Distributed Novelty Detection at the Edge for IoT Network Security

Luís Puhl Guilherme Weigert Cassales Helio Crestana Guardia Hermes Senger

Universidade Federal de São Carlos, Brasil
https://www2.ufscar.br/

August 19, 2021

Contents

Introdução - Cenário

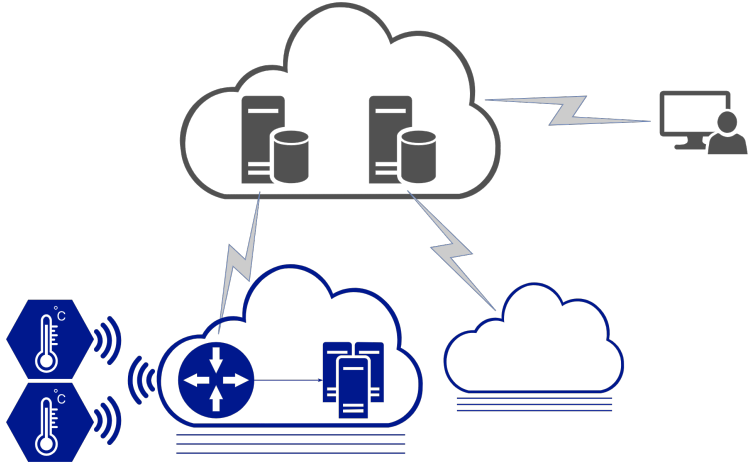


Figure: Visão geral de IoT, Névoa e Nuvem.

O autor.

Estado da Arte e Trabalhos Relacionados

Sistemas de detecção de intrusão em redes

- Ferramenta BigFlow [**?**]:
  - Sistema de detecção de intrusão por anomalia para redes de alta velocidade;
  - \+ Integração da extração dos descritores de fluxo à emissão de alarmes;
  - \+ Capacidade de tratamento de grandes volumes;
  - – Atualização semanal com avaliação de um especialista;
  - – Execução somente em nuvem.

Network Intrusion Detection based on Machine Learning is not a novel concept. The plethora of network applications and ways of exploiting them motivate using automated means to detect known and novel attacks. There are, though, open questions and challenges on this subject, such as reducing the false positive rate and detecting attacks in a timely fashion [**?**].

Resultados - Variação Processadores

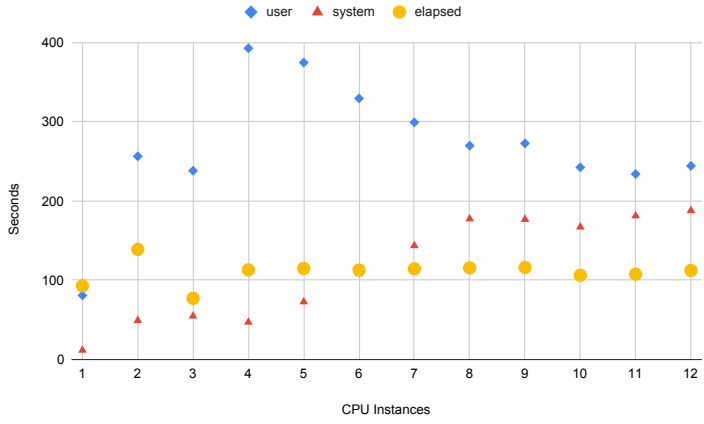


Figure: Métricas de tempo para execuções do mfog com variação no número de processadores.

O autor.

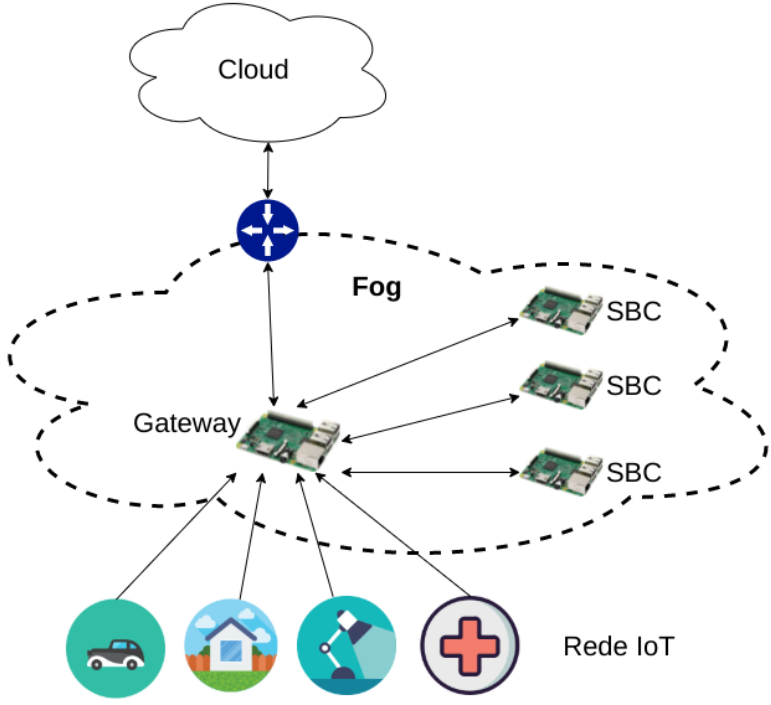
Conclusão

Resultados obtidos:

- Algoritmo minas distribuído e a arquitetura arch implementada com modificações;
- Distribuição tem pequeno efeito sobre as métricas de qualidade;
  - Maior efeito é a redução de etiquetas novidade na versão distribuída;
- Resultados mostram que a implementação mfog não atinge escala pelo CCR e eficiência;

Bibliography I

Appendix


Cloud
Fog
SBC
SBC
SBC
Gateway
Rede IoT