Desafios Computacionais para Resiliência a Desastres Naturais

Alberto Schaeffer-Filho, Gabriel Nazar, Jéferson Nobre, Juliano Wickboldt, Lisandro Granville, Luciano Gaspary, Weverton Cordeiro

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

{alberto,glnazar,jcnobre,jwickboldt,granville,paschoal,wlccordeiro}
@inf.ufrgs.br

Resumo. *Com a frequente ocorrência de desastres naturais, as infraestruturas da sociedade são postas à prova. Do ponto de vista de sistemas computacionais e de comunicação, a operação dos mesmos é desafiada não só pela própria natureza dos desastres, como inundações e tempestades, mas também pela carga crítica que se impõe aos sistemas durante ações de atendimento às emergências. Sistemas de monitoramento e de alerta devem agir com celeridade para notificar a população e as autoridades. A infraestrutura de comunicação deve manter-se disponível para uso por populações em risco e por equipes de resgate. Neste documento, apresentamos o grande desafio de desenvolver sistemas de computação e de comunicação que incorporaram a resiliência a desastres de forma sistemática, capazes de atuar com eficácia na minimização de prejuízos humanos, sociais e econômicos causados por tais fenômenos.*

Abstract. *With the frequent occurrence of natural disasters, society's infrastructures are put to the test. From the perspective of computer and communication systems, their operation is challenged not only by the nature of disasters themselves, such as floods and storms, but also by the critical load imposed on systems during emergency response actions. Monitoring and warning systems must act quickly to notify the population and authorities. Communication infrastructure must remain available for use by populations at risk and by rescue teams. In this document, we present the major challenge of developing computing and communication systems that systematically incorporate disaster resilience, enabling effective action to minimize the human, social, and economic losses caused by such events.*

1. Introdução

Desastres naturais, incluindo eventos climáticos extremos como tempestades intensas, ciclones e inundações, têm tido um impacto crescente nas infraestruturas urbanas e rurais, desafiando a resiliência e a sustentabilidade de cidades inteiras [Marasco et al. 2022]. A intensidade e a frequência desses eventos, exacerbadas pelas mudanças climáticas, podem sobrecarregar os sistemas de drenagem, danificar redes de transporte, além de comprometer a integridade dos canais de comunicação e de infraestruturas de computação. Como um exemplo muito representativo, recentemente a enchente histórica no Rio Grande do Sul afetou a infraestrutura da região metropolitana de Porto Alegre e de diversas outras

partes do estado. Nos primeiros cinco dias de chuvas já havia mais de 400 mil pontos sem energia elétrica, pelo menos 186 municípios sem sinal de internet e telefone e mais de 1 milhão de residências sem abastecimento de água [BBC 2024].

Sistemas computacionais e de comunicação para monitoramento e de alerta rápido, como os utilizados para avisar populações locais sobre a ocorrência de *tsunamis*, furacões ou enchentes repentinas, devem operar com extrema rapidez e precisão. Falhas nesse tipo de sistema ou mesmo o atraso em minutos, ou em certos casos até mesmo segundos, pode significar a diferença entre vidas salvas ou perdidas. Esses sistemas precisam ser robustos o suficiente para funcionar mesmo quando parte da infraestrutura está comprometida pelo próprio desastre, o que implica na necessidade de soluções distribuídas, redundantes e com capacidades de autossuficiência energética e de capacidade processamento de dados.

Além dos sistemas específicos para monitoramento e alerta de desastres, a própria infraestrutura básica de comunicação, tanto para as populações em risco quanto para as equipes de resgate, deve manter-se disponível a todo momento. No entanto, durante um desastre, essa comunicação é frequentemente interrompida, seja pela destruição das torres de celular, pela falha no fornecimento de energia ou pela ruptura de cabos de transmissão. Ademais, durante um desastre, o volume de dados gerados e processados aumenta significativamente. Sensores ambientais, dispositivos de monitoramento e sistemas de alerta rápido são acionados simultaneamente, sobrecarregando redes e servidores. Adicionalmente, a conectividade da população com esses sistemas, seja para obter informações vitais ou para solicitar ajuda, cria um aumento abrupto na demanda de comunicação, que muitas vezes não foi dimensionada para lidar com picos tão elevados.

Neste contexto, surge o grande desafio de desenvolver sistemas de computação e comunicação que incorporem a resiliência a desastres de forma sistemática. Resiliência pode ser entendida como a capacidade de lidar com, e superar, situações adversas. Estratégias de resiliência podem tipicamente envolver etapas ativas (antecipação e preparação) e reativas (detecção e mitigação) e empregam princípios como redundância, diversidade, conectividade e associação [Sterbenz et al. 2010]. Nesse documento, defendemos que um dos Grande Desafios a serem superados é a capacidade de desenvolver e utilizar mecanismos e técnicas computacionais para promover resiliência de uma forma sistemática, especialmente em situações de desastres naturais. Soluções emergenciais, como redes móveis temporárias, satélites e drones equipados com estações rádio base, podem ser exploradas para garantir a continuidade dos serviços. O uso de tecnologias emergentes, como inteligência artificial e aprendizado de máquina, podem também potencialmente otimizar a alocação de recursos e a priorização de tarefas durante as fases críticas de um desastre, aumentando a eficácia das ações de resposta. Por fim, ressalta-se que esse desafio está alinhado ao manifesto "Tecnologias Digitais para o Meio Ambiente" aprovado na assembleia da SBC em 2022 [Sociedade Brasileira de Computação 2022], o que reforça uma demanda já expressa recentemente pela comunidade.

2. Resiliência: Um Modelo Conceitual de Referência

Resiliência é uma noção aplicável a diversas situações, e denota a capacidade de "se recuperar" em ou após situações adversas. Qualquer estratégia para resiliência terá um conjunto familiar de etapas que são basicamente ativas (antecipação e preparação) e re-

ativas (detecção e mitigação). O modelo conceitual [Dobson et al. 2019] descrito nesta seção fornece orientação sobre o projeto e a operação de um sistema resiliente, aplicando princípios como redundância, diversidade, conectividade e associação. Ele captura os principais componentes do processo de resiliência, dentro de um *loop* de controle *online* e de um *loop offline* denotado por D^2R^2+DR, conforme mostrado na Figura 1.

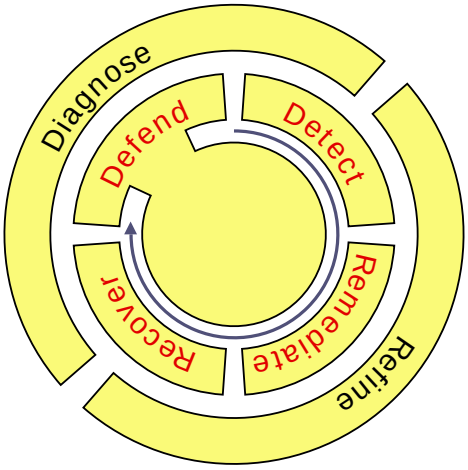

Figura 1. Modelo conceitual de resiliência D^2R^2+DR [Dobson et al. 2019]

A primeira parte interna da figura, representada por D^2R^2, especifica um *loop* de controle em tempo real: *defender*, *detectar*, *remediar*, *recuperar*. O centro do círculo denota defesas estruturais, como caminhos redundantes geodiversos. A primeira parte do *loop* de controle consiste em defesas operacionais ativas, por exemplo, mecanismos de proteção previamente instalados. Caso uma situação adversa ocorra e passe pelas defesas, a detecção precisa identificar e sinalizar a ameaça. Os mecanismos de remediação são, então, aplicados para garantir o melhor serviço possível durante um evento adverso em andamento (como uma sobrecarga operacional, uma falha ou um ataque) ou após um evento que destruiu partes da infraestrutura (como um desastre em larga escala). Por exemplo, o tráfego pode ser redirecionado em torno de áreas de infraestrutura com falha. Finalmente, a recuperação retorna a infraestrutura (no exemplo, de rede) às operações normais assim que o evento adverso cessar e os elementos de infraestrutura com falha forem reparados. O *loop* externo DR, *diagnose* e *refinement*, representa um controle não em tempo real por meio do qual os aspectos de infraestrutura relacionados à resiliência, bem como as estratégias operacionais, são analisados e aprimorados, refletindo as experiências e os desenvolvimentos de longo prazo dentro do ambiente.

3. Desastres e Adversidades: o Estudo de Caso da Grande Enchente no RS

Nos meses de abril e maio de 2024, fortes chuvas atingiram o estado do Rio Grande do Sul. A cheia dos cinco rios do interior do estado que deságuam no lago Guaíba[1] que banha a capital Porto Alegre levou a uma elevação histórica do nível das águas (Figura 2), que superou o nível observado na, até então, maior enchente de 1941. Os impactos foram sem precedentes: mais da metade dos bairros de Porto Alegre foram inundados; 70% da população da cidade ficou sem abastecimento de água devido à inundação de estações de

[1]Popularmente conhecido como rio Guaíba, tecnicamente trata-se de um lago e não de um rio.

(a) Antes **(b) Depois**

Figura 2. Imagens de satélite mostrando a elevação do nível das águas em maio de 2024 [MetSul 2024]

tratamento de água; 19 das 23 estações de bombeamento de água que deveriam eliminar a água da enchente deixaram de operar; muitos bairros ficaram sem luz; o aeroporto Salgado Filho interrompeu suas operações, e as principais rodovias de acesso à cidade foram alagadas [Ling and Inglês 2024]. A infraestrutura de comunicação de dados foi severamente afetada, uma vez que antenas 5G de alcance limitado ficaram inoperantes (sendo necessário, quando possível, o uso de tecnologias "legadas" de 3G ou inferiores). O maior *datacenter* de Porto Alegre, que está localizado em uma área que foi completamente alagada, teve sua operação muito dificultada. Além disso, o Centro de Tecnologia da Informação e Comunicação do Estado do Rio Grande do Sul (PROCERGS) e a Companhia de Processamento de Dados de Porto Alegre (PROCEMPA) tiveram sua operação paralisada ou em nível de grande contingência. Esses múltiplos eventos "em cascata" levaram ao colapso do funcionamento da cidade e da região por mais de trinta dias, acarretando a morte de centenas de pessoas e a prejuízos incalculáveis.

Posicionando lado-a-lado o estudo de caso recém referido e o modelo conceitual de resiliência D^2R^2+DR introduzido na Seção 2, podemos realizar, de maneira simplificada, o seguinte *enquadramento*. A cidade de Porto Alegre conta com um sistema contra inundação construído na década de 1970. O sistema de proteção consiste de um conjunto de mecanismos de defesa, incluindo diques, comportas e casas de bombeamento, além de um muro que atinge 6m acima do nível do mar. No entanto, os mecanismos que deveriam realizar a *defesa* quanto a ameaças previamente antecipadas falharam: a água do Guaíba vazou por comportas que se romperam e inundou as casas de bombas que deveriam eliminar a água. Mecanismos de *detecção* como sensores que medem o nível de elevação do Guaíba e sistemas de monitoramento igualmente falharam ou produziram resultados inconsistentes. As etapas de *mitigação* envolveram a evacuação de bairros inteiros e tentativas de contenção da água que transbordava através do uso de sacos de areia. Ainda, nesta etapa, podemos incluir o desligamento preventivo de um dos datacenters da PROCEMPA [Procempa 2024] e o uso de infraestruturas alternativas de sensoriamento do nível da água [CORREIO DO POVO 2024]. Mais de três meses após o incidente, ações de *recuperação* ainda persistem, ao passo que diversos bairros ainda passam por reconstrução e retomada. A médio prazo, ações de *diagnóstico* e *refinamento* precisarão ser tomadas, incluindo reforços nas barreiras de proteção (*e.g.*, comportas, di-

ques e estações de bombeamento) e o aprimoramento dos sistemas de monitoramento, alerta e protocolos de resposta a incidentes.

4. Desafios, Áreas Habilitadoras e Oportunidades

A área de Computação tem muito a contribuir na prevenção e no gerenciamento de desastres como o relatado anteriormente, seja de forma direta ou indireta. A seguir, são discutidos desafios e oportunidades de pesquisa em um conjunto amplo de áreas da Computação.

Tecnologias de comunicação. *Desafio:* Devido a seu baixo alcance e posicionamento, parte da infraestrutura de 5G foi destruída durante as fortes chuvas e enchente. Além disso, em certas regiões as operadoras de telefonia tiveram sua operação completamente comprometida. *Oportunidade:* Tecnologias legadas como 3G assumiram o papel, e empresas de telefonia estabeleceram acordos para permitir que clientes de empresas concorrentes compartilhassem a infraestrutura de comunicação. Em certas localidades que ficaram sem cobertura, Mobile Ad Hoc Networks (MANETs) poderiam ter sido utilizadas se as soluções estivessem implementadas nos celulares dos moradores [Safari et al. 2023]. Contudo, o cenário de desastres naturais demanda MANETs com características até então não contempladas, requerendo avanços de pesquisa substanciais. Aspectos abertos a investigação incluem: *trade-off* entre comunicação em padrões mínimos e eficiência energética; interfaceamento oportunístico com a Internet (por subconjunto de equipamentos 3G operacionais ou via poucos pontos-chave em que haja tal comunicação disponível); estratégias inovadoras de monitoramento e teste de infraestruturas que, em tese, só serão ativadas em meio a crises; aplicações projetadas para comunicações de emergência e de uso simplificado (requisito particularmente importante em países como os do Hemisfério Sul em que a população é menos "educada" para episódios de catástrofe).

Infraestruturas de TIC. *Desafio:* Com o alagamento de bairros inteiros, a estrutura física de *datacenters* e de outras infraestruturas críticas de computação foram comprometidas, causando interrupção de serviços. *Oportunidade:* Aspectos para pesquisa nos próximos dez anos incluem, por exemplo, modelagem dessas infraestruturas e verificação formal de requisitos de resiliência em situação de catástrofe; e projeto de estratégias "agressivas" de migração e provisionamento sob demanda de infraestruturas de rede e computação, com preservação de estado e usando, como ponto de partida, funcionalidades básicas oferecidas por tecnologias de virtualização.

Sensoriamento e ciência de dados. *Desafio:* Coleta em tempo real de dados de monitoramento da infraestrutura física de proteção (níveis das águas, integridade das comportas, operação dos diques) e o pré-processamento dessas informações. *Oportunidade:* Redes de sensores (ambientais, hidrológicos, etc) podem ter um papel crucial no aprimoramento dos sistemas de monitoramento e emissão de alertas, utilizando técnicas para acompanhamento de tendências e mudanças em variáveis críticas para antecipar possíveis desastres [Ray et al. 2017]. Apesar de décadas de pesquisa na área, desastres naturais elevam os requisitos observados até agora em ambientes como os de *smart cities*, demandando pesquisa básica e aplicada em: projeto de dispositivos robustos;

métodos computacionais inovadores capazes de "compensar" coletas incompletas e falhas; mecanismos para processamento de grandes volumes de dados em tempo "quase real"; modelos preditivos acurados de fenômenos bastante "caóticos"; projeto de ferramentas e mecanismos de visualização para apoiar a tomada rápida de decisão; e integração com atuadores visando à automação de determinadas ações, eliminando humanos "desesperados" e despreparados de parte do processo de remedição.

Planejamento, robótica e drones. *Desafio:* A dificuldade de acesso a áreas alagadas e a escassez de embarcações da defesa civil dificultaram as ações de resgate. *Oportunidade:* O uso de drones em ações de resgate oferece diversas oportunidades de pesquisa, como o desenvolvimento de algoritmos para mapeamento em tempo real de áreas afetadas combinado com algoritmos de processamento de imagens para localizar sobreviventes [Shaheen et al. 2023]. A pesquisa pode incluir o planejamento de rotas de entrega eficientes para suprimentos em locais de difícil acesso e o emprego de drones para estabelecer redes de comunicação temporárias em áreas impactadas [Flores 2024]. Além disso, a integração de sensores para monitorar condições ambientais e o avanço em técnicas de inteligência artificial para analisar dados e tomar decisões rápidas são áreas promissoras.

5. Métricas de Avaliação

Para avaliar o progresso de soluções computacionais voltadas à resiliência frente a desastres, é essencial definir métricas claras, contextualizadas e multidimensionais:

- Do ponto de vista *técnico-operacional*, o tempo médio de resposta a emergências, a cobertura de sensores e redes de comunicação, e a precisão de modelos preditivos são fundamentais. Também devem ser observados aspectos como dependabilidade, confiabilidade e tolerância a falhas [Macêdo et al. 2023], que são temas correlatos tratados em sistemas críticos.
- Na dimensão *social*, métricas como número de pessoas alcançadas por sistemas de alerta, tempo médio de evacuação em áreas de risco e o grau de inclusão digital da população usuária são cruciais para medir o impacto humano.
- A *sustentabilidade* das soluções pode ser avaliada por indicadores como o custo por área atendida, a capacidade de operar em ambientes com infraestrutura limitada e o tempo necessário para implantação.

Por fim, indicadores qualitativos, como a confiança da população nas tecnologias, o engajamento em treinamentos e a coleta de feedback por plataformas participativas, complementam a avaliação. Essas métricas, quando combinadas, permitem um acompanhamento estruturado do impacto e da efetividade das soluções.

6. Conclusões

Diante dos desafios enfrentados pelo Brasil frente a desastres naturais cada vez mais frequentes e severos, as diversas áreas da Computação oferecem oportunidades únicas para tornar nossa sociedade mais resiliente. Tecnologias de comunicação tolerantes a falhas, redes ad hoc emergenciais, sensores ambientais robustos, infraestruturas computacionais

adaptativas e o uso de inteligência artificial para previsão e tomada de decisão são apenas alguns exemplos de ferramentas que podem ser desenvolvidas ou adaptadas para o contexto brasileiro.

No entanto, é fundamental que essas tecnologias sejam pensadas de forma contextualizada, levando em conta as particularidades socioeconômicas, geográficas e infraestruturais do país. Isso inclui desde o desenvolvimento de soluções acessíveis e usáveis por populações vulneráveis até a adaptação de tecnologias internacionais – como drones de resgate, modelos de previsão com aprendizado de máquina, ou redes de sensores para cidades inteligentes – à nossa realidade. Investir em pesquisa aplicada, formação interdisciplinar e parcerias com órgãos públicos e defesa civil é essencial para transformar essas oportunidades em soluções concretas e eficazes para o Brasil.

Referências

BBC (2024). A cronologia da tragédia no rio grande do sul. BBC News Brasil: https://www.bbc.com/portuguese/articles/cd1qwpg3z77o. Acessado em setembro de 2024.

CORREIO DO POVO (2024). Sistema de monitoramento dá suporte nas enchentes de porto alegre. https://www.correiodopovo.com.br/not%C3%ADcias/chuvasnors/sistema-de-monitoramento-d%C3%A1-suporte-nas-enchentes-de-porto-alegre-1.1490745.

Dobson, S., Hutchison, D., Mauthe, A., Schaeffer-Filho, A., Smith, P., and Sterbenz, J. P. G. (2019). Self-organization and resilience for networked systems: Design principles and open research issues. *Proceedings of the IEEE*, 107(4):819–834.

Flores, H. (2024). Opportunistic multi-drone networks: Filling the spatiotemporal holes of collaborative and distributed applications. *IEEE Internet of Things Magazine*, 7(2):94–100.

Ling, A. and Inglês, R. (2024). Como porto alegre ficou debaixo d'água. Folha de São Paulo: https://www1.folha.uol.com.br/cotidiano/2024/05/como-porto-alegre-ficou-debaixo-dagua.shtml. Acessado em agosto de 2024.

Macêdo, R. J., de Sá, A. S., Freitas, A. E. S., Veríssimo, P. E., Gorender, S., and de Sá, M. O. S. (2023). *42a Jornada de Atualização em Informática*, chapter Confiabilidade e Segurança nos Sistemas Distribuídos Físico-Digitais. SBC. https://doi.org/10.5753/sbc.12853.0.2.

Marasco, S., Kammouh, O., and Cimellaro, G. P. (2022). Disaster resilience quantification of communities: A risk-based approach. *International Journal of Disaster Risk Reduction*, 70:102778.

MetSul (2024). Imagens de satélite mostram enchente arrasadora na grande porto alegre. https://metsul.com/imagens-de-satelite-mostram-enchente-arrasadora-na-grande-porto-alegre/.

Procempa (2024). Procempa mantém operações apesar de alagamento. https://prefeitura.poa.br/procempa/noticias/procempa-mantem-operacoes-apesar-de-alagamento.

Ray, P. P., Mukherjee, M., and Shu, L. (2017). Internet of things for disaster management: State-of-the-art and prospects. *IEEE Access*, 5:18818–18835.

Safari, F., Savić, I., Kunze, H., Ernst, J., and Gillis, D. (2023). A review of ai-based manet routing protocols. In *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 43–50.

Shaheen, M. M. Z., Amer, H. H., and Ali, N. A. (2023). Robust air-to-air channel model for swarms of drones in search and rescue missions. *IEEE Access*, 11:68890–68896.

Sociedade Brasileira de Computação (2022). Tecnologias digitais para o meio ambiente: Manifesto SBC. coordenação de Marcelo Rita Pias e Raimundo José de Araújo Macêdo. 10.5753/sbc.rt.2022.07.01.

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., and Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245 – 1265. Resilient and Survivable networks.