

Uma Implementação Distribuída em Névoa do Algoritmo de Detecção de Novidade em Fluxos de Dados MINAS

Luís Henrique Puhl de Souza

Orientador: Prof. Dr. Hermes Senger

Fevereiro 2020

Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Departamento de Computação

Programa de Pós-Graduação em Ciência da Computação

1. Introdução
2. Fundamentos
3. Estado da Arte e Trabalhos Relacionados
4. Proposta
5. Resultados Preliminares
6. Considerações Finais

Introdução

- Crescimento do número de dispositivos IoT e riscos associados;
- Detecção de intrusão em redes por novidade
- Um sistema para detecção de intrusão em Redes IoT implementando em névoa
- A hipótese do trabalho é que o algoritmo MINAS pode ser distribuído em nós de nuvem e névoa reduzindo a latência e com pouco comprometimento na qualidade de detecção.

Fundamentos

- Ambientes de computação Distribuída;
- Plataformas de processamento distribuído de fluxos;
- Métodos Detecção de Novidade;

Ambientes de computação Distribuída

- Computação em Nuvem (*Cloud Computing*):

Características: Serviço sob Demanda, Amplo acesso à rede, Agrupamento de recursos, Elasticidade, Serviço mensurado;

Implementações: Nuvem privada, Nuvem comunitária, Nuvem pública, Nuvem híbrida (MELL; GRANCE, 2012).

Ambientes de computação Distribuída

- Computação de Borda (*Edge Computing*) (SHI et al., 2016):
Refere-se a qualquer recurso computacional ou de rede entre os dispositivos de borda e centro de dados hospedados em nuvem.
- Computação em Névoa (*Fog Computing*) (BONOMI et al., 2012; DASTJERDI; BUYYA, 2016):
Características: Mobilidade, Heterogeneidade, Baixa Latência, Distribuição geográfica, Alto número de nós, Interoperabilidade e federação, Uso de fluxo de dados e aplicações em tempo real (IEEE Communications Society, 2018).

Plataformas de processamento distribuído de fluxos

- Mineração de Dados e Fluxo de Dados;
- Arquiteturas *Lambda* e *Kappa*;
- *MapReduce* e *Apache Hadoop*;
- *Apache Spark*, *Resilient Distributed Dataset* e *micro-batching* para *Spark Streaming*;
- *Apache Storm*;
- *Apache Flink*;

Fundamentos

```
DataStream<String> lines = env.addSource(  
    new FlinkKafkaConsumer<> (...));  
  
DataStream<Event> events = lines.map((line) -> parse(line));  
  
DataStream<Statistics> stats = events  
    .keyBy("id")  
    .timeWindow(Time.seconds(10))  
    .apply(new MyWindowAggregationFunction());  
  
stats.addSink(new BucketingSink(path));
```

Source

Transformation

Transformation

Sink

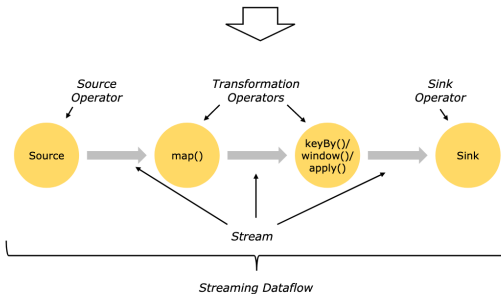


Figura 1: Exemplo de código e *data flow* do Apache Flink (Apache Flink, 2020)

Métodos Detecção de Novidade;

Estado da Arte e Trabalhos Relacionados

- Extensões do Algoritmo MINAS;
- Sistemas de detecção de intrusão em redes;

Proposta

- Plataforma de processamento distribuído;
- Arquitetura IDS-IoT;
- M-FOG e a distribuição do algoritmo MINAS;

Proposta

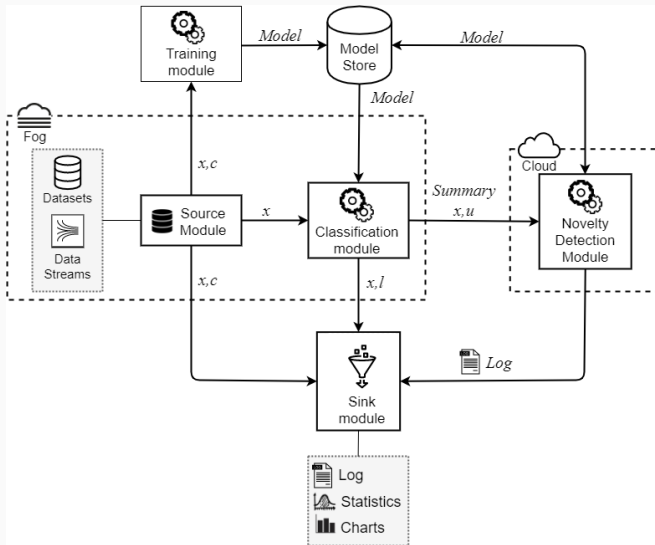


Figura 2: Arquitetura e fluxos de dados do sistema M-FOG.


Resultados Preliminares


- Python e Kafka;
- Flink;


Considerações Finais


Trabalho continua com a finalização da implementação e validação do MFOG com MINAS.


Obrigado!


 Apache Flink. *Apache Flink*. 2020. Disponível em: <https://flink.apache.org/>.

 BONOMI, F. et al. Fog computing and its role in the internet of things. In: *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. [s.n.], 2012. p. 13–16. ISBN 9781450315197. Disponível em: <http://www.lispmob.org>.

 DASTJERDI, A. V.; BUYYA, R. Fog computing: Helping the internet of things realize its potential. *Computer*, IEEE, v. 49, n. 8, p. 112–116, Aug 2016. ISSN 1558-0814.

 IEEE Communications Society. *IEEE Std 1934-2018: IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing*. IEEE, 2018. 176 p. ISBN 9781504450171. Disponível em: <https://ieeexplore.ieee.org/document/8423800>.

 MELL, P.; GRANCE, T. The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. In: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Public Cloud Computing: Security and Privacy Guidelines*. 2012. p. 97–101. ISBN 9781620819821. Disponível em: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>.

 SHI, W. et al. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, Institute of Electrical and Electronics Engineers Inc., v. 3, n. 5, p. 637–646, oct 2016. ISSN 23274662. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7488250>.

Recomendações de Leitura

empty