). Toward a trust evaluation mechanism in the social Internet of Things. *Sensors*, 17(6):1346.

Umarani, V. e Sundaram, K. S. (2013). Survey of various trust models and their behavior in wireless sensor networks. *International Journal of Emerging Technology and Advanced Engineering*, 3(10):180–188.

van de Leemput, I. A., Wichers, M., Cramer, A. O., Borsboom, D., Tuerlinckx, F., Kuppens, P., van Nes, E. H., Viechtbauer, W., Giltay, E. J., Aggen, S. H. et al. (2014). Critical slowing down as early warning for the onset and termination of depression. *Proceedings of the National Academy of Sciences*, 111(1):87–92.

Vasilomanolakis, E., Wolf, J. H., Böck, L., Karuppayah, S. e Mühlhäuser, M. (2017). I trust my zombies: A trust-enabled botnet. *arXiv preprint arXiv:1712.03713*.

Vimalachandran, P., Wang, H., Zhang, Y., Heyward, B. e Zhao, Y. (2017). Preserving patient-centred controls in electronic health record systems: A reliance-based model implication. Em *Orange Technologies (ICOT), 2017 International Conference on*, páginas 37–44. IEEE.

Vivekavardhana, R. B. e Sudhindra, K. R. (2014). Survey of Trust Models in Wireless Sensor Networks. *International Journal of Advanced Information Science and Technology (IJAIST)*, 31(31).

Wagenseller, P., Wang, F. e Wu, W. (2018). Size matters: A comparative analysis of community detection algorithms. *IEEE Transactions on Computational Social Systems*, 5(4):951–960.

Wallgren, L., Raza, S. e Voigt, T. (2013). Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8):794326.

Wang, F., Orton, K., Wagenseller, P. e Xu, K. (2018). Towards understanding community interests with topic modeling. *IEEE Access*, 6:24660–24668.

Wang, J., Abid, H., Lee, S., Shu, L. e Xia, F. (2011). A secured health care application architecture for cyber-physical systems. *CoRR*, abs/1201.0213.

Wang, Y., Chen, R., Cho, J.-H. e Tsai, J. J. (2017). Trust-based task assignment with multiobjective optimization in service-oriented ad hoc networks. *IEEE Transactions on Network and Service Management*, 14(1):217–232.

Wood, D., Apthorpe, N. e Feamster, N. (2017). Cleartext data transmissions in consumer iot medical devices. Em *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, páginas 7–12. ACM.

Wu, Z. e Palmer, M. (1994). Verbs semantics and lexical selection. Em *Association for Computational Linguistics*, páginas 133–138.

Xie, J., Kelley, S. e Szymanski, B. K. (2013). Overlapping community detection in networks: The state-of-the-art and comparative study. *Acm computing surveys (csur)*, 45(4):43.

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

Yang, L., Ding, C., Wu, M. e Wang, K. (2017). Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance. *Computer Networks*, 129:410–428.

Yedidia, J. S., Freeman, W. T. e Weiss, Y. (2003). Understanding belief propagation and its generalizations. *Exploring artificial intelligence in the new millennium*, 8:236–239.

Yuqiang, C., Jianlan, G. e Xuanzi, H. (2010). The research of Internet of Things' supporting technologies which face the logistics industry. Em *Computational Intelligence and Security (CIS)*, páginas 659–663. IEEE.

Zhang, Y. e Wu, X. (2016). Access control in Internet of Things: A survey. Em *Asia-Pacific Engineering and Technology Conference (APETC 2017)*.

Zrelli, R., Yeddes, M. e Hadj-Alouane, N. B. (2017). Checking and enforcing security through opacity in healthcare applications. Em *International Conference on Service-Oriented Computing*, páginas 161–173. Springer.

Zuo, X. e Iamnitchi, A. (2016). A survey of socially aware peer-to-peer systems. *ACM Computing Surveys (CSUR)*, 49(1):9.

APÊNDICE A – ANÁLISE COMPLEMENTAR

Este Apêndice apresenta uma análise complementar dos resultados das simulações dos Cenários 1 e 2 com eventos críticos aos 890s, os quais não foram apresentados no Capítulo 5. Além disso, analisa-se suas contribuições para demonstrar a robustez, através da disponibilidade e da confiabilidade, e a segurança, através da disponibilidade, do STEALTH na garantia da disseminação de dados sensíveis.

A.1 CARACTERIZAÇÃO DO MODELO DE MOBILIDADE

Como discutido na Subseção 5.4.1, inicialmente o modelo de mobilidade foi caraterizado, a fim de viabilizar as demais avaliações dos resultados obtidos. Nessa seção são apresentados os resultados complementares de caracterização das vizinhanças para os cenários 1 e 2 com eventos críticos ocorridos aos 890s de simulação. Com isso, verifica-se a evolução das vizinhanças dos nós praticamente ao longo de toda a simulação, exceto nos 10s finais.

As Figuras A.1 e A.2 demonstram como se comportam as vizinhanças dos nós. Nas Figuras A.1(a) e A.2(a) constata-se que a vizinhança dos nós analisados - 37, 52 e 70 - tiveram um comportamento semelhante na tendência da quantidade de vizinhos - média e instantânea. Os nós 37 e 52 mantiveram um N_N semelhante nos cenário 1 e 2. A vizinhança do nó 70 destacou-se em quantidade de nós, sendo quase o triplo da do nó 37.

As Figuras A.1(b) e A.2(b) apresentam a evolução da vizinhança em torno dos nós 37, 52, e 70, conforme o cenário avaliado e em uma determinada rodada de simulação. A evolução da vizinhança é computada a partir de 25s do início de cada simulação, que é o tempo mínimo para que todos os 100 nós envolvidos estejam em condições de enviar e receber mensagens normalmente. A presença da vizinhança do nó 70 no cenário 1 é ilustrada na Figura A.1(b). Observa-se que o STEALTH criou redes locais em torno desse nó em quase 100% do tempo que ele esteve ativo na simulação. Próximo dos 400s e aos 890s, quando entrou em situação emergencial, ele não possuía vizinho algum. Esse resultado distingue-se daqueles nas Figuras 5.1, 5.2 e 5.1, pois quando os nós entraram em situação emergencial naqueles cenários, o modelo de mobilidade favoreceu a formação da vizinhança.

Os nós entraram em situação emergencial próximo do final da simulação, aos 890s. Nesse momento, foi observado que a mobilidade de todos os nós envolvidos na simulação é esparsa. Esse momento foi escolhido para se acompanhar a evolução das vizinhanças dos nós durante o máximo de tempo da simulação. O nó 70, por exemplo, não teve vizinhos aos 890s, como se constata na Figura A.1(b), assim como o nó 37 na Figura A.2(b). Logo, nessas rodadas de simulação esses nós não tiveram sucesso na disseminação de seus dados sensíveis.

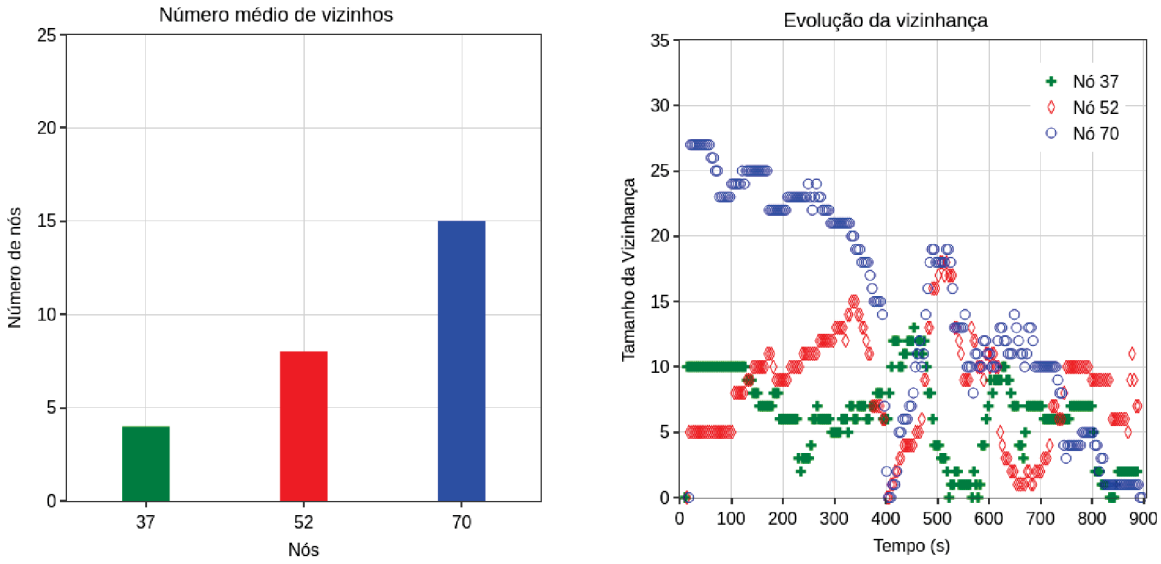


Figura A.1: Dinamicidade e tamanho das redes locais ao longo do tempo
Cenário 1 - Evento crítico aos 890s da simulação

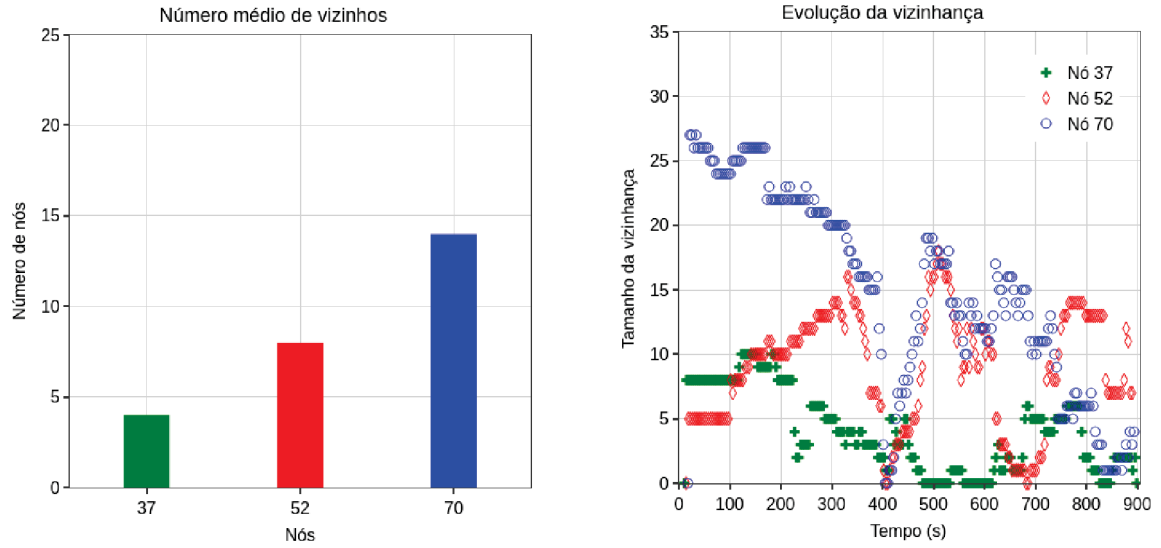


Figura A.2: Dinamicidade e tamanho das redes locais ao longo do tempo
Cenário 2 - Evento crítico aos 890s da simulação

A.2 DISPONIBILIDADE

O Número Médio de Comunidades de Interesse em Saúde, N_C, estabelecidas por cada nó avaliado ao longo das respectivas simulações é distinto e é apresentado nas Figuras A.3(a) e A.4(a). Como os nós entraram em situação emergencial aos 890s, próximo do final de cada rodada de simulação, eles estabeleceram uma quantidade maior de comunidades do que os cenários onde os eventos críticos ocorreram aos 300s e 485s. No cenário 1, conforme demonstra a Figura A.3(a), o nó 37 estabeleceu um $N_C = 10$ para todas as simulações. No cenário 2, a quantidade de comunidades estabelecidas por cada nó foi ainda maior, como demonstra a Figura A.4(a). O nó 70 estabeleceu uma quantidade ainda maior de comunidades, $N_C = 28$, o que aumenta a disponibilidade para disseminação de seus dados em situações emergenciais. Isso

caracteriza a dinamicidade das redes locais estabelecidas, especialmente da sua topologia. A mobilidade dos nós através de caminhos distintos, associada aos aspectos sociais - interesses - atribuídos a eles, impactou na formação dessas comunidades.

As Figuras A.3(b) e A.4(b) apresentam os gráficos da dinamicidade das comunidades de saúde dos nós 37, 52 e 70 estabelecidas pelo STEALTH e seu tamanho ao longo do tempo em uma rodada específica de simulação. Os resultados mostram que o STEALTH acompanhou a dinamicidade das redes locais criadas, especialmente diante da mobilidade dos nós. Ele conseguiu verificar as mudanças nas vizinhanças dos nós e ajustou suas comunidades de interesse em saúde, a fim de mantê-las atualizadas. No cenário 1, o nó 37 manteve comunidades de saúde em 93,06% do tempo de simulação em que esteve ativo. Durante esse período de tempo, o sistema esteve pronto para disseminar seus dados sensíveis, pois identificou nós que poderiam auxiliá-lo. Ao entrar em situação emergencial, aos 890s, ele possuía vizinhos ao seu redor, estabelecendo uma comunidade com um deles. O nó 52 manteve um comportamento melhor e estabeleceu comunidades por 96,30% do tempo, até que entrou em situação emergencial. Por fim, constata-se que o nó 70 manteve comunidades de saúde por 93,98% do tempo. No cenário 2, constata-se que o nó 37 manteve comunidades de saúde em 63,93% do tempo de simulação em que esteve ativo. Durante esse período de tempo, o sistema esteve pronto para disseminar seus dados sensíveis, pois identificou nós que poderiam auxiliá-lo. Porém, ao entrar em situação emergencial, aos 890s, não havia vizinhos ao seu redor, não estabelecendo assim uma comunidade. Logo, não disseminou seus dados sensíveis. O nó 52 manteve um comportamento distinto e estabeleceu comunidades por 97,22% do tempo, até que entrou em situação emergencial. Por fim, constata-se que o nó 70 foi aquele que manteve comunidades de saúde por mais tempo, 98,8%. Esse comportamento é corroborado pela Figura A.4(a), onde o nó 37 estabeleceu o menor N_C, 12, enquanto o nó 70 apresentou o maior valor entre todos os nós, 28.

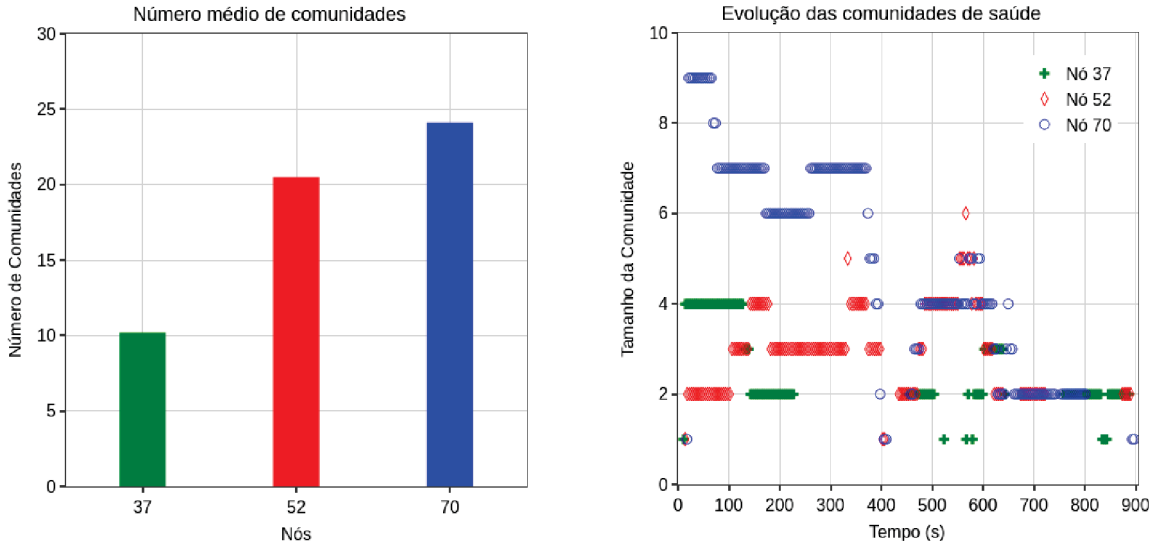


Figura A.3: Disponibilidade da comunidade de saúde ao longo do tempo
Cenário 1 - Evento crítico em 890s de simulação

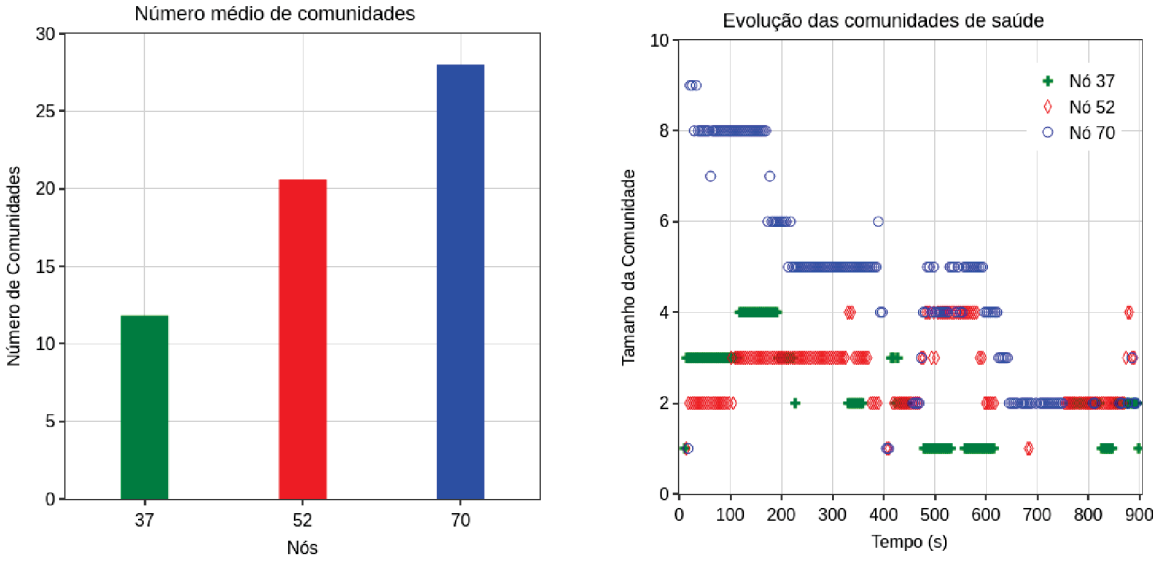


Figura A.4: Disponibilidade da comunidade de saúde ao longo do tempo
Cenário 2 - Evento crítico em 890s de simulação

A.2.1 Confiabilidade

A análise da confiabilidade verifica a capacidade do sistema em disseminar com sucesso e de maneira controlada os dados sensíveis das pessoas em situação emergencial. O comportamento dos nós selecionados - 37, 52 e 70 - nos cenários 1 e 2 com eventos críticos aos 890s demonstra essa situação. O nó 52 foi bem-sucedido (TS) em 28,57% das situações emergenciais ao longo das simulações, quando seus dados disseminados foram acessados com sucesso. Isso é demonstrado na Tabela A.1. O agrupamento dos nós em comunidades de interesse impacta diretamente na TS, pois garante a disseminação dos dados sensíveis de um nó em situação emergencial apenas a um outro nó dentre aqueles que pertençam à sua comunidade de interesse em saúde. A importância do emprego das CoI para controlar a disseminação dos dados sensíveis dos nós é constatada pelos dados não acessados (TNa). Em 80% das situações emergenciais, os dados sensíveis do nó 37 não foram acessados por outros nós. Isso ocorreu devido à falta de uma comunidade de saúde durante as situações emergenciais, visto que próximo do final da simulação as interações são reduzidas, ou a sua conexão com os outros nós foi interrompida por conta da sua mobilidade.

Tabela A.1: Disseminação dos dados

Cenário		**UM**		**DOIS**	
Métrica		TS (%)	TN_a (%)	TS (%)	TN_a (%)
Nó	37	20	**80**	14,29	85,71
	52	**28,57**	71,43	22,86	77,14
	70	0	**100**	62,86	37,14

O tempo médio de acesso aos dados sensíveis (MTA) representa o custo em relação ao tempo para que os dados sensíveis disseminados por um nó em situação emergencial sejam acessados. Ele é impactado diretamente pela dinamicidade das redes locais estabelecidas, cuja topologia se modifica com a mobilidade dos nós. A Tabela A.3 sumariza os resultados obtidos, onde é possível constatar que eles atendem à latência máxima de 125ms estabelecida pela IEEE para entrega de alertas médicos Association et al. (2012). Enquanto os dados sensíveis do nó 52 foram acessados imediatamente ($MTA = 0$), os do nó 37 foram acessados, em média, após 8ms

de sua disseminação. No cenário 1, o nó 70 não disseminou seus dados em nenhuma rodada de simulação. Isso ocorreu devido à falta de uma comunidade de saúde durante as situações emergenciais, visto que próximo do final da simulação as interações são reduzidas ou a sua conexão com os outros nós foi interrompida por conta da sua mobilidade. O emprego das comunidades de interesse contribui para o processo de tomada decisão de verificação do nó adequado e reduz o tempo de acesso aos dados disseminados.

Tabela A.2: Latência no acesso aos dados disseminados

Métrica		MTA (ms)	
Cenário		**UM**	**DOIS**
Nó	37	5	8
	52	**0**	**0**
	70	-	3

Os dados sensíveis dos nós em situação emergencial foram disseminados somente aos nós pertencentes às suas comunidades de saúde e diante das competências previstas na Tabela 5.2. O emprego de interesses e competências, associados à formação de comunidades de interesse, além de possibilitar avaliar a confiança dos nós, permite controlar a disseminação dos seus dados sensíveis. Isso ocorre em uma condição *Zero-Knowledge*, visto que as comunidades de saúde são recriadas periodicamente e desconsideram interações anteriores entre os nós da rede. O sucesso no acesso aos dados por competência (TS_{Skill}) indica a prevalência das competências nas comunidades estabelecidas no momento em que os nós entram em situação emergencial, como se observa na Tabela A.3. No cenário 1, sempre que o nó 37 entrou em situação emergencial, ele disseminou seus dados a pessoas com competência em outras áreas que não a de saúde. A situação do nó 70 é a esperada, visto que quando em situação emergencial, ele não disseminou seus dados, TS =0, conforme apresentado na Tabela A.1. No cenário 2, 50% do total de dados disseminados foram para nós com competência de médico. Isso indica que em 50% das situações emergenciais, o STEALTH detectou a presença de pelo menos um médico na comunidade de saúde disponível.

Tabela A.3: Controle de disseminação

Métrica		Taxa de Acesso por competência (TS_{Skill}) (%)					
Cenário		**UM**			**DOIS**		
Nó		37	52	70	37	52	70
Competência	Médico	0	22,22	**0**	7,60	**50,00**	18,18
	Enfermeiro	0	11,11	**0**	7,60	30,00	13,64
	Cuidador	0	22,22	**0**	7,60	16,67	36,36
	Outras	**100**	44,44	**0**	76,92	3,33	31,82

As Figuras A.5 e A.6 exibem o estado das redes locais estabelecidas pelos nós avaliados e disponíveis quando eles entraram em situação emergencial. O momento da disseminação dos dados sensíveis dos nós avaliados no cenário 1 é exibido na Figura A.5. Nela observa-se os vizinhos em torno de cada nó avaliado e suas respectivas comunidades de saúde em uma rodada de simulação específica. O nó 37 possuía apenas um vizinho na sua comunidade de saúde, o nó 70, que detinha a competência *outra*, como ilustra a Figura A.5(a). Constata-se, também, o tipo de comunidade criada pelo STEALTH, sobreposta (Chakraborty et al., 2017) (Chakraborty et al., 2012) (Xie et al., 2013). O nó 37 mantém uma comunidade de saúde com o nó 70, assim como

mantém outra com o nó 88. O nó 52, como ilustra a Figura A.5(b), possuía uma quantidade maior de vizinhos, 7, mas sua comunidade de saúde tinha apenas um membro, nó 61, que detinha a competência de médico. A condição do nó 70 foi constatada pelas métricas anteriores. Assim, devido à ausência de vizinhos, como se observa na Figura A.5(c), esse nó ficou sozinho na sua comunidade de saúde e não conseguiu disseminar seus dados sensíveis a outro nó.

A Figura A.6 apresenta as configurações de redes locais para uma rodada de simulação do cenário 2 no momento em que os nós avaliados entraram em situação emergencial. O comportamento do nó 37 é idêntico ao do nó 70 citado anteriormente. O nó 37 não conseguiu disseminar seus dados por não possuir vizinhos ao seu redor. O nó 52 possuía vários vizinhos e dois deles pertenciam à sua comunidade de saúde, 13 e 41. Ambos possuíam a mesma competência - outra. Logo, como a verificação do nó para o qual os dados sensíveis devem ser disseminados ocorre em função da confiança medida para cada nó, que leva em conta competência e interesses, a escolha do nó 13 se deu porque ele possui mais interesses em comum com o nó 52.

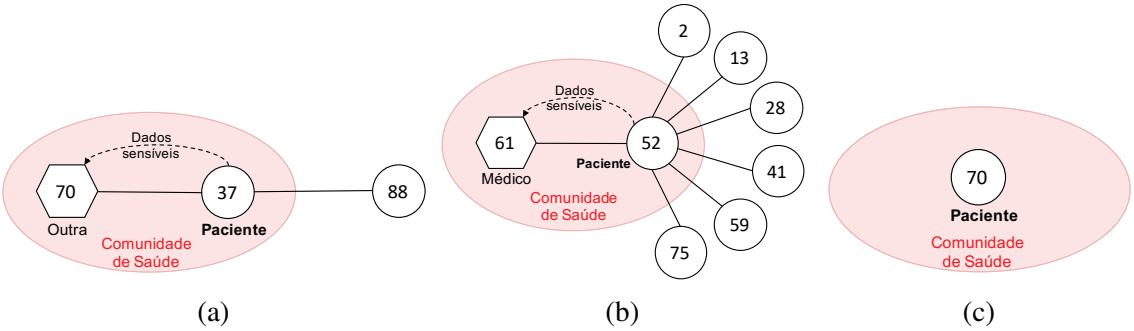


Figura A.5: Comunidades de saúde dos nós 37, 52 e 70 durante situação emergencial
Cenário 1 - Evento crítico em 890s de simulação

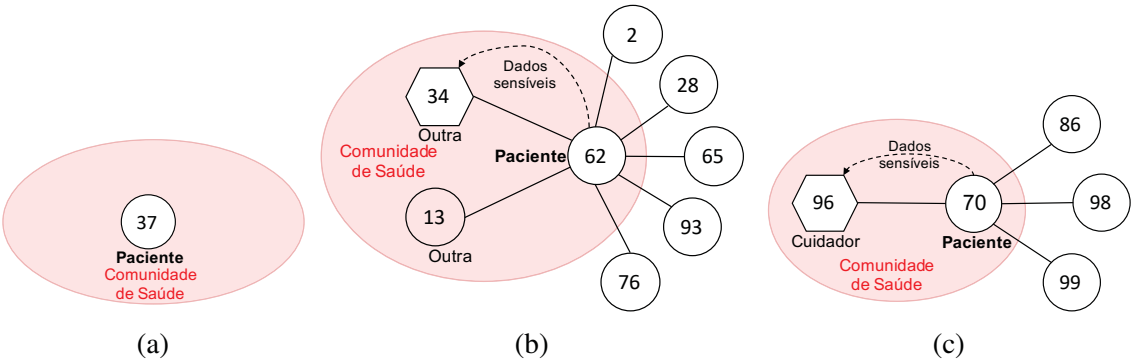


Figura A.6: Comunidades de saúde dos nós 37, 52 e 70 durante situação emergencial
Cenário 2 - Evento crítico em 890s de simulação

APÊNDICE B – CONCEITOS COMPLEMENTARES

Os conceitos relacionados à Internet das Coisas (IoT) e aos mecanismos de controle de acesso disponíveis na literatura auxiliam na compreensão desse trabalho. Logo, a Seção B.1 apresenta alguns conceitos sobre a IoT, enquanto a Seção B.2 descreve os diversos mecanismos de controle de acesso encontrados na literatura e suas principais características.

B.1 INTERNET DAS COISAS

O crescimento contínuo do número de dispositivos aptos a serem conectados em rede traz desafios ao seu uso em redes, especialmente no que tange à Internet das Coisas (IoT). Observa-se essa tendência em diversas pesquisas realizadas no mercado, que ressaltam a importância da IoT nos próximos anos. Segundo Ericsson (2018), o crescimento da IoT e a quantidade de dispositivos conectados resultam das aplicações emergentes e de novos modelos de negócios, da padronização e queda dos custos dos equipamentos. Para 2022, há uma previsão de que aproximadamente 29 bilhões de dispositivos conectados, dos quais 18 bilhões relacionados à IoT. Esse cenário motiva o estudo desse tipo de rede e incentiva cada vez mais a alocação de recursos financeiros, seja nos ambientes acadêmicos, seja nas empresas de tecnologia e de serviços.

O uso da IoT beneficia diversas áreas, inclusive a saúde, por exemplo, e segundo Farahani et al. (2017), o gerenciamento das atividades de cuidados aos pacientes tem sido um desafio, considerando a insuficiência e diminuição da efetividade dos serviços prestados frente ao crescente aumento das demandas de uma população cada vez mais idosa e com doenças crônicas. A IoT contribui para a melhoria dos cuidados aos pacientes pelo emprego de sensores inteligentes usados junto ao seu corpo. Ela oferece condições para que sinais vitais como batimentos cardíacos, pressão sanguínea e nível de glicose, entre outros, sejam coletados e, posteriormente, enviados a *smartphones*, por exemplo, que os encaminharão à uma unidade de saúde, através da Internet.

B.1.1 Características

Kevin Ashton propôs o conceito de Internet das coisas em 1999. Na época, ele se referiu à IoT como objetos interoperáveis identificáveis de maneira única e conectados pela tecnologia de identificação por rádio frequência (do inglês, *Radio-Frequency Identification* - RFID) (Li et al., 2015). Atribui-se o termo Internet das Coisas aos *Auto-ID Labs* (Atzori et al., 2010) (Labs, 2018), uma rede independente composta por 7 laboratórios de pesquisas acadêmicas. Semanticamente, esse termo significa uma rede mundial de objetos interconectados e endereçados de forma única, baseada em protocolos de comunicação padrão (INFSO, 2008). Contudo, não há uma delimitação exata para as *coisas*, mas entende-se que elas são animais, pessoas ou objetos, variando conforme o domínio de aplicação. Em uma residência, as *coisas* seriam eletrodomésticos, luminárias, fechaduras, portas, por exemplo. Em um ambiente industrial, o conjunto de *coisas* contempla, entre outros, peças, ferramentas, máquinas diversas e sensores. Na área de saúde, as *coisas* são, entre outros, os instrumentos médicos, os sensores instalados junto ao corpo humano e os dispositivos implantados no corpo humano (do inglês, *Implantable Medical Devices* - IMD).

A comunicação na IoT não se limita aos equipamentos, mas também entre as pessoas e o ambiente ao seu redor. Individualmente, as *coisas* do dia-a-dia como os equipamentos das pessoas, veículos, computadores, equipamentos médicos, entre outros, terão uma identificação única, que permitirá que elas se comuniquem entre si. Além disso, como essas *coisas sentem* o ambiente

onde se encontram, também terão a capacidade de verificar as identidades de outras *coisas*. Além disso, elas se comunicarão e compartilharão informações, muitas vezes autonomamente, dispensando a ação do ser humano (Abomhara e Køien, 2014).

B.1.2 Arquitetura

O uso de uma arquitetura de IoT aberta e baseada em camadas maximiza a interoperabilidade entre os sistemas heterogêneos e recursos distribuídos existentes, e permite sua implementação (Abomhara e Køien, 2014). A literatura disponibiliza diversos tipos de arquitetura para a IoT, vários deles aplicam o conceito de camadas. Bandyopadhyay e Sen (2011) propuseram uma arquitetura para IoT em várias camadas, que parte de uma camada de baixo nível para a aquisição dos dados, chegando a camada de aplicação no topo. Ela atende aos requisitos dos vários domínios onde seja aplicada, tais como indústrias, empresas e governo. Nessa proposta, as camadas de Internet servem como um meio de comunicação comum, transportado os dados capturados nas camadas de *gateway* de acesso e de borda até a camada de aplicação, que fica responsável por utilizá-los. Uma outra arquitetura apresentada por Yuqiang et al. (2010) divide-se em três camadas - percepção, rede e aplicação. A camada de percepção coleta os dados, enquanto a camada de rede responde pela sua transmissão. A camada de aplicação reconhece e percebe as relações entre dispositivos e entre pessoas e dispositivos, possuindo uma função inteligente.

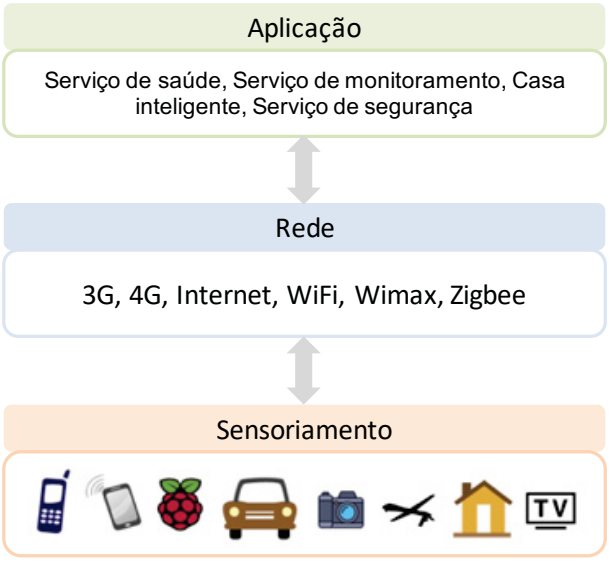


Figura B.1: Arquitetura da IoT

A Figura B.1, elaborada como base no trabalho de Li et al. (2014), apresenta um exemplo de uma arquitetura básica da IoT, que se divide em três camadas distintas - sensoriamento, rede e aplicação. As *coisas*, ou seja, os dispositivos, encontram-se na camada de sensoriamento. Elas coletam informações e, posteriormente, encaminham-nas à Internet, pela camada de rede, fazendo uso das tecnologias de comunicação existentes. A camada de aplicação responde pelas aplicações como saúde, vigilância, entre outras, assim como monitora e controla os sensores.

B.1.3 Domínios de Aplicação

A IoT permeia diversos domínios para melhorar a execução de tarefas, auxiliar nas tomadas de decisões e aprimorar processos industriais, entre outras finalidades. Os seres humanos mantêm muitas dessas atividades usando sistemas com tecnologias antigas. Logo, seu uso oferece

novas possibilidades em termos de produtos e serviços. Domínios como vigilância, logística e processos industriais, entre outros, beneficiam-se da tecnologia RFID, que possibilita sua integração às redes IoT. Além disso, a evolução das tecnologias de rede levou a IoT a outros domínios rapidamente, como residências, onde ocorre a integração de mecanismos automáticos existentes, a chamada domótica; o monitoramento ambiental, veículos autônomos, entre outros.

O uso da Internet das Coisas também impõe desafios, que variam conforme a área e o objetivo a ser atingido. No domínio de saúde, por exemplo, a carência de padronização para conexão dos equipamentos médicos em rede (Farahani et al., 2017) impede a interoperabilidade desses dispositivos de forma ampla e em qualquer ambiente. No domínio da domótica, equipamentos já são fabricados contemplando a possibilidade de serem conectados em redes . Há vários trabalhos na literatura ocupando-se do uso da IoT em diversos domínios, a fim de atender aos principais desafios que surgem. Porém, ainda não solucionam as questões como um todo. A Tabela B.1 apresenta alguns domínios de aplicação passíveis de uso da IoT, apresentando as áreas de maior destaque em cada um deles, seus benefícios e os desafios identificados.

Tabela B.1: Domínios de aplicação da IoT - Benefícios e desafios

Domínios da aplicação	**Benefícios**	**Desafios**
Vigilância	Novas tecnologias Possibilidade de gestão ubíqua	Equipamentos antigos Necessidade de interfaces com as redes
Monitoramento ambiental	Uso do RFID Sensores disponíveis no mercado	Necessidade de sensores diversos Mobilidade
Domótica	Ambientes restritos Segurança física	Equipamentos despreparados para conexão em rede Falta de padronização
Processos industriais	Ambientes restritos Segurança física Uso de RFID	Equipamentos despreparados para conexão em rede Falta de padronização
Veículos autônomos	Alguns dispositivos já preparados para conexão em rede	Falta de padronização dos veículos e ambiente Mobilidade Conectividade
Saúde	Uso de smartphones com sensores embarcados Conexão com a Internet	Necessidade de privacidade Falta de padronização dos sensores

Dentre os vários domínios de aplicação da IoT abordados na literatura, como a vigilância, o monitoramento ambiental, a automatização residencial, os processos industriais, a logística e veículos autônomos, destaca-se a área de saúde. A evolução das tecnologias em torno da IoT trouxe benefícios a essa área, ampliando o atendimento oferecido aos cidadãos e promovendo melhorias na sua qualidade de vida. Esse quadro ganha mais destaque quando se observa o aumento constante nos custos dos serviços de saúde, enquanto cresce o número de pessoas idosas e com doenças crônicas dentro da população. Logo, o atendimento de enfermagem em unidades de saúde envolve um grande número de profissionais, pois demanda o monitoramento do estado de saúde dos pacientes diuturnamente. A IoT oferece condições de se rastrear a localização e as condições do paciente, além de seus sinais vitais, alertando os profissionais de saúde sobre alterações que fujam à normalidade. Diante disso, por exemplo, quando um paciente necessita repousar, mas se levanta da cama, sensores no seu corpo e na própria cama atuam. Eles coletam as informações e as repassam, mediante um sistema de comunicação disponível, aos profissionais de saúde competentes, facultando um pronto atendimento.

A tomada de decisão em situações de emergência e as consequentes ações devem ocorrer no menor tempo possível, a fim de minimizar a possibilidade de perda da vida do paciente. Logo, a IoT viabiliza a instalação de sensores junto ao corpo do paciente ou dentro dele, coletando seus

sinais vitais para envio à uma central de monitoramento instalada em uma unidade de saúde. Ações são empreendidas remotamente, dependendo do tipo de dispositivo que o paciente leva junto ao corpo, acontecendo antes que uma equipe de atendimento de emergência chegue ao local, agilizando os primeiros socorros. Tão logo esse paciente dá entrada em uma unidade de saúde, acontece uma correlação entre seus sinais vitais e outras informações pessoais disponíveis em servidores dessa instituição para uso no atendimento.

A telemedicina é um outro setor da saúde com grande potencial para uso da IoT, empregando os *smartphones* disponíveis junto à população (Farahani et al., 2017). Eles possuem diversos sensores embarcados, conectam-se a outros aparelhos e facilitam a comunicação com a Internet. *Smartphones* auxiliam os pacientes a verificarem suas condições de saúde, contribuindo na prevenção de doenças. Além disso, permitem que os profissionais de saúde atendam seus pacientes virtualmente. Os sinais vitais dos pacientes são coletados por dispositivos implantados dentro do corpo humano e por dispositivos ou sensores vestíveis (do inglês, *wearable*) (Sriram, 2017) (Wang et al., 2011), por exemplo, inclusive em situações de emergência, pela comunicação disponível pelos *smartphones* (Farahani et al., 2017) (Sriram, 2017) (Wang et al., 2011). Além de ficarem armazenados no próprio dispositivo, também são armazenadas na *cloud* (Vimalachandran et al., 2017) ou *fog* (Farahani et al., 2017), conforme a necessidade.

B.2 TÉCNICAS DE CONTROLE DE ACESSO

Um controle de acesso tem como função principal conceder ou negar acesso a um determinado recurso baseado em um amplo conjunto de critérios (Abomhara e Køien, 2014), sendo de grande importância a existência de conexões de rede seguras entre dispositivos. Trata-se de uma restrição seletiva de acesso a um dado local, recurso ou informação, ou seja, refere-se às permissões no uso de recursos de um sistema ou rede. Trata-se de um sistema com diversos componentes e funcionalidades ou de um serviço que faz parte de um sistema. Um controle de acesso visa identificar ou autenticar os usuários e dispositivos como entidades legítimas para acessarem alguns recursos, sendo atribuído aos diferentes atores de uma rede (Sicari et al., 2015). Sua correta identificação na rede compreende um desafio frente à situações como mobilidade e capacidade de processamento, especialmente diante da ampliação da computação ubíqua. Além disso, no caso da IoT, ela demanda uma reformulação da arquitetura de nomes, endereçamento e descoberta de dispositivos nos ambientes, para que o acesso possa ser devidamente controlado. Logo, deve-se tornar as regras de controle de acesso mais fáceis e simples.

Segundo Ouaddah et al. (2017), controle de acesso e confiança são noções intimamente relacionadas, de modo que o acesso a um dispositivo em particular a outro depende do nível de confiança existente entre eles. A relação de confiança entre dois dispositivos afeta diretamente as interações entre eles. Logo, quando dois dispositivos confiam um no outro, eles ficam propensos a compartilhar serviços e recursos (Zhang e Wu, 2016). Diversos aspectos de confiança são empregados para possibilitar sua mensuração, tais como experiências, conhecimento, recomendações, reputação, entre outras. A confiança é dividida em confiança na identidade e confiança no comportamento. A confiança na identidade é usada para indicar a identidade de uma entidade, comumente considerada nos modelos de controle de acesso tradicionais. A partir dessa verificação, entidades confiáveis acessam os recursos disponíveis. Porém, essa verificação não assegura que as entidades identificadas se comportarão de maneira correta e implica levar em conta seu comportamento na avaliação para a concessão do acesso (Lin et al., 2013).

Há diversos modelos de controle de acesso na literatura. Para que possam atuar, eles necessitam de algum critério ou política de acesso elaborada previamente, por exemplo. Dentre as principais técnicas existentes para o controle de acesso, encontram-se aquelas baseadas em

atributos - ABAC, políticas - PBAC, papéis - RBAC e uso - UCON (Ouaddah et al., 2017); baseados em papéis e localização - SRBAC (Hansen e Oleshchuk, 2003); e baseados em confiança - TBAC (Bernabe et al., 2016). Esses modelos foram pesquisados e posteriormente classificados conforme os critérios que empregam para funcionarem, dando origem à Figura B.2.

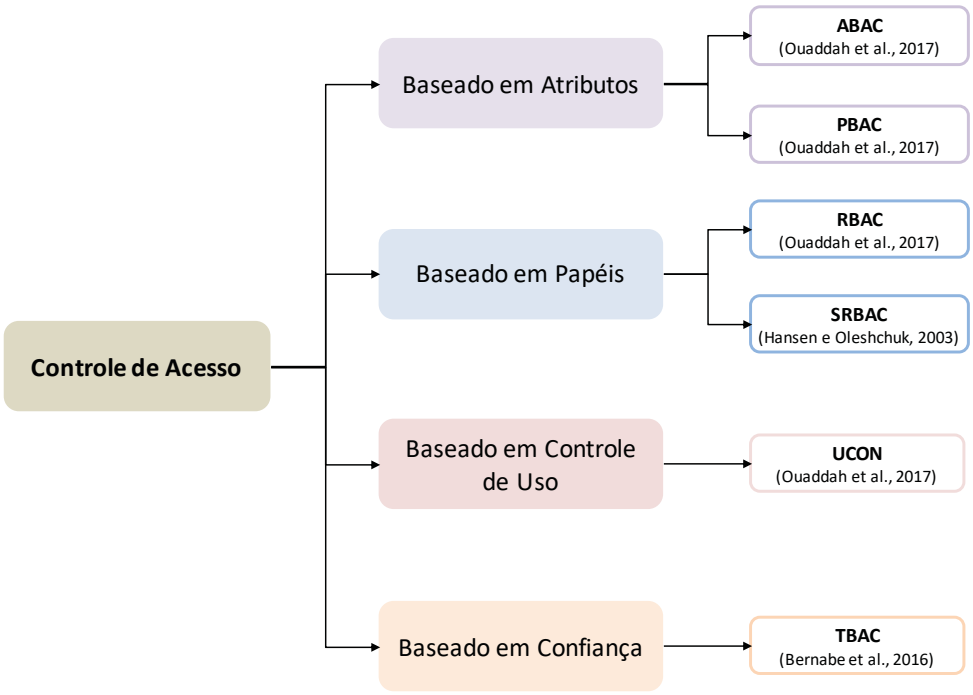


Figura B.2: Técnicas de controle de acesso

B.2.1 Controle de Acesso Baseado em Atributos (ABAC)

O controle de acesso baseado em atributos (ABAC) atua de acordo com os atributos de um indivíduo ou objeto, que o identificam. O controle ocorre a partir do momento em que é iniciada uma requisição de acesso (Ouaddah et al., 2017). O ABAC ambém conhecido como controle de acesso baseado em políticas (do inglês, *Policy-based access control* - PBAC), que especificam as condições sobre as quais o acesso aos recursos será concedido. Esse modelo compõe-se de dois aspectos: um modelo de políticas e outro de arquitetura, que aplica as políticas.

B.2.2 Controle de Acesso Baseado em Papéis (RBAC)

O controle de acesso baseado em papéis (RBAC) é baseado nos papéis atribuídos aos usuários, sendo as permissões atribuídas aos papéis. Sempre que um usuário é autenticado corretamente por um sistema, ela ativa um conjunto de papéis atribuídos ao seu usuário no ambiente, tal que ele possa executar suas tarefas. Este modelo se diferencia dos modelos tradicionais, que se baseiam nas informações de identificação dos usuários (Hansen e Oleshchuk, 2003). Ele é composto por quatro componentes distintos - *núcleo, sua hierarquia, separação estática das relações de trabalho e separação dinâmica das relações de trabalho*, que, individualmente, atribuem ao modelo um conjunto de funcionalidades (Ouaddah et al., 2017). O modo de operação do RBAC o torna inapropriado para modelar políticas de segurança para cenários de IoT complexos e ambíguos, pois criar e atribuir papéis tornam-se um desafio nesse tipo de ambiente.

Esse modelo tem a vantagem de simplificar a administração das autorizações. A troca de função de um usuário em um ambiente de trabalho, por exemplo, demanda do administrador

de segurança apenas a revogação e atribuição de um novo papel a esse usuário. O RBAC possui flexibilidade sobre as diversas políticas de segurança, já que atua diante dos papéis existentes. Todavia, enfrenta dificuldades com relação à mobilidade dos dispositivos, que faz com que os usuários necessitem de acesso aos recursos existentes a partir de quaisquer locais. Isso torna a gestão de papéis e autorizações um desafio, especialmente com grande dinamicidade na rede.

B.2.3 Controle de Acesso Baseado em Papéis - Espacial (SRBAC)

O controle de acesso baseado em papéis - Espacial (SRBAC) é uma extensão do RBAC, que incorpora a informação de localização do dispositivo a partir do qual foi requisitado o acesso a um recurso (Hansen e Oleshchuk, 2003). Ela representa aqueles locais identificáveis por parte do sistema onde o modelo está sendo aplicado. Ele atende aos ambientes de redes sem fio, onde a localização do usuário impacta nas suas permissões e papéis dentro da rede. Esse modelo consiste de cinco componentes básicos - usuários, papéis, permissões, sessões e localização, que representam, respectivamente, os papéis, permissões, sessões e localizações dos usuários.

A localização dos usuários e objetos é estimada por diversas técnicas, que variam conforme o ambiente, se é interno ou externo. O sistema de posicionamento global (do inglês, *Global Positioning System* - GPS) é empregada nos ambientes externos. Para isso, ele requer uma linha de visada entre o dispositivo móvel e o sistema GPS, ou seja, não deve haver obstáculos entre o sistema GPS e o dispositivo móvel utilizado. Em ambientes internos usa-se sinais de radiofrequência, infravermelho e ultrassom para estimar a localização dos usuários e objetos. Damiani et al. (2007) apresentaram um *framework* chamado GEO-RBAC, que estende o modelo RBAC usando o conceito de papel espacial, suportando os aspectos espaciais que envolvem os papéis, objetos e informações contextuais, além da posição do usuário.

B.2.4 Controle de Acesso Baseado em Controle de Uso (UCON)

O controle de acesso baseado em controle de uso (UCON) atua baseado no uso dos recursos, lidando com a autorização de acesso de forma continuada, ou seja, desde antes, durante e após da execução do acesso (Ouaddah et al., 2017). Ele incorpora alguns diferenciais acerca dos modelos de controle de acesso tradicionais, que se concentram somente quando da requisição do acesso. Ele acompanha as mudanças nos atributos dos sujeitos e objetos ao longo do tempo de uso, a fim de revogar um acesso concedido diante de alguma mudança nos atributos durante esse tempo, cancelando o uso do recurso por parte do sujeito ou objeto requisitante. Essa característica torna o UCON compatível com o ambiente de redes IoT, por exemplo, dada à sua natureza dinâmica. A concessão do acesso acontece entre o dispositivo e o serviço, conforme políticas de controle previamente elaboradas conforme o grau de confiança do dispositivo, do nível de confiança demandando pelo serviço e de outras informações.

O UCON consiste de três componentes centrais e três adicionais, que estão envolvidos principalmente com o processo de autorização. No núcleo do modelo estão os sujeitos, objetos e direitos. Os sujeitos são consumidores, provedores ou identificadores. Os consumidores são entidades que recebem direitos e objetos e usam os direitos para acesso aos objetos. Os provedores proveem objetos e detém direitos sobre eles. Os identificadores são entidades ou objetos digitais, que incluem sua informação sensível à privacidade (Park e Sandhu, 2002).

O modelo UCON deu origem ao modelo UCON_{ABC}, que integra autorizações (A), obrigações (B) e condições (C). Ele relega a administração, delegação e outras questões a um segundo plano, enquanto avalia as autorizações (A), obrigações (B) e condições (C) para a tomada de decisão quanto ao uso do recurso requisitado, enquanto os modelos de controle de acesso tradicionais empregam apenas a autorização para a tomada de decisão (Park e Sandhu,

2004). Nesse modelo, como os atributos dos sujeitos e objetos modificam-se em consequência do acesso aos recursos, facilitam a criação de políticas para controle da conta de acesso ao sistema. Os objetos associam-se aos seus atributos, assim como os sujeitos possuem direitos sobre os objetos. Um sujeito acessa um objeto conforme esses direitos (Ouaddah et al., 2017).

As decisões no modelo UCON$_{ABC}$ baseiam-se nos atributos dos sujeitos, objetos, autorizações, obrigações e as condições quando da requisição do recurso desejado (Sandhu e Park, 2003). Ele assume que há uma requisição de uso de um determinado objeto e que a tomada de decisão acontece tanto antes como durante o exercício dos direitos requisitados. A tomada de decisão após o uso não impacta na decisão de uso corrente. Além disso, eventuais mudanças nos atributos do sujeito ou objetos ao longo do uso resultam em efeitos colaterais do próprio uso.

B.2.5 Controle de Acesso Baseado em Confiança (TBAC)

O controle de acesso baseado em confiança (do inglês, *Trust-Based Access Control* - TBAC) usa confiança como critério para conceder acesso aos recursos. Isso possibilita a troca segura de informações entre dispositivos confiáveis e o seu emprego em redes IoT (Bernabe et al., 2016). Ele emprega entidades, como gerentes de confiança e gerentes de autorização, e exige destes dispositivos recursos computacionais mais robustos. Inicialmente, o TBAC avalia separadamente a qualidade do serviço, a segurança, a reputação e o relacionamento social do objeto. Em seguida, analisa o conjunto com um todo mediante o uso da lógica *Fuzzy*, avaliando-se o seu resultado para a concessão do acesso ao recurso pleiteado. Mahalle et al. (2013) apresentam um *framework* com uma abordagem *Fuzzy* para o controle de acesso baseado em confiança (do inglês, *Fuzzy approach to the Trust-Based Access Control* - FTBAC), que usa o FTBAC.

O uso do modelo de controle de acesso baseado em confiança possibilita a troca segura de informações entre dispositivos que mantém uma relação de confiança e permite seu emprego em redes IoT (Bernabe et al., 2016). Isso ocorre em razão da identidade dos dispositivos nem sempre ser obtida antecipadamente em ambientes dinâmicos (Mahalle et al., 2013) (Zhang e Wu, 2016), pois suas características de mobilidade dos dispositivos e dinamicidade das redes existentes tornam a gestão das identidades um processo desafiador.