SISTEMA DISTRIBUÍDO DE MONITORAMENTO DE REDE PARA PREVISÃO DE DESASTRE

Regina Melo Silveira[1], Rafael Pasquini[2], Luciana Arantes[3] e Pierre Sens[3]
[1]*Escola Politécnica da Universidade de São Paulo, SP, Brasil*
[2]*Universidade Federal de Uberlândia, Minas Gerais, Brasil*
[3]*Sorbonne Université, CNRS, INRIA, LIP6, Paris, França*

RESUMO

O uso de sistema de monitoramento para áreas de risco tem aumentado significativamente, especialmente com o uso de aplicações de IoT. No entanto, as situações de risco devido a desastres naturais podem causar mal funcionamento das redes de comunicação inviabilizando tal monitoração. Por este motivo, outros métodos de identificação de desastres precisam ser desenvolvidos, o que tem impulsionado os sistemas de Aviso Antecipado (ou *Early Warning*), que conseguem verificar uma situação anômala com antecedência. Neste trabalho propomos um mecanismo de detecção de desastres a partir da monitoração distribuída do sinal da rede fatiada. A arquitetura do sistema é elaborado baseado na arquitetura NECOS e um levantamento de possíveis métodos para a automação do sistema é apresentado.

PALAVRAS-CHAVES

Previsão de Desastres, Monitoramento Distribuído, *Early Warning*, Rede Fatiada (*Sliced Networking*)

1. INTRODUÇÃO

Todos os anos, várias regiões do planeta são atingidas por desastres naturais como terremotos, furacões, tsunamis, abalos sísmicos, inundações, incêndios e deslizamentos de terra, causando um grande prejuízo humano e econômico. As atuais tecnologias de redes de comunicação e as tecnologias voltadas para Internet das Coisas (IoT - *Internet of Things*) têm potencializado e impulsionado inúmeras aplicações, incluindo as para monitoração, com grande benefício para a sociedade. No entanto, vários desafios ainda devem ser superados para garantir que estes serviços funcionem adequadamente.

A falta de comunicação devido a um desastre dificulta, ou até impossibilita, a divulgação do evento, e consequentemente a ativação de ações de resgate. Portanto, a necessidade de projetar e implantar mecanismos de detecção de falhas em redes tem-se mostrado primordial para situações de risco, em desastres naturais ou eventos provocados que colocam em risco a vida humana ou o meio ambiente (Gomes et al., 2016).

Devido a estas constatações, está surgindo um novo campo de pesquisa denominado Aviso Antecipado (do inglês, *Early Warning*) (Esposito et al., 2022). E uma maneira não ortodoxa de fazer previsão de desastre antecipado é a partir do monitoramento do funcionamento de uma rede de comunicação. Na ocorrência de algum evento que cause deterioração do sinal de comunicação, como por exemplo, a queda de um prédio que bloqueia o sinal de uma rede sem fio, a avaria de um dos equipamentos de rede ou o rompimento parcial de uma fibra óptica, o desempenho da rede poderá ser utilizado como um parâmetro de identificação precoce do evento. A alta capacidade de mineração e processamento de dados, advindos dos mecanismos de *Big Data*, e a capacidade de automação de processos, utilizando inteligência artificial e aprendizado de máquina, viabilizam o *Early Warning*.

O projeto ADMITS tem como objetivo a criação de métodos de análises de dados de forma distribuída para gerenciamento do sistema de informação, de tal forma que seja possível fazer previsão de uma situação crítica. Para tanto, considera-se uma arquitetura com implementação de fatiamento (*Sliced Network*), baseado nos paradigmas de Redes Definidas por Software (SDN - *Software Defined Network*) e Funções de Rede Virtualizadas (NFV - *Network Function Virtualization*). Neste trabalho é proposto a flexibilização desta arquitetura de rede fatiada, de forma que agentes de monitoração possam ser estrategicamente instalados no módulo de orquestração de cada domínio de rede, fazendo a monitoramento da rede de forma distribuída.

2. AMBIENTE DE REDE

Atualmente, várias tecnologias de rede prevêem a utilização de fatiamento de rede. Tal técnica é considerada a chave para o atendimento a milhões de conexões concorrentes, que utilizam a mesma infraestrutura de rede, sem no entanto gerar competição entre as mesmas. Isto acontece pois este fatiamento permite criar uma instância da rede, com alocação de recursos exclusivos, com garantia de isolamento de tráfego e flexibilidade para atender conexões fim-a-fim com diferentes requisitos.

A técnica de fatiamento em uma rede traz como principais benefícios o isolamento e a flexibilidade, podendo ser implantada fim-a-fim ou em segmentos específicos da rede (Afolabi et al., 2018). O modelo fim-a-fim prevê que a fatia seja configurada na entrada da rede, configurando de acordo com os requisitos de QoS e SLA contratado. O fatiamento pode ser oferecido pelo provedor de infraestrutura de rede (NP - *Network Provider*) como um serviço, NSAAS (*Network Slice As A Service*) (Clayman et al, 2021), e pode ser gerenciado pelo próprio NP ou pelo provedor de serviço (*Internet Service Provider*).

Este projeto se baseia na arquitetura NECOS (Farias et al., 2019), que apresenta como vantagens: i) ser uma arquitetura bastante generalista, permitindo portanto seu acoplamento à diversas tecnologias de rede, como 5G, IEEE 802.16 ou ainda tecnologias ópticas como WDM; ii) ser uma arquitetura softwarizada, que permite integração com funções SDN; iii) ser baseada em fatiamento de rede e NFV, o que permite garantia de reserva de recursos fim-a-fim; e iv) ser uma arquitetura distribuída, onde *Slice Agents* instalados em diferentes setores da rede (borda, rede e núcleo), e em diferentes domínios, participam da administração e orquestração das fatias, para garantir o bom desempenho fim-a-fim.

Então, considerando a arquitetura NECOS (Farias et al., 2019), temos um *Slice Orchestrator* e o IMA (*Infrastructure & Monitoring Abstraction*) que através da interface *northbound* monitora o ciclo de vida da fatia. A figura 1a ilustra a arquitetura NECOS e seus módulos.

A princípio a rede fatiada, implementada utilizando instanciação de rede, tem recursos garantidos a partir da reserva antecipada dos mesmos, antes do início do envio dos dados. Sendo assim, qualquer distúrbio da rede que não atenda o QoS e o SLA especificados, com certeza não ocorreu devido a competição por recursos, como é o caso em redes não fatiadas (Yu et al., 2020). Sendo assim, é possível inferir que tal distúrbio seja causado por algum evento externo a rede, podendo caracterizar um desastre.

3. TRABALHOS CORRELATOS

Alguns projetos de pesquisa têm explorado a questão da detecção da falha de uma rede de comunicação com diferentes objetivos e propósitos. Considerando sistemas distribuídos, Rossetto (Rossetto et al., 2018) propôs um detector de falhas não confiável, chamado de Impact FD, onde um nó monitora um conjunto de nós (sensores, dispositivos, processos), e o oráculo FD do nó monitor envia a indicação de confiança em relação ao conjunto de nós monitorados como um todo e não para cada um desses nós. Já no trabalho de Gomes (Gomes et al., 2016) são discutidas as questões de vulnerabilidade da rede em caso de disruptura devido a desastres, propondo um algoritmo de roteamento resiliente a estes eventos.

No escopo de *Early Warning*, Esposito et al. (2022) faz um levantamento de como a infraestrutura de IoT pode ser utilizada para Aviso Antecipado, utilizando quatro casos de estudos: tsunami, inundação, terremoto e deslizamento de terra. O trabalho é bem extenso e completo, mas se restringe a aplicações de IoT, como monitoração e vigilância, salientando as vulnerabilidades deste tipo de serviço em termos de recuperação e restrição de recursos.

A proposta feita aqui traz como diferencial ser de escopo geral, independente do tipo de ocorrência, e consegue se antecipar a qualquer sistema de monitorização ou vigilância do ambiente de risco.

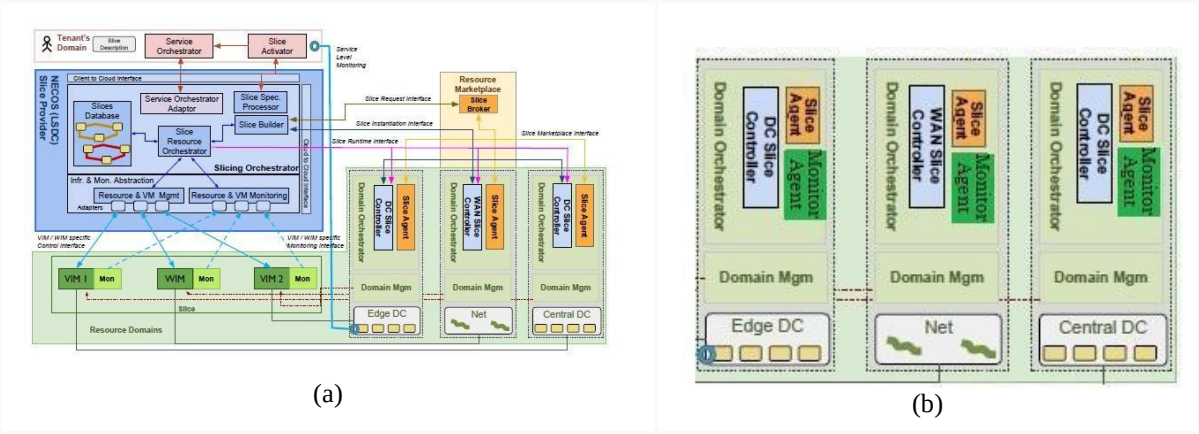

Figura 1. (a) Arquitetura NECOS (Farias et al., 2019); (b) Visão Parcial da Arquitetura NECOS mostrando a inclusão do Agente Monitor Distribuído. Modificado de (Farias et al., 2019)

4. ARQUITETURA DISTRIBUÍDA PARA MONITORAMENTO

Para que o monitoramento da rede fim-a-fim possa ser realizado, com identificação de casos de falha devido a desastres, é necessário elaborar uma arquitetura distribuída com monitoração ativa. Para isso, um agente de monitoramento (MA) foi adicionado na arquitetura NECOS, como mostra a figura 1b, que deve estar ativo em pontos específicos, no elemento orquestrador de cada domínio.

A arquitetura distribuída proposta neste trabalho não atenderá todas as conexões, mas somente as conexões com requisitos específicos de suporte a aplicações de risco. Portanto, considera-se que há um estado da rede em que esse serviço de monitoração é solicitado a partir da negociação do serviço, baseado nos critérios de SLA.

O MA deve utilizar algoritmos de análise de dados em tempo real que devem ser projetados para executar com eficiência, oferecendo ganho de tempo em relação à dispositivos IoT de monitoramento de áreas de risco. Desta forma, é possível obter resposta rápida em situações críticas e disparar sinal de alerta em caso de desastre. Técnicas que envolvam processo de aprendizagem devem ser utilizadas para melhorar o desempenho do agente, tornando-se adaptativo e mais imune a falsos positivos.

4.1 Mecanismos de Automação

A detecção de falhas de uma rede pode ser realizada através da análise de seu desempenho e degradação do serviço de transmissão. Este mecanismo deve ser reativo, ou seja, assim que é detectada a falha, uma ação deve ser tomada imediatamente. Quanto menor o tempo entre a detecção e a ação, maiores as chances de prevenção e reversão da situação. Sendo assim, este mecanismo de detecção deve ser realizado de forma automática.

Vários mecanismos têm sido propostos na literatura para a automatização de uma detecção de falha em rede. Estes utilizam parâmetros da rede, como atraso ou perda de pacotes, para verificar seu comportamento. Como descreve Nassif et al. (2021) aprendizado por máquina (ML - *Machine Learning*) tem se mostrado eficiente na detecção de anomalias e falhas de comportamento de redes. Entre as possibilidades de uso de ML para a identificação de falha está o método de Classificação, que pode ser implementado na forma de aprendizado supervisionado (Boutaba et al., 2018), utilizando os parâmetros de QoS como valores alvo.

Como descreve Kwon et al. (2017), outros métodos de ML também usados para detecção de falhas em rede são os métodos de Aprendizagem Profunda (DL - *Deep Learning*), considerando nesta linha os seguintes algoritmos: Máquina de Boltzmann Restrita (RBM), Máquina de Boltzmann Profunda (DBM), Rede Neural Profunda (DNN) e Rede Neural Recorrente (RNN).

5. CONSIDERAÇÕES FINAIS

Este artigo propõe uma arquitetura que utiliza agentes de monitoração para a detecção de falhas em uma rede de comunicação com o objetivo de prever a ocorrência de algum desastre em região de risco. A proposta se baseia no fato de que a verificação de alguma anomalia na rede é mais eficiente do que a monitorização ou vigilância de sistemas de IoT. Esta proposta só é factível com o uso de técnicas de fatiamento de rede, onde os recursos são garantidos com isolamento e sem concorrência com outras conexões. A proposta utiliza como arquitetura base a plataforma NECOS, que prevê o fatiamento de rede e a possibilidade de integração com várias tecnologias de rede.

Como trabalhos futuros será feita uma análise detalhada dos métodos de detecção da falha da rede, avaliando-os através de simulação, para a definição do melhor mecanismo a ser utilizado no sistema.

AGRADECIMENTOS

Este trabalho foi parcialmente financiado pelo projeto STIC AMSUD - COOPERAÇÃO EM CIÊNCIA E TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO FRANÇA - AMÉRICA DO SUL - CAPES/CDEFI - 88887.697040/2022-00.

REFERÊNCIAS

Afolabi, Ibrahim, et al. "Network slicing & softwarization: A survey on principles, enabling technologies & solutions." IEEE Communications Surveys & Tutorials (2018).

Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. Journal of Internet Services and Applications, 9(1), 1-99.

Clayman, S., Neto, A., Verdi, F., Correa, S., Sampaio, S., Sakelariou, I., ... & Serrat, J. (2021). The necos approach to end-to-end cloud-network slicing as a service. IEEE Communications Magazine, 59(3), 91-97.

Esposito, M., Palma, L., Belli, A., Sabbatini, L., & Pierleoni, P. (2022). Recent Advances in Internet of Things Solutions for Early Warning Systems: A Review. Sensors, 22(6), 2124.

ETSI TS 128 530 V17.2.0 (2022-05) - 5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 version 17.2.0 Release 17) https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf

Farias, F., Pinheiro, B., Abelém, A., Maciel Jr, P., Rocha, A., Verdi, F., ... & Rothenberg, C. (2019, May). Projeto NECOS: Rumo ao Fatiamento Leve de Recursos em Infraestruturas de Nuvens Federadas. In Anais do X Workshop de Pesquisa Experimental da Internet do Futuro (pp. 56-63). SBC.

Gomes, T., Tapolcai, J., Esposito, C., Hutchison, D., Kuipers, F., Rak, J., ... & Tornatore, M. (2016, September). A survey of strategies for communication networks to protect against large-scale natural disasters. In 2016 8th international workshop on resilient networks design and modeling (RNDM) (pp. 11-22). IEEE.

Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). *A survey of deep learning-based network anomaly detection*. Cluster Computing, 22(1), 949-961.

Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). *Machine learning for anomaly detection: A systematic review*. Ieee Access, 9, 78658-78700.

Pasquini, R., Miani, R. S., Coelho, P. R., Neto, A. V., Hidalgo, N., Gutiérrez, M., ... & Grampín, E. (2020, June). *ADMITS: Architecting Distributed Monitoring and Analytics in IoT-based Disaster Scenarios*. In Anais do XII Simpósio Brasileiro de Computação Ubíqua e Pervasiva (pp. 11-20). SBC.

Rossetto, A., Geyer, C., Arantes, L., and Sens, P.. Impact fd: An unreliable failure detector based on process relevance and confidence in the system. Computer Journal, To be published, 2018.

Yu, H., Musumeci, F., Zhang, J., Tornatore, M., & Ji, Y. (2020). Isolation-aware 5G RAN slice mapping over WDM metro-aggregation networks. Journal of Lightwave Technology, 38(6), 1125-1137.