Detecção de malware em ambientes IoT habilitados por SDN

Cristian H. M. Souza

Carlos H. Arima

Agenda

- Introdução
- Motivação
- Visão geral da proposta
- Validação e resultados
- Conclusões e trabalhos futuros

Introdução

Introdução

- *Malwares* continuam sendo um dos principais desafios à segurança dos sistemas computacionais.

- O advento do paradigma IoT foi acompanhado pelo aumento do número de programas maliciosos com foco nas arquiteturas ARM e MIPS.

- Soluções a nível de rede que utilizam *machine learning* têm se mostrado efetivas na detecção e mitigação de *malwares*.

Introdução

- Diante do exposto, a tecnologia SDN se apresenta como uma solução viável para o desenvolvimento de soluções robustas para classificação de tráfego.

- Pesquisas recentes elevam o potencial de SDN por meio da construção de planos de dados programáveis.

- A linguagem P4 permite a implantação de soluções de segurança diretamente em *switches* programáveis.

Motivação

Motivação

- Inspirado pelo poder e flexibilidade dos *switches* programáveis, este trabalho propõe uma abordagem híbrida para detecção de artefatos maliciosos em ambientes IoT habilitados pela tecnologia SDN.

- A abordagem é composta pela detecção de assinaturas maliciosas e pela classificação do tráfego por meio de *machine learning*.

- Diferentemente das abordagens tradicionais, a solução é acoplada diretamente aos *switches* da rede, o que reduz a ocorrência de pontos únicos de falha e otimiza a utilização dos recursos presentes na infraestrutura.

Visão geral da proposta

Visão geral da proposta

- A arquitetura proposta tem como requisito a detecção agnóstica de artefatos maliciosos em ambientes IoT.

- Para se atingir esse objetivo, a solução é acoplada diretamente aos comutadores presentes na rede.

- O procedimento adotado pela solução consiste na análise e classificação do tráfego da rede.

Visão geral da proposta – Módulos

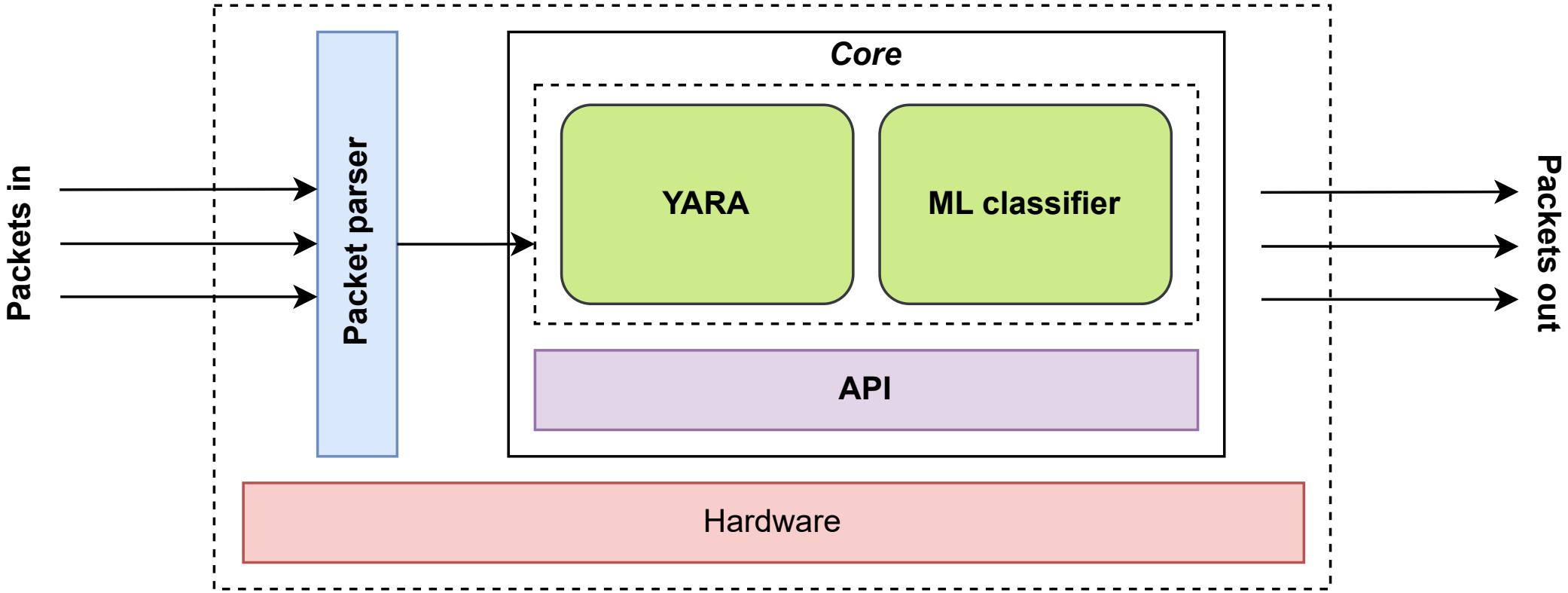
- **Packet parser:** responsável por realizar o pré-processamento dos pacotes.

- **Core – YARA:** utilizado para classificar famílias de *malware* conhecidas.
  - https://github.com/Yara-Rules/rules

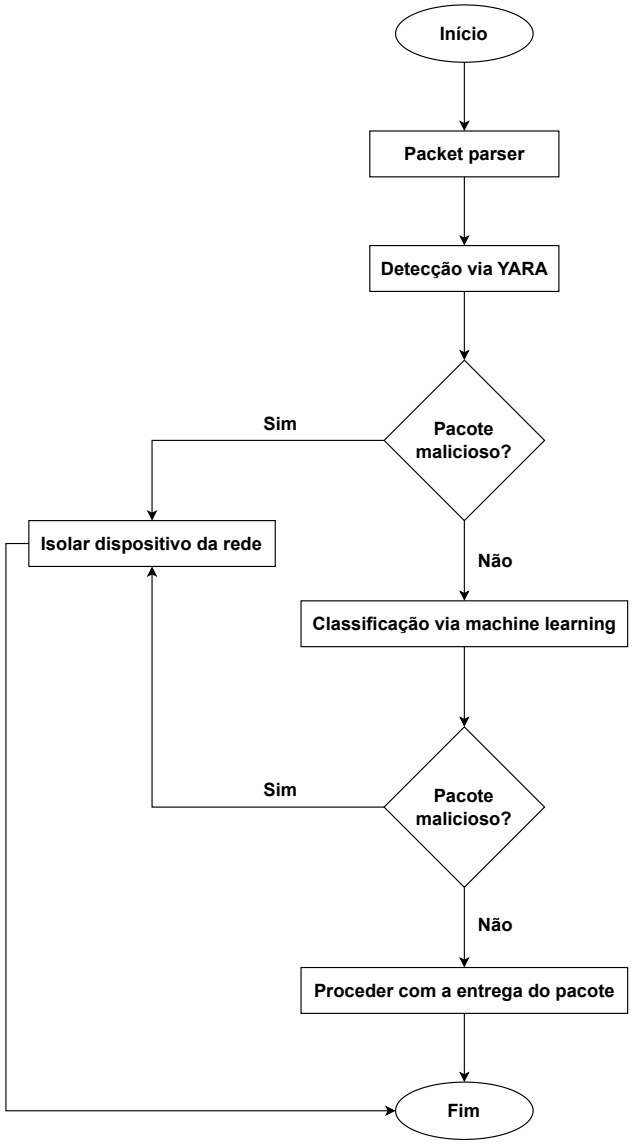
- **Core – ML classifier:** realiza a classificação de malwares desconhecidos por meio do algoritmo Random Forest.
  - Treinado com o dataset IoT-23

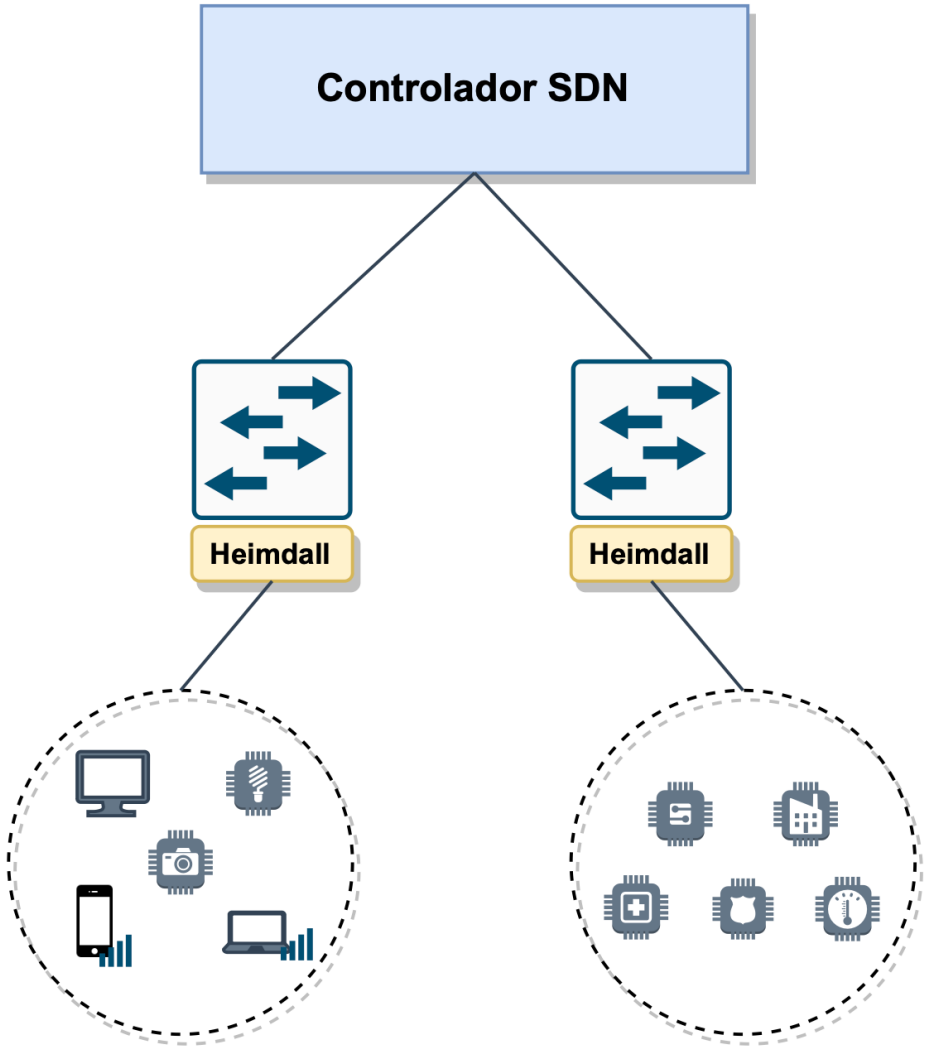
- **API:** provê uma interface de fácil gerenciamento para a solução.

Visão geral da proposta



Visão geral da proposta





Trabalhos relacionados

Proposta	Problema	Estratégia	Classificador	Dataset	Acurácia
(WOO; KIM; CHUNG, 2017)	Detecção de arquivos PE maliciosos	Análise de tráfego	CART	Indisponível	94.3%
(LETTERI; PENNA; GASPERIS, 2018)	Detecção de *botnets* em redes SDN	Análise de tráfego	MLP	HogZilla	96%
(CUSACK; MICHEL; KELLER, 2018)	Detecção de *ransomwares* a nível de rede	Análise de tráfego	Random Forest	Indisponível	87%
(MAEDA et al., 2019)	Detecção e isolamento de máquinas infectadas por *botnets*	Análise de tráfego	MLP	CTU-13 e ISOT	99.2%
(KHAN; AKHUNZADA, 2021)	Detecção de *malwares* em ambientes IoMT	Análise de tráfego	CNN e LSTM	Indisponível	99.83%
(MUTHANNA et al., 2022)	Detecção de intrusões em ambientes IoT	Análise de tráfego	Cu-LSTM-GRU	CICIDS2017	99.23%
(CHANG et al., 2022)	Detecção de *malwares* em ambientes IoT	Análise de tráfego	CNN	IoT-23	99%
(CHAGANTI et al., 2023)	Detecção de intrusões em ambientes IoT	Análise de tráfego	LSTM	SDNIoT e SDN-NF-TJ	97.1%

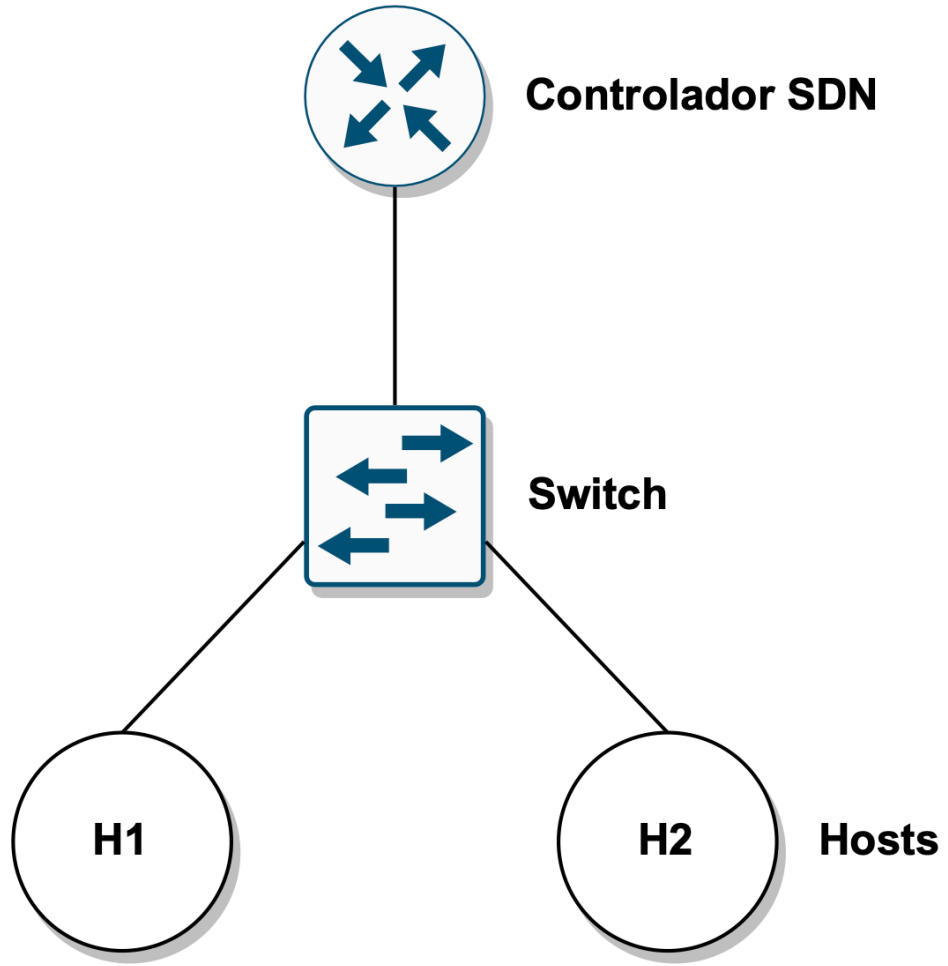
Validação e resultados

Validação e resultados

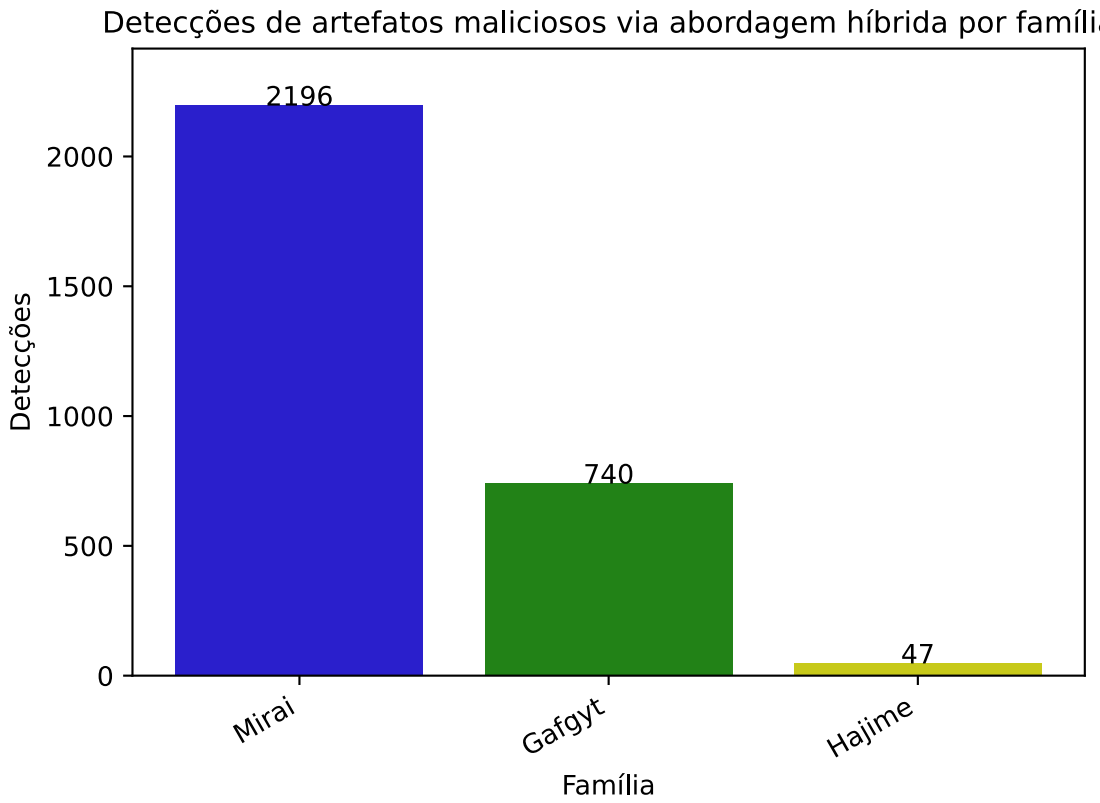
- A solução foi avaliada em uma plataforma de teste emulada por meio da ferramenta Mininet e com o uso do *software* BMv2 P4.

- A topologia utilizada para os testes consistiu em 2 dispositivos ARM emulados (H1 e H2) via QEMU, 1 *switch* programável emulado e habilitado com a solução, e 1 controlador SDN.

- 3030 artefatos reais baixados da plataforma Malware Bazaar.
  - Famílias: Mirai (2220), Gafgyt (754) e Hajime (56).

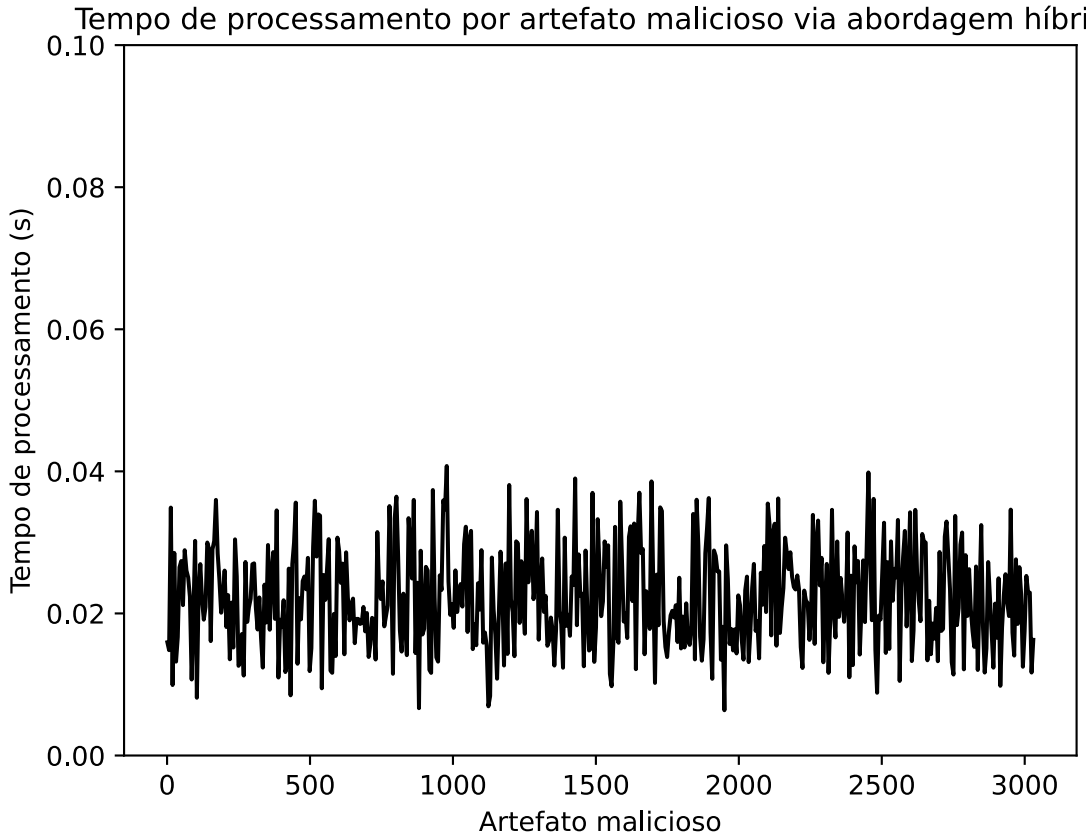


Validação e resultados



Família	Quantidade	Detectados	Taxa de detecção
Mirai	2.220	2.196	98.91%
Gafgyt	754	740	98.14%
Hajime	56	47	83.92%
Total	**3.030**	**2.983**	**98.44%**

Validação e resultados



Abordagem	**Tempo médio**	**Menor registro**	**Maior registro**	**Acurácia**
YARA	0.0218s	0.0006s	0.0399s	63%
Random Forest	0.0259s	0.0170s	0.0349s	94.12%
Híbrida	0.0217s	0.0006s	0.0347s	98.44%

Conclusões e trabalhos futuros

Conclusões e trabalhos futuros

- Este trabalho introduz uma solução para detecção de artefatos maliciosos em ambientes IoT habilitados por SDN.

- A arquitetura da ferramenta proposta se diferencia do estado da arte por fazer o uso de uma abordagem híbrida.

- Os resultados obtidos evidenciam que a abordagem híbrida proposta foi capaz de atingir uma acurácia de **98.44%** e um tempo de processamento médio de **0.0217s**.

Conclusões e trabalhos futuros

- Como trabalhos futuros, pretende-se implementar um módulo que possibilite a análise dos artefatos detectados.

- Também pretende-se avaliar a ferramenta em *switches* SDN reais, com o objetivo de determinar a eficiência da solução ao ser executada em um *hardware* dedicado.

Detecção de malware em ambientes IoT habilitados por SDN

Cristian H. M. Souza

Carlos H. Arima