Coordenação de Múltiplos Eventos Críticos de Saúde Por Redes Dinâmicas de Interesses Sociais

Agnaldo Batista[1], **Giovanni da Silva**[1], **Michele Nogueira**[1], **Aldri Santos**[1]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR

{asbatista,grsilva,michele,aldri}@inf.ufpr.br

Resumo. *O atendimento apropriado de múltiplos eventos urbanos críticos depende de uma disseminação coordenada às entidades adequadas e no momento oportuno. Na área de saúde, ambientes estruturados como hospitais, por exemplo, suportam adequadamente a disseminação dos eventos críticos. Contudo, tratar esses eventos é um desafio fora desses ambientes, pois a falta de infraestrutura de rede compromete o serviço. Este artigo apresenta o sistema C-STEALTH para atender eventos críticos de saúde de maneira distribuída, mediante o agrupamento de dispositivos em comunidades através de redes dinâmicas. Essas estratégias oferecem um serviço resiliente à mobilidade das pessoas e às falhas de comunicação, confiabilidade na disseminação dos dados e redução da latência na sua entrega. Simulações no NS-3 mostram que C-STEALTH oferece uma confiabilidade de disseminação de eventos superior a 94% com uma latência de até 166ms e 100% de disponibilidade da rede em alguns casos.*

1. Introdução

Atualmente, os serviços computacionais auxiliam na execução de muitas atividades no dia-a-dia das pessoas, contribuindo para a melhoria de sua qualidade de vida, além de outros benefícios. As tecnologias de comunicação de dados permitem às pessoas se manterem conectadas em redes continuamente, destacando-se aquelas voltadas à comunicação sem fio como a telefonia móvel (3G e 4G), o *bluetooth* e o WiFi. Elas favorecem a mobilidade das pessoas, sendo aplicadas em diversos domínios, tais como saúde, transportes, segurança pública, entre outros [Gharaibeh et al. 2017]. A garantia de mobilidade e a conexão continua viabilizam diversos serviços em redes na área de saúde, tais como agendar consultas e obter resultados de exames, entre outros. Eles possibilitam a monitoração contínua, diagnóstico médico e avaliação do desempenho físico humano. O acompanhamento remoto do estado de pacientes vem recebendo atenção [Gharaibeh et al. 2017]. Contudo, em ambientes urbanos e esparsos não construídos para atender serviços de saúde, a falta de infraestrutura de rede inviabiliza o uso desses serviços.

Vários serviços disponibilizados em ambientes urbanos automaticamente demandam criar e manter redes locais ou globais, estabelecidas dinamicamente. Serviços de saúde, por exemplo, são preservados através dessa infraestrutura, inclusive na presença de catástrofes. Nesse contexto, o tratamento de eventos apoia-se na conexão contínua das pessoas em redes. Eles acontecem de maneira isolada ou concorrente, demandando ações para seu correto tratamento [Baldoni et al. 2011], especialmente diante da dinamicidade da rede. Eventos são mudanças inesperadas, anormalidades ou falhas que alteram o estado esperado de um sistema. Em um sistema distribuído, por exemplo, as trocas de mensagens são consideradas eventos, enquanto que para as pessoas, alterações nas suas

condições normais de saúde caracterizam-se como eventos críticos. Esses eventos exigem respostas rápidas e efetivas, nem sempre possíveis como ocorre em surtos de doenças ou em cenários de conflitos, dados os desafios para esses eventos chegarem ao conhecimento dos profissionais de saúde [Organization 2019]. Assim, é crucial o acesso aos dados sensíveis e privados da pessoa em situação emergencial a fim de antecipar e ampliar a eficácia do atendimento. Por exemplo, cada minuto em parada respiratória diminui em 10% a probabilidade de sobrevida de uma pessoa [Pazin-Filho et al. 2003]. Logo, a coordenação de topologias de redes dinâmicas para suportar múltiplos eventos críticos em ambientes urbanos torna-se natural. Nos últimos anos, o uso massivo de *smartphones*, associado ao avanço das suas tecnologias de rede, tem proporcionado o estabelecimento de redes dinâmicas nesses locais, além do surgimento de novas estratégias para lidar com eventos.

A literatura apresenta diversas técnicas para lidar com eventos em ambientes urbanos. Contudo, geralmente empregam infraestruturas de redes previamente existentes, tais como WiFi e telefonia móvel. Eventos catastróficos como tempestades, terremotos, entre outros, impactam o funcionamento dos serviços, muitas vezes interrompendo-os. Em geral, o gerenciamento de eventos nesses ambientes trata situações específicas, tais como transporte público [Kolios et al. 2016], de atendimentos de emergências, de acessos à áreas de segurança [Technologies 2015]. Eles disseminam imagens, situações emergenciais e localização, entre outras informações. Contudo, são abordagens centralizadas e demandam infraestruturas de redes robustas e dispositivos específicos ao gerenciamento de eventos. As redes dinâmicas viabilizam serviços em ambientes urbanos ao permitirem a comunicação direta entre dispositivos. Nelas, os nós e conexões mudam ao longo do tempo, aparecendo e desaparecendo a qualquer momento [Márquez and Weber 2019]. Elas englobam as redes oportunísticas, cujas mensagens recebidas são armazenadas ou transportadas até serem encaminhadas a outros nós, onde apoiam as tomadas de decisões [Borrego et al. 2019]. Essa disseminação possibilita lidar com eventos na rede.

Este trabalho apresenta C-STEALTH (***C**oncurrent - **S**ocial **T**rust-Based H**EALTH** Information Dissemination Control)*, um sistema para tratar eventos críticos de saúde concorrentes em ambientes urbanos para suportar o seu gerenciamento e disseminação por redes dinâmicas. Nesta nova abordagem, diante de eventos de dispositivos próximos, cada dispositivo com o C-STEALTH instalado coordenará para disseminar seu evento a outro dispositivo próximo. Essa coordenação acontece através das mensagens trocadas entre os dispositivos durante os eventos críticos e observa as condições de saúde de seus proprietários, de modo que os eventos sejam disseminados somente às pessoas aptas (i.e., usuários do sistema com interesse em saúde para auxiliar pessoas próximas em situação emergencial). Além disso, essa disseminação depende da manutenção contínua da rede, a fim de permitir a verificação de dispositivos próximos. O C-STEALTH foi avaliado no simulador NS-3 para analisar sua robustez na manutenção de redes dinâmicas para suportar a coordenação da disseminação de múltiplos de eventos críticos em situações emergenciais. Os resultados promissores mostram que a confiabilidade do C-STEALTH na disseminação de eventos críticos superou 94% com uma latência máxima de 166ms e disponibilidade da rede de 100% em alguns casos.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve o C-STEALTH e detalha o funcionamento dos seus módulos e componentes. A Seção 4 detalha a avaliação e os resultados obtidos. A Seção 5

apresenta a conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

As soluções que tratam múltiplos eventos concorrentes de saúde na literatura geralmente aplicam-se aos ambientes de cuidados de saúde estruturados, como hospitais e clínicas. Contudo, externo a esses locais surgem desafios devido à mobilidade das pessoas e à fragilidade das infraestruturas das redes. Nessas condições, o tratamento de múltiplos eventos concorrentes demanda o emprego de abordagens diversas. Os pesquisadores têm buscado difundir os eventos com baixa latência e às entidades adequadas. Assim, embora haja soluções para redes de sensores sem fio (WSN) [Boukerche et al. 2004, Wu et al. 2016], Internet das Coisas (IoT) [Dar et al. 2015], redes pessoais (PAN) [Blount et al. 2007], WSN e redes corporais (WBAN) [Souil and Bouabdallah 2011] e redes *ad hoc* [Nittel et al. 2012, Batista et al. 2019], entre outras, e a mobilidade dos dispositivos seja considerada, ainda são incipientes as soluções em redes dinâmicas, que suportem redes complexas.

[Wu et al. 2016] propuseram um *framework* com um protocolo de colaboração dinâmico para WSN, a fim de detectar eventos de saúde em redes dinâmicas. Os sensores da rede colaboram na detecção do evento e na sua difusão para um servidor central, responsável pelas tomadas de decisões. Embora considere a mobilidade dos sensores, a solução é centralizada. [Boukerche et al. 2004] propuseram a difusão de eventos em WSN para oferecer rapidez, confiabilidade e tolerância à falhas no canal de comunicação. Trata-se de um protocolo para difusão de eventos através de rotas desde o sensor até o destinatário final, responsável pelas tomadas de decisões. Os nós vizinhos suportam uma rota dinâmica para a difusão dos eventos. [Souil and Bouabdallah 2011] discutiram a qualidade de serviço na manuseio de múltiplos eventos diante da associação de sensores corporais sem fio às WSN. O trabalho oferece confiabilidade na detecção e encaminhamento de eventos. A análise e o tratamento acontecem após ordenamento e de maneira centralizada.

Em [Blount et al. 2007], uma rede PAN composta por sensores corporais viabiliza disseminar eventos críticos através da Internet a um servidor remoto. Os sensores coletam os dados vitais das pessoas e enviam a um dispositivo hub para encaminhá-las a um servidor remoto. Essa solução provê confiabilidade na coleta dos eventos dos sensores, inclusive diante de falhas da rede. O conhecimento prévio dos dispositivos permite uma interação segura e inviabiliza seu emprego em redes dinâmicas. Contudo, os dispositivos dependem de uma infraestrutura de redes previamente estabelecida para disseminar os eventos, que são tratados de maneira centralizada em um dispositivo remoto, fora da rede PAN. Em [Nittel et al. 2012], dispositivos agentes previamente conhecidos coletam eventos emergenciais de saúde e os difundem por redes *ad hoc*. O destinatário final é responsável pelas tomadas de decisões. Essas redes proveem rotas para difusão dos eventos através dos dispositivos próximos e mantém uma infraestrutura de rede oportunística, servindo de alternativa às redes comumente existentes. Em nosso trabalho anterior [Batista et al. 2019], nós propusemos um sistema para disseminação de dados pessoais sensíveis em ambientes urbanos, focado em aspectos sociais e na segurança da entrega de dados, chamado STEALTH. Ele provê uma infraestrutura por meio de redes dinâmicas. Contudo, não trata a existência de eventos concorrentes e falhas na disseminação.

Em [Dar et al. 2015], os autores propõem uma arquitetura para integração de dispositivos e centralização das decisões, via Internet, para IoT. Dispositivos coletam eventos

de saúde de pessoas monitoradas e envia a uma entidade central remota para gerenciamento. Essa monitoração requer uma infraestrutura de rede previamente estabelecida para seu funcionamento adequado. Além disso, por ocorrer de maneira remota, o tempo para as tomadas de decisões impacta o atendimento de saúde.

3. Coordenação de Múltiplos Eventos Críticos de Saúde

Esta seção apresenta uma visão geral do modelo de rede e dos componentes do sistema C-STEALTH, bem como o seu funcionamento. O sistema C-STEALTH trata múltiplos eventos (ex. queda do nível de insulina, alteração de batimentos cardíacos e alteração de pressão arterial) concorrentes de saúde, onde um evento influencia o tratamento de outro, permitindo aos dispositivos tomar decisões nessas condições. O sistema também provê a coordenação de eventos que acontecem em momentos próximos, não simultâneos, o que impacta o seu atendimento. Além disso, ele lida com as falhas na disseminação desses eventos decorrentes dessa concorrência.

O sistema C-STEALTH executa sobre um conjunto de dispositivos portáveis (nós) interligados numa rede de comunicação sem fio denotados por $D = \{d_1, d_2, ..., d_j\}$, onde $d_j \in D$. Esses nós possuem capacidade de processamento e de comunicação para agrupar nós e disseminar dados. Assume-se que cada nó possui um identificador único (Id), imutável no tempo, e competência e interesses, como atributos individuais de confiança herdados dos seus proprietários, que os torna também aptos a atuar em determinado tipo de atendimento. O conjunto de competências $S = \{s_1, s_2, ..., s_k\}$, tal que $|S| \neq 0$, onde uma competência s_n representa uma habilidade, perícia ou conhecimento em uma área de atuação, tal como médico, policial, enfermeiro, e outros. Assume-se, também, que cada nó está associado a um conjunto de interesses $I_n = \{i_1, i_2, ..., i_z\}$, tal que $|I_n| \neq 0$ e $I_n \subset I$, onde I é o conjunto de todos os interesses. Um interesse é um *hobby*, gosto ou preferência definido manualmente pelo usuário do dispositivo, 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 representada por tuplas $\langle$nó, período, interesse$\rangle$, 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 $t_{s*} \leq t_{e*}$[1]. Um evento E é representado pela tupla $\langle$identificador do nó, instante, dados sensíveis$\rangle$, e será disseminado quando um nó entrar em situação emergencial. Por simplicidade, assume-se que os nós desconectados ou com falhas intermitentes não atuam na rede. Além disso, os nós conectados possuem comportamento honesto, sendo desconsiderada a ocorrência de ataques ao funcionamento do sistema.

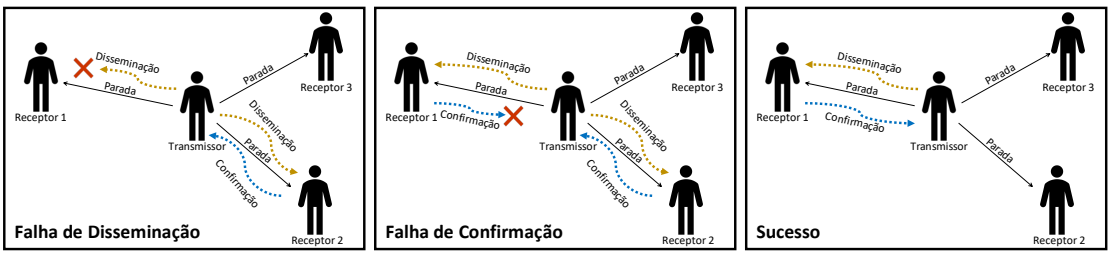

Figura 1. Robustez contra falhas na entrega de dados sensíveis

O sistema C-STEALTH trata modelos de falhas esperadas na transmissão de dados sensíveis ao usuário destino, o que auxiliará na presença de eventos críticos de saúde,

[1]Definição adaptada do conceito de comunidades dinâmicas proposto por [Coscia et al. 2011] e revisado por [Rossetti and Cazabet 2018]

tais como queda do nível de insulina, alteração de batimentos cardíacos e alteração de pressão arterial, entre outros. Assume-se a possibilidade de falhas na recepção e na confirmação da entrega dos dados, como mostram dois dos cenários de rede social ilustrados na Figura 1. Na falha de disseminação, o usuário destino não recebe os dados devido a sua mobilidade ou por falhas no seu dispositivo, por exemplo. Na falha de confirmação, o usuário destino recebe os dados sensíveis, mas a confirmação não é recebida pelo transmissor diante de sua mobilidade ou falha dos dispositivos, ou o usuário destino também se encontrar em situação emergencial. O sucesso na disseminação acontece quando o usuário destino recebe os dados sensíveis e o transmissor, a confirmação do recebimento.

3.1. Arquitetura C-STEALTH

A arquitetura do sistema C-STEALTH é composta pelos módulos de (i) **Gestão de Comunidades** e de (ii) **Gestão de Eventos Críticos**, como ilustra a Figura 2. O módulo Gestão de Comunidades cria e atualiza as comunidades de interesse em saúde (CIS) estabelecidas ao longo do tempo a partir da interação entre os dispositivos das pessoas portadoras. O módulo Gestão de Eventos Críticos verifica e coordena a disseminação dos eventos críticos da pessoa em situação emergencial ao dispositivo da pessoa adequada.

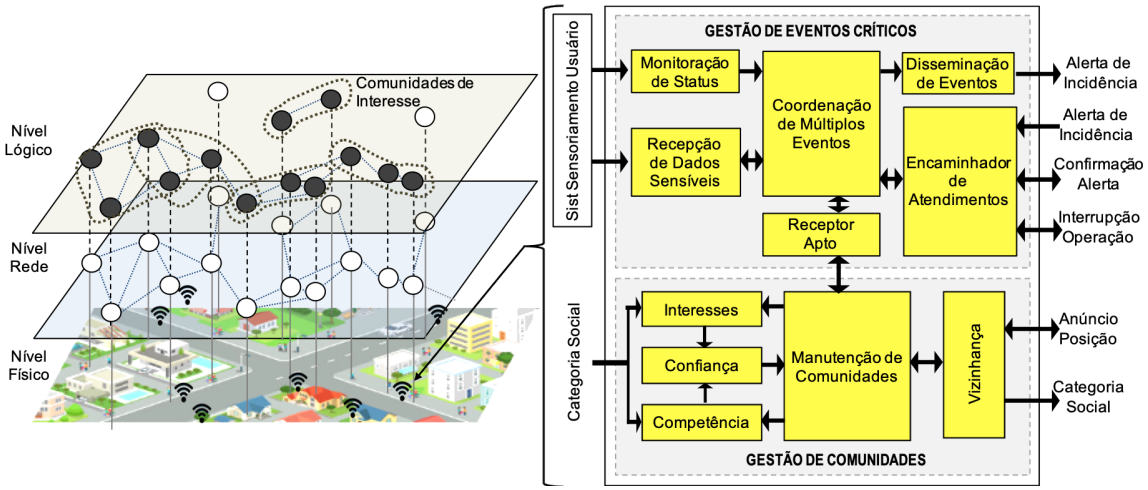

Figura 2. Arquitetura C-STEALTH

3.1.1. Módulo Gestão de Comunidades

Este módulo verifica a vizinhança dos nós, mantém as CISs, e identifica os nós vizinhos para participar de suas CISs. Esses nós são aqueles no raio de cobertura de outros nós. Este módulo é composto por componentes que identificam a vizinhança de um nó e os agrupa em CIS; medem a confiança dos nós e identificam aquele com a confiança mais elevada dentro de uma CIS; e coordenam a criação, extinção e modificação das CISs, a partir das informações de interação com os nós vizinhos. Assim, este módulo garante que as CISs acompanhem a evolução das redes locais estabelecidas ao longo do tempo para suportar a coordenação da disseminação de eventos críticos.

Os nós iniciam sua operação de forma isolada e, na medida em que se movimentam, encontram outros nós e estabelecem CIS. Como descreve o Algoritmo 1, cada nó inicia sua operação em condições normais ($l.3$). Periodicamente, o nó inicializa sua lista de vizinhos ($l.5$), anuncia sua posição por mensagens em *broadcast* ($l.6$) à procura de nós

vizinhos e aguarda um intervalo de tempo até um novo anúncio (*l*.7). Assim, o custo da troca de mensagens de comunidades de interesse e competências entre os nós consiste apenas das mensagens trocadas entre os vizinhos, não impactando na escalabilidade. Quando um nó vizinho percebe que um nó anuncia a sua posição (*l*.10), ele encaminha a este nó anunciador uma mensagem com sua categoria social, informando sua competência e interesses (*l*.13). O nó anunciador, ao receber essa mensagem, do nó vizinho, verifica a existência de interesse em comum em saúde entre eles (*l*.16). Quando há esse interesse, ele mede a confiança do nó vizinho (*l*.17) e o insere na sua lista de vizinhos (*l*.18), dentro da sua CIS. Essa medição considera a confiança do nó vizinho sobre sua competência (*l*.22) e os interesses em comum entre eles (*l*.23-25).

Algoritmo 1: Gestão de Comunidades

```
1  for each node d ∈ D do
2      procedure SEARCHNEIGHBORS( )
3          emergency ← False
4          while (True) do
5              NeighborList ← 0
6              SendAnnounce( )
7              WaitInterval( )
8          end while
9      end procedure
10     procedure RECEIVEANNOUNCE( )
11         neighskill ← GetSkill( )
12         neighinterest ← GetInterests( )
13         AnswerAnnounce(id, neighskill, neighinterest)
14     end procedure
15     procedure RECEIVEANSWER (id, neighskill, neighinterests)
16         if (CommonInterests(neighinterests) AND HealthInterest(neighinterests))
17             neightrust ← EvaluateNeighborTrust(neighskill, neighinterests)
18             NeighborList ← RegisterNeighbor(id, neighskill, neighinterests, neightrust)
19         end if
20     end procedure
21     procedure EVALUATENEIGHBORTRUST (neighskill, neighinterests)
22         skilltrust ← GetSkillTrust(skill, SkillsTaxonomy)
23         numcommoninterests ← GetNumCommonInterests(interests)
24         numnodeinterests ← GetNumNodeInterests( )
25         interesttrust ← numcommoninterests / numnodeinterests
26         return (skilltrust + interesttrust) / 2
27     end procedure
```

3.1.2. Módulo Gestão de Eventos Críticos

Este módulo consiste de seis componentes, sendo os componentes *Coordenação de Múltiplos Eventos* e *Encaminhador de Atendimentos* exclusivos para a coordenação e o encaminhamento da gestão de múltiplos eventos. O componente *Coordenação de Múltiplos Eventos* gerencia as tomadas de decisões sobre os eventos críticos do nó e aqueles recebidos dos nós vizinhos. O componente *Monitoração de Status* verifica a condição de saúde da pessoa ao receber seu status de saúde, encaminhando ao componente *Coordenação de Múltiplos Eventos*. Esse componente possibilita ao componente *Disponibilidade* do STEALTH executar a coordenação dos múltiplos eventos. Um dispositivo médico, que a pessoa porta junto ao seu corpo, identifica um evento crítico e informa ao sistema C-STEALTH. O componente *Recepção de Dados Sensíveis* obtém os dados sensíveis da pessoa em situação emergencial, a partir de solicitação do componente *Coordenação*

de Múltiplos Eventos, que garante sua disseminação apenas nessas condições. O componente *Receptor Apto* verifica a pessoa adequada para se disseminar os dados sensíveis, garantindo que seja aquela com a competência mais elevada em saúde e que não esteja em situação emergencial. O componente *Disseminação de Eventos* dissemina os eventos críticos quando o componente *Coordenação de Múltiplos Eventos* entrega os dados sensíveis e o identificador da pessoa adequada. Essa disseminação ocorre por mensagens de alerta de incidência às pessoas que pertençam à CIS do nó e na medida de sua competência em saúde. O componente *Encaminhador de Atendimentos* incorpora ao componente *Disseminação* do STEALTH a adoção de ações diante das interrupções de operação dos nós vizinhos. Ele envia mensagens sobre a interrupção da operação do nó quando recebe de um nó vizinho a confirmação do recebimento de seu evento crítico. Ele também confirma o recebimento de mensagens de alerta dos nós vizinhos para atendê-los.

Algoritmo 2: Gestão de Eventos Críticos

```
1  for each node d ∈ D do
2      procedure HANDLEEMERGENCYEVENT( )
3          emergency ← True
4          AckAlertReceived ← False
5          while (emergency) do
6              neighid ← GetHigherScoreNeighbor( )
7              neighskill ← GetNeighborSkill (neighid)
8              criticaldata ← GetCriticalData (neighskill)
9              SendAlert(neighid, criticaldata)
10             WaitInterval( )
11             if (AckAlertReceived OR |NeighborList| < 2) then
12                 SendStopAnnounce(id)
13                 StopOperation( )
14             Else
15                 NeighborList ← RemoveNeighbor(neighid)
16             end if
17         end while
18     end procedure
19     procedure RECEIVEALERT (id, criticaldata)
20         if (emergency == False) then
21             SendAckAlert(id)
22         end if
23     end procedure
24     procedure RECEIVEACKALERT (id)
25         AckAlertReceived ← True
26         SendStopAnnounce(id)
27         StopOperation( )
28     end procedure
29     procedure RECEIVESTOPANNOUCE (id)
30         NeighborList ← RemoveNeighbor(id)
31     end procedure
```

Os nós pertencentes às CISs apoiam os nós que representam as pessoas em situação emergencial, como descrito no Algoritmo 2. Quando várias pessoas encontram-se nessa situação, o tratamento dos eventos é coordenado por troca de mensagens para garantir que um número maior de nós seja atendido adequadamente. Ao ocorrer um evento crítico com um determinado nó (*l*.3) e enquanto não for atendido (*l*.5), ele verifica o nó vizinho com a confiança mais elevada (*l*.6) e obtém o dado sensível apropriado (*l*.7-8). Em seguida, ele envia uma mensagem de alerta de incidência para o nó selecionado (*l*.9) com seu dado sensível e aguarda um intervalo de tempo (*l*.10). Ao receber a confirmação de recebimento da mensagem (*l*.11), o nó anuncia por *broadcast* a interrupção de sua operação (*l*.12) e a encerra (*l*.13). Caso contrário, ele remove o nó vizinho de lista de

vizinhos (l.15) e busca um novo vizinho para enviar a mensagem de alerta. Ao receber uma mensagem de alerta, se estiver operando em condições normais (l.19), o nó confirma seu recebimento (l.21). Ao receber a confirmação de recebimento de uma mensagem de alerta (l.24), o nó anuncia (l.26) e interrompe sua operação (l.27). Quando um nó percebe que outro nó anuncia a interrupção de sua operação (l.29), ele exclui esse nó da sua lista de vizinhos (l.30), impedindo que ele seja selecionado para receber seus dados sensíveis.

3.2. Funcionamento

A operação do sistema C-STEALTH e a coordenação da disseminação de dados sensíveis diante de múltiplos eventos concorrentes pode ser observada a seguir. Considere uma área urbana onde oito pessoas se deslocam a pé pelas ruas: um executivo, um piloto, um policial, um médico, um cuidador, uma enfermeira, um garçom e um advogado. Cada pessoa possui habilidade para executar tarefas no seu dia-a-dia e, eventualmente, necessita de atendimento emergencial. As pessoas possuem um interesse em comum em saúde e não mantém relações entre si. A enfermeira, o policial, o cuidador e o médico possuem interesse em saúde por conta da sua profissão, e as demais pessoas se interessam por saúde para ajudar pessoas necessitadas. Todos portam um dispositivo móvel, *smartphone*, para se conectarem em redes. O C-STEALTH roda nesses *smartphones* e está configurado para operar. Essas pessoas portam um dispositivo junto ao corpo para verificar um sinal vital, ex. sua pressão arterial, e reportar a um aplicativo instalado em seu *smartphone*. Esse aplicativo se comunica com o C-STEALTH para informar os valores medidos.

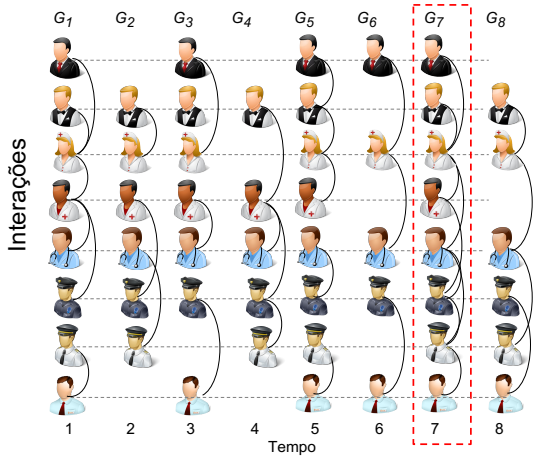

Figura 3. Interações no tempo

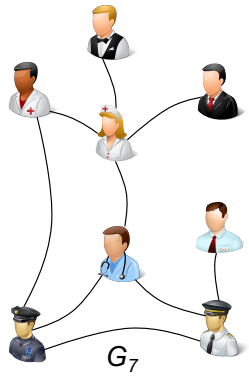

Figura 4. Grafo da rede em t_7

A Figura 3 ilustra as interações entre pessoas ao longo do tempo $t = \{1, 2, ..., 8\}$, resultantes da sua mobilidade, quando seus dispositivos estabelecem redes *ad hoc* para trocarem dados entre si. Assume-se que o médico e a enfermeira entram em situação emergencial simultaneamente em t_7. Nesse instante, seus dispositivos interagem com os de outras pessoas, como ilustra o grafo G_7 (Figura 4), e cada um deles forma sua própria CIS. Os dispositivos do médico e da enfermeira medem a confiança dos demais e os inserem na sua respectiva lista de vizinhos. Diante do evento crítico, o C-STEALTH rodando no *smartphone* do médico identifica a enfermeira como a pessoa com o maior valor de confiança na sua CIS, enquanto a enfermeira identifica o médico na sua CIS. Assim, eles disseminam seus dados sensíveis um para o outro. Esses múltiplos eventos são tratados individualmente por cada dispositivo. Os dispositivos do médico e da enfermeira não

atendem ao evento recebido por se encontrarem em situação emergencial e não confirmam seu atendimento. Diante da ausência dessa confirmação, o dispositivo do médico exclui a enfermeira da sua CIS, enquanto o da enfermeira exclui o médico da sua. Em seguida, eles verificam novamente o vizinho com o maior valor confiança na sua CIS. Através de G_7 (Figura 4), constata-se que na CIS do médico é o policial, enquanto na da enfermeira é o cuidador, para os quais eles disseminam seus dados sensíveis, respectivamente.

4. Avaliação

Esta seção apresenta a metodologia de avaliação para análise do desempenho do sistema C-STEALTH. Ele foi implementado no simulador NS-3, versão 3.28, instalado no sistema operacional Debian, versão 9.1. O cenário de avaliação compreende 100 dispositivos (nós) móveis representando o comportamento de movimentação de usuários em um ambiente urbano. Esses usuários portam *smartphones* e deslocam-se em uma área de 400m x 430m da Cidade de Estocolmo (Suécia) com velocidades entre 0,5m/s e 2,0m/s. Eles atuam sobre um modelo de mobilidade realista que considera as características do ambiente [Helgason et al. 2014]. Os nós estabelecem redes *ad hoc* através de transmissão no padrão IEEE 802.11n e uso do protocolo UDP. Os nós têm raio de alcance de 50m, e formam CIS com os nós vizinhos a cada 4s. Este tempo é suficiente a uma pessoa deslocando entre 2m e 8m poder prestar um atendimento em razão da sua proximidade. Além disso, eles são configurados randomicamente com aspectos sociais, isto é, a cada repetição de simulação eles possuem uma única competência e um conjunto de interesses, com um mínimo de um e máximo de cinco. A Tabela 1 lista a distribuição desses aspectos. Uma análise comparativa entre o C-STEALTH e o STEALTH, um sistema para um sistema para disseminação de dados pessoais sensíveis em ambientes urbanos, focado em aspectos sociais e na segurança da entrega de dados [Batista et al. 2019], é apresentada. Modificou-se a classe *node* do NS-3 para o atendimento de múltiplos eventos. As instruções para executar a aplicação e seus códigos podem ser encontrados no GitHub.[2]

Tabela 1. Distribuição dos aspectos sociais atribuídos

Aspectos Sociais	**Competências**				**Interesses**				
	Méd	Enf	Cuid	Out	Saú	Tur	Mús	Fil	Liv
# de Nós	10	15	20	55	20	30	45	60	15

Tabela 2. Eventos agendados

Nós	30 e 53	70 e 98	92 e 95
Tempo (s)	360	300	350

Os nós foram enumerados de 1 a 100 e a avaliação do comportamento do sistema C-STEALTH ocorreu por meio de seis deles - 30, 53, 70, 92, 95 e 98, sendo uma quantidade suficiente para analisar o comportamento do sistema. Eles são analisados em pares simultâneos, visto que cada par de nós entra em situação emergencial no mesmo instante de tempo, a fim de se caracterizar os múltiplos eventos. Enquanto esses nós mantém a mesma configuração em todas as repetições de simulações, os demais são configurados randomicamente a cada repetição. O tempo de simulação é de 900s, que possibilita aos indivíduos caminharem 450m$\sim$1800m. Os eventos críticos dos nós selecionados são agendados para os instantes apresentados na Tabela 2, a fim de caracterizar os eventos concorrentes; embora eles pudessem ocorrer a qualquer instante durante a operação dos nós. Assume-se que todos os nós apresentam um comportamento honesto e há mecanismos de segurança para validação das suas identidades e proteção na transmissão dos dados. Assume-se, também, que a identificação de um evento crítico acontece por um dispositivo que as pessoas portam junto ao corpo e que informa ao C-STEALTH. Os resultados

[2]https://github.com/agnaldosb/c-stealth

exibidos correspondem à média de 35 simulações e um intervalo de confiança de 95%. As definições das métricas de avaliação de desempenho encontram-se na Tabela 3. A análise da disponibilidade das redes estabelecidas C-STEALTH considera a evolução das CIS ao longo do tempo e a métrica N_C. A análise da confiabilidade na coordenação e disseminação dos eventos críticos é mensurada pelas métricas HR, FR, ANE e ADE.

Tabela 3. Métricas de avaliação de desempenho

Descrição	Equação
Número Médio de Comunidades de Interesse em Saúde (N_C) computa a média do somatório de todas as CIS formadas em cada execução y, conforme o total de possibilidades de mudanças (t_s) das CIS, por um nó x em todas as execuções (N_S).	$N_C = \sum_{x=1}^{N_S} \sum_{y=1}^{t_s} \frac{C_{xy}}{t_s \times N_S}$
Taxa de Eventos Entregues (HR) indica a taxa de eventos que foram entregues com sucesso às pessoas adequadas, sendo a razão entre o total de eventos entregues com sucesso (ED_{Sucess}) e o total de eventos ocorridos (E_{Disp}).	$HR = \frac{ED_{Success}}{E_{Disp}} \times 100$
Taxa de Erro na Entrega de Eventos (FR) indica a taxa de eventos não entregues às pessoas adequadas nas situações emergenciais [Boukerche et al. 2004].	$FR = 100 - HR$
Número Médio de Disseminação dos Eventos (ANE) indica o número médio de vezes que um evento crítico de um nó foi disseminado (N_D) até que a confirmação de seu recebimento fosse recebida pelo nó em todas as simulações realizadas. Ele corresponde à razão do somatório dos N_D e o N_S.	$ANE = \sum_{i=1}^{N_S} \frac{N_{D_i}}{N_S}$
Atraso Médio na Entrega de Eventos (ADE) computa o tempo médio de entrega dos eventos de um determinado nó para todas as simulações realizadas [Boukerche et al. 2004]. Ele corresponde ao somatório da razão entre as diferenças entre o momento em que os eventos foram recebidos (t_r) e o momento da sua disseminação (t_d), e o total de execuções (N_S).	$ADE = \sum_{i=1}^{N_S} \frac{tr_i - td_i}{N_S}$

4.1. Análise de Disponibilidade

A análise da disponibilidade verifica a prontidão do C-STEALTH na coordenação dos múltiplos eventos críticos das pessoas em situação emergencial. Esse comportamento é observado através da Tabela 4, que sumariza a quantidade média de CIS (N_C) estabelecidas, e na Figura 5. O nó 53 obteve o melhor resultado e formou em média 8,65 CISs, seguido do nó 92. Os nós 70 e 98 estabeleceram a menor quantidade de CIS durante sua operação. Esse comportamento caracteriza a dinamicidade das redes locais estabelecidas pelo C-STEALTH, especialmente sua topologia. Essas redes são estabelecidas enquanto os nós estão em operação. A densidade de nós, sua mobilidade e seu tempo de operação, além dos aspectos sociais que lhes são atribuídos impactam diretamente a quantidade de CIS (N_C) estabelecidas. Assim, como os nós 30 e 53 operaram durante 360s (Tabela 2), eles formaram mais CIS que os nós 70 e 98, que operaram por 300s. Por outro lado, o sistema STEALTH estabeleceu em média um número menor de comunidades que o C-STEALTH, apesar de ambos os sistemas gerenciarem as redes locais de forma idêntica. Em ambos os casos, o custo para formar as comunidades leva em conta o envio das mensagens de anúncio de presença de cada nó a cada 4 segundos e o recebimento das mensagens de identificação dos nós vizinhos. A diferença entre os N_C se deve aos aspectos sociais atribuídos aos nós na sua inicialização, que acontece de forma randômica a cada repetição de simulação. Um maior N_C indica uma maior disponibilidade da rede para suportar a disseminação de eventos críticos.

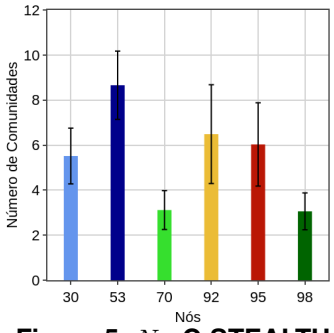

Figura 5. N_C C-STEALTH

Tabela 4. Número de comunidades (N_C)

		Número Médio de Comunidades (N_C)	
Sistema		**C-STEALTH**	**STEALTH**
Nó	**30**	5,51	4,06
	53	8,65	7,80
	70	3,11	2,74
	98	3,05	2,74
	92	6,48	7,54
	95	6,02	5,20

A dinamicidade e o tamanho das CIS dos nós avaliados durante uma repetição específica de simulação são representadas na Figura 6. Eles foram selecionados em pares - 30/53, 70/98 e 92/95 - para garantir que nos momentos dos eventos críticos um nó do par pertencesse à CIS do outro nó do par, e os eventos fossem disseminados pelo menos uma vez. Os nós 70 e 98 (Figura 6(b)), e 92 e 95 (Figura 6(c)) mantiveram CIS em 100% do tempo de operação. Esse comportamento demonstra a disponibilidade das redes locais estabelecidas para suportar a disseminação dos eventos críticos, visto que nós vizinhos foram identificados com sucesso e incorporados as suas CIS. Os nós 30 e 53 (Figura 6(a)) apresentaram um comportamento distinto. Enquanto o nó 30 estabeleceu CIS durante 72,53% do seu tempo de operação, o nó 53 obteve um desempenho inferior, formando CIS em 55,22% do tempo. Os nós 70 e 98 (Figura 6(b)) estabeleceram quantidades de CIS idênticas ao longo do tempo. Analisando-se os *logs* do sistema, observou-se que as CIS estabelecidas incorporavam os mesmos nós, indicando que nós 70 e 98 estiveram muito próximos durante todo o seu tempo de operação e percorreram caminhos semelhantes. Na medida em que as vizinhanças dos nós mudavam, ele atualizava suas CIS. Esses resultados mostram que o C-STEALTH acompanhou a dinamicidade das redes locais estabelecidas.

4.2. Análise de Confiabilidade

A análise da confiabilidade do C-STEALTH verifica sua capacidade em disseminar eventos críticos com sucesso na presença de eventos simultâneos de forma coordenada. A Tabela 5 sumariza os resultados da disseminação dos eventos. O nó 30 disseminou a maior quantidade de eventos, obtendo êxito (HR) em 97,14% deles. O nó 53 apresentou um resultado próximo, 94,29% de sucesso na disseminação de seus eventos. Esses resultados indicam que diante dos eventos críticos, esses nós identificaram vizinhos próximos para disseminarem os eventos. Esse desempenho relaciona-se com o agrupamento dos nós em CIS, visto que elas impactam diretamente a HR. As CIS suportam a disseminação dos dados sensíveis de um nó em situação emergencial apenas a um outro nó que pertença a elas. Os nós 70 e 98 obtiveram resultados idênticos e não foram bem-sucedidos (FR) na disseminação de 34,29% dos eventos. Isso indica que em mais de 60% dos eventos, o C-STEALTH não identificou pessoas aptas para recebê-los. O desempenho do STEALTH foi totalmente distinto, visto que não trata múltiplos eventos concorrentes. Logo, ele impediu que os nós avaliados fossem bem-sucedidos na disseminação dos seus eventos críticos na presença de múltiplos eventos concorrentes (HR = 0%).

A verificação da coordenação dos múltiplos eventos críticos do C-STEALTH apoia-se em situações emergenciais simultâneas de nós próximos fisicamente. Para assegurar essa situação, os nós avaliados foram escolhidos em pares, para que um nó de a

um par pertença à CIS do outro e vice-versa. Assim, eles selecionam um ao outro para disseminar seu evento crítico. Os números de disseminações de eventos (ANE) são apresentados na Tabela 6. Em 94% das simulações, o nó 30 foi bem-sucedido ao disseminar seus eventos em uma segunda tentativa e em uma das repetições de simulações teve que enviar os dados uma terceira vez para ter sucesso na entrega do evento crítico, o que é ilustrado na Figura 7. Inicialmente, o nó 30 enviou seus dados sensíveis ao nó 53, seu par, que também se encontrava em situação emergencial. Assim, após excluí-lo de sua CIS, enviou os dados para o nó 88, que não confirmou seu recebimento. Finalmente, excluído o nó 88 de sua CIS, o nó 30 enviou seus dados sensíveis ao nó 47, que confirmou seu recebimento. No STEALTH, por outro lado, os nós disseminaram seus eventos uma única vez em cada repetição de simulação, como ilustra a Tabela 6. Por não tratar eventos concorrentes e não realizar uma coordenação para atendê-los, o STEALTH interrompe a entrega dos eventos após a primeira disseminação e não conclui esse processo.

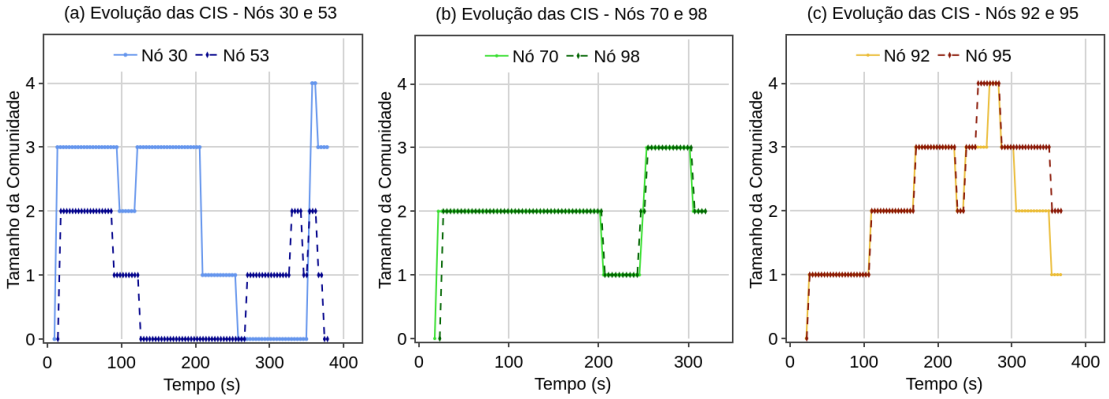

Figura 6. Dinamicidade da CIS ao longo do tempo

As trocas de mensagens diante de um evento crítico suportam as tomadas de decisão sobre as suas disseminações. Em uma das repetições de simulação, ilustrada na Figura 8, o nó 30 não obteve sucesso na disseminação de seu evento crítico. Inicialmente, ele enviou os dados sensíveis ao nó 53, seu par, que também se encontrava em situação emergencial e não confirmou o recebimento dos dados. Assim, o nó 30 excluiu o nó 53 de sua CIS, que ficou vazia, impedindo a disseminação de seu evento crítico. Os múltiplos eventos concorrentes influenciam o seu atendimento, porém a coordenação do C-STEALTH obteve sucesso na disseminação de 79,04% de todos os eventos críticos.

Tabela 5. Disseminação eventos

Sistema	Nós	HR (%)	FR (%)
C-STEALTH	30	97,14	12,86
	53	94,29	15,71
	70	65,71	34,29
	98	65,71	34,29
	92	71,43	28,57
	95	74,29	25,71
STEALTH	Todos	0	100

Tabela 6. No. de disseminações

Sistema	Nós	# Simulações		
		1	2	3
C-STEALTH	30	1	33	1
	53	2	33	0
	70	12	23	0
	98	12	23	0
	92	10	35	0
	95	9	26	0
STEALTH	Todos	35	0	0

Múltiplos eventos concorrentes impactam a latência de entrega dos eventos (ADE), visto que demandam seu envio repetidamente, diante da impossibilidade de serem atendidos por nós que também estejam em situação emergencial. Essa latência caracteriza o custo de tempo para entrega dos eventos críticos disseminados à pessoa adequada.

Além disso, a dinamicidade das redes locais estabelecidas influencia a composição das CIS, enquanto que a mobilidade dos dispositivos altera a topologia da rede. Através da Tabela 7 constata-se que a ADE do STEALTH não foi avaliada, visto que o sistema não foi bem-sucedido na disseminação dos eventos críticos. Por outro lado, em geral os eventos disseminados pelo C-STEALTH foram entregues com uma latência abaixo de 93ms, atendendo ao valor máximo de 125ms estabelecido pela IEEE para entrega de alertas médicos [Association et al. 2012]. Apenas o nó 33 teve um custo superior, ADE = 166ms, pois a maioria das suas disseminações de eventos foram confirmadas após uma segunda tentativa (Tabela 6). Esse custo se deve à coordenação para tratar dos eventos concorrentes e à mobilidade dos nós vizinhos. Em geral, o emprego das CISs contribuiu para o tratamento de múltiplos eventos simultâneos e reduziu o atraso na sua disseminação.

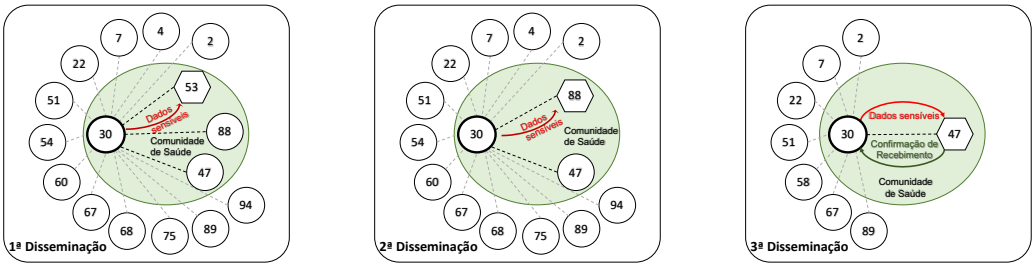

Figura 7. Disseminação de dados sensíveis com sucesso

Tabela 7. Latência dos eventos

Sistema	Nó	ADE (ms)
C-STEALTH	30	166
	53	93
	70	82
	98	88
	92	56
	95	54
STEALTH	Todos	-

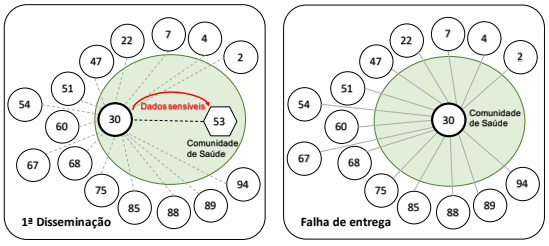

Figura 8. Falha na entrega de dados sensíveis

5. Conclusão

Este trabalho apresentou C-STEALTH, um sistema para suportar o atendimento de múltiplos eventos críticos de saúde em redes locais dinâmicas sem fio. Ele estabelece agrupamentos virtuais apoiado em atributos sociais, a fim de permitir aos dispositivos coordenarem a disseminação de seus eventos críticos de forma robusta diante de situações emergenciais concorrentes. Simulações avaliaram a eficácia do C-STEALTH e os resultados demonstraram sua capacidade de coordenar a disseminação de dados sensíveis diante de múltiplos eventos concorrentes. O C-STEALTH obteve uma confiabilidade superior a 94% disseminação dos dados e uma latência máxima de 166ms, além de uma disponibilidade da rede de até 100% em alguns casos. Como trabalhos futuros, serão investigadas questões associadas à unicidade dos identificadores dos nós, à autenticação mútua e à confiabilidade do sistema na presença de comportamento malicioso, além da extração dos aspectos sociais dos usuários a partir de suas redes sociais.

Referências

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.

Baldoni, R., Bonomi, S., Lodi, G., Platania, M., and Querzoni, L. (2011). Data Dissemination Supporting Complex Event Pattern Detection. *IJNGC*, 24.

Batista, A., Santos, A., and Nogueira, M. (2019). Disseminação Robusta de Dados Pessoais Sensíveis Baseada em Comunidade de Interesse e Confiança Social para Suportar Situações Emergenciais de Saúde. In *Anais do XIX SBSEG*, Porto Alegre, RS, Brasil. SBC.

Blount, M., Batra, V. M., Capella, A. N., Ebling, M. R., Jerome, W. F., Martin, S. M., Nidd, M., Niemi, M. R., and Wright, S. P. (2007). Remote health-care monitoring using personal care connect. *IBM systems journal*, 46(1):95–113.

Borrego, C., Borrell, J., and Robles, S. (2019). Efficient broadcast in opportunistic networks using optimal stopping theory. *Ad Hoc Networks*, 88:5–17.

Boukerche, A., Boukerche, A., Pazzi, R. W. N., and Araujo, R. B. (2004). A Fast and Reliable Protocol for Wireless Sensor Networks in Critical Conditions Monitoring Applications. In *Proceedings of the 7th ACM MSWiM*, pages 157–164. ACM.

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

Dar, K., Taherkordi, A., Baraki, H., Eliassen, F., and Geihs, K. (2015). A resource oriented integration architecture for the internet of things: A business process perspective. *Pervasive and Mobile Computing*, 20:145–159.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., and Al-Fuqaha, A. (2017). Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Communications Surveys & Tutorials*, 19(4):2456–2501.

Helgason, Ó., Kouyoumdjieva, S. T., and Karlsson, G. (2014). Opportunistic Communication and Human Mobility. *IEEE Transactions on Mobile Computing*, 13(7):1597–1610.

Kolios, P., Panayiotou, C., Ellinas, G., and Polycarpou, M. (2016). Data-Driven Event Triggering for IoT Applications. *IEEE Internet of Things Journal*, 3(6):1146–1158.

Márquez, R. and Weber, R. (2019). Overlapping Community Detection in Static and Dynamic Social Networks. In *Proceedings of the Twelfth ACM WSDM*, pages 822–823. ACM.

Nittel, S., Dorr, C., and Whittier, J. C. (2012). LocalAlert: Simulating Decentralized Ad-Hoc Collaboration in Emergency Situations. In *GIScience*, pages 146–159. Springer.

Organization, W. H. (2019). Who's work in emergencies: prepare, prevent, detect and respond: annual report 2018. Technical documents, World Health Organization.

Pazin-Filho, A., Santos, J. C., Castro, R. B. P., Bueno, C. D. F., and Schmidt, A. (2003). Parada cardiorrespiratória (pcr). *Medicina (Ribeirão Preto. Online)*, 36(2/4):163–178.

Rossetti, G. and Cazabet, R. (2018). Community Discovery in Dynamic Networks: a Survey. *ACM CSUR*, 51(2):35.

Souil, M. and Bouabdallah, A. (2011). On QoS Provisioning in Context-Aware Wireless Sensor Networks for Healthcare. In *Proceedings of 20th ICCCN*, pages 1–6. IEEE.

Technologies, H. (2015). Bhubaneswar's "Smart Safety" City Surveillance Project Powered by Honeywell Technologies. https://www.honeywell.com/en-us/newsroom/news/2015/05/bhubaneswars-smart-safety-city-surveillance-project-powered-by-honeywell-technologies. [Online]. Acessado em Dez. 2019.

Wu, H., Cao, J., and Fan, X. (2016). Dynamic collaborative in-network event detection in wireless sensor networks. *Telecommunication Systems*, 62(1):43–58.