

## Plan Overview

---

*A Data Management Plan created using DMPTool*

**DMP ID:** <https://doi.org/10.48321/D1148F70f1>

**Title:** Detecção e mitigação de ataques de interrupção de tráfego em redes de sensores sem fio com RPL

**Creator:** Daniel Soriano - **ORCID:** [0009-0003-4433-7844](https://orcid.org/0009-0003-4433-7844)

**Affiliation:** Universidade de São Paulo ([www5.usp.br](http://www5.usp.br))

**Principal Investigator:** Daniel Francis Soriano

**Data Manager:** Daniel Francis Soriano

**Project Administrator:** Daniel Francis Soriano

**Funder:** Universidade de São Paulo ([www5.usp.br](http://www5.usp.br))

**Template:** Template USP - Mínimo

### **Project abstract:**

Redes de sensores sem fio tem como objetivo o monitoramento de vários aspectos dos ambientes onde são instaladas. Os nós de sensoriamento transmitem os dados coletados do ambiente pelos nós vizinhos até que sejam entregues ao sorvedouro para registro e contabilização. Existem diversos ataques que podem interromper, total ou parcialmente, a coleta desses dados pelo sorvedouro, como blackhole, sinkhole e gray hole/selective forwarding. Este trabalho apresenta um framework de camada de aplicação para redes de sensores sem fio (RSSF) baseadas em RPL, que detecta e mitiga ataques de interrupção de tráfego de dados, ao mesmo tempo em que informa o sorvedouro (e os gestores da rede) sobre os nós suspeitos usando uma rota alternativa, evitando assim a interceptação e/ou interrupção pelos atacantes. A reação local faz com que os nós afetados relemos os atacantes a nós-folhas, impedindo-os de atuarem como roteadores, efetivamente mitigando os ataques. Ao concentrar a função de monitoramento ao sorvedouro, os gestores da rede conseguem identificar os nós comprometidos, e com isso removê-los fisicamente da rede.

Os experimentos realizados mostram que o framework proposto manteve a taxa de perda de pacotes próxima de 2% ou inferior na maioria dos cenários testados. Além disso, também conseguiu manter um baixo overhead de mensagem de controle (4,67% em cenário sem ataque e 9,74% em cenário com ataque). Ao mesmo tempo, foi também capaz de fornecer aos gestores da rede informações sobre a localização dos invasores.

**Start date:** 11-12-2019

**End date:** 03-04-2024

**Last modified:** 03-16-2024

**Copyright information:**

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customize it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

---

## Detecção e mitigação de ataques de interrupção de tráfego em redes de sensores sem fio com RPL - Descrição dos Dados e Metadados produzidos pelo projeto

Serão coletados dados resultantes dos experimentos feitos com o simulador Cooja da plataforma Contiki-ng. O simulador Cooja simula redes de sensores sem fio e cada simulação é definida por um arquivo no formato XML de extensão ".csc", que traz os detalhes do cenário simulado e o posicionamento dos nós, além de um log do console de saída no formato .txt. Os logs de saída de cada simulação são processados e o resultado disso é um outro arquivo, também no formato .txt, com estatísticas e contabilizações calculadas a partir de cada arquivo de simulação.

Os dados serão coletados a partir de simulações com a ferramenta Cooja, a partir de simulações estruturadas como descrito a seguir.

Cada experimento foi implementado com pelo menos duas variações de cenário, o cenário chamado de BASELINE é o cenário de controle, onde a simulação é feita sem a execução do framework proposto, para avaliar os impactos de ataques em redes não protegidas pelo nosso framework. O cenário DMAIT reproduz as configurações do cenário BASELINE, porém agora os nós das redes simuladas executam o nosso framework, e assim podemos contabilizar e comparar os benefícios obtidos com nosso framework. Em alguns experimentos foram usados cenários adicionais que desligam o envio de ACKs (com o nome dos arquivos/pastas acrescido de "-NOACK"), ou ainda cenários onde nenhum ataque ocorre (com o nome dos arquivos/pastas acrescido de "-NOATTACK").

Cada experimento é armazenado em uma pasta diferente, e nelas temos pastas separadas para cada variação de cenário. Em cada cenário temos os arquivos da simulação (.csc), os arquivos de console de saída ("\*log.txt") e o arquivo de saída processado ("\*-PROCESADO.txt"). Para cada cenário foram executados entre 10 e 15 simulações, cada uma com uma semente (seed) de simulação diferente. A semente de simulação encontra-se registrada em cada arquivo de simulação (.csc), e os arquivos trazem o texto "-seedX" no nome, onde "X" é um número inteiro, identificando os arquivos relativos à mesma semente.

---

---

---