Detecção multimétrica distribuída de ataques de negação de serviço em redes de sensores sem fio definidas por software

Marcos Paulo Simão Barros[1], **Gustavo A. Nunez Segura**[2], **Cíntia Borges Margi**[1]

[1]Escola Politécnica da Universidade de São Paulo (EPUSP) – São Paulo – SP – Brasil

[2]Escuela de Ingeniería Eléctrica – Universidad de Costa Rica – San José – Costa Rica

{marcospsibarros,cintia}@usp.br, gustavoalonso.nunez@ucr.ac.cr

Abstract. *Wireless Sensor Networks are part of the Internet of Things infrastructure, and the use of software defined networking paradigm brings flexibility to sharing constrained resources. Mechanisms to detect denial of service attacks are necessary. IDIT-SDN is a cooperative approach to detect SDN control plane attacks combining distributed anomaly detection with centralized mechanisms. Due to limited storage, distributed detection was based in only one metric. Thus, this work describes the proposal and implemention of detection based on monitoring simultaneously two metrics. Results show that there is an increase in detection rates, which occur in less time.*

Resumo. *Redes de sensores sem fio compõe a infraestrutura da Internet da Coisas, e o uso do paradigma de redes definidas por software é uma alternativa para trazer flexibilidade no compartilhamento dos recursos restritos. Mecanismos de detecção de ataques de negação de serviço são necessários. O IDIT-SDN é um mecanismo cooperativo de detecção de ataques ao plano de controle SDN que combina a detecção de anomalias distribuída com mecanismos centralizados. Devido ao armazenamento restrito, a detecção distribuída baseia-se em uma única métrica. Assim, este trabalho propõe e implementa a detecção baseada no monitoramento simultâneo de duas métricas. Resultados obtidos indicam que há aumento nas taxas de detecção, além de serem mais rápidas.*

1. Introdução

Redes de sensores sem fio (RSSF) compõe a infraestrutura da Internet da Coisas (IoT - *Internet of Things*). Devido às suas características e recursos restritos que dispõe, são necessários protocolos específicos para a comunicação nesse cenário como o RPL [Alexander et al. 2012] ou o arcabouço IT-SDN [Alves et al. 2019]. Dada a criticidade de muitas dessas infraestruturas de IoT torna-se necessário o entendimento de possíveis ataques de negação de serviço nestes cenários, bem como a determinação de mecanismos para detecção e mitigação dos mesmos [Carrer and Margi 2023, Segura et al. 2019].

No contexto de RSSFs que utilizam o arcabouço IT-SDN [Alves et al. 2019], o IDIT-SDN [Segura et al. 2023] é um mecanismo cooperativo de detecção de ataques ao plano de controle que combina a detecção de anomalias distribuída com mecanismos centralizados, e resultado de pesquisa de doutorado no grupo. Quando ocorrem ataques de negação de serviço, ocorre uma mudança no comportamento da rede que é observada nas métricas de desempenho da rede [Segura et al. 2019]. A detecção de ataques centralizada foi desenvolvida baseada na análise de *Change Point* (CP) [Segura et al. 2020].

Para melhorar a taxa de detecção de ataques, os autores propuseram que cada nó da RSSF monitore o seu comportamento em termos de duas métricas de comunicação e execute o algoritmo de análise de CP [Segura et al. 2021]. A vantagem dessa abordagem distribuída é não aumentar o tráfego de pacotes na rede, e consequentemente o consumo de energia, utilizando o processamento disponível no nó.

Contudo, devido à limitação de armazenamento do dispositivo usado, a detecção foi realizada com o monitoramento de uma única métrica por vez. Assim, este trabalho apresenta uma nova proposta e implementação de detecção baseada no monitoramento simultâneo das duas métricas definidas [Segura et al. 2021]. Para validar a proposta, os experimentos realizados simularam redes de 36 e 100 dispositivos, testando a análise de CP com e sem atacantes, e avaliando cada métrica em função da topologia e do tempo para a detecção (mesmos que os trabalhos anteriores). Os resultados mostram que a utilização de duas métricas leva ao aumento nas taxas de detecções de CP, sobretudo em dispositivos a um salto dos atacantes. Além disso, a utilização de duas métricas ao mesmo tempo promove detecções mais rápidas, sendo possível explorar as peculiaridades do comportamento das detecções de cada métrica.

2. IDIT-SDN

O arcabouço de segurança IDIT-SDN [Segura et al. 2023] permite que todos os dispositivos da rede cooperem para a detecção de um possível ataque. Com o arcabouço, o dispositivo é capaz de detectar uma anomalia em seu comportamento. Como uma rede sob ataque tem seu comportamento alterado [Segura et al. 2019], tais anomalias podem estar relacionadas a ataques de negação de serviço distribuídos (DDoS).

O detector de anomalias é baseado na análise de *Change Point* (CP), seguindo a proposto descrita em [Segura et al. 2020]. O algoritmo do detector é composto por duas rotinas, uma de monitoramento e a outra de detecção. A rotina de monitoramento, extrai informações ao longo do tempo e as acumula em uma série temporal, e com base nela calcula a variância e soma cumulativa. Na rotina de detecção, baseado nas estatísticas calculadas na rotina anterior, é feito um teste de hipótese. Se o valor encontrado exceder o valor crítico, um *Change point* (CP) foi detectado e um alerta é disparado.

O método é iterativo, pois a cada nova amostra verifica-se a existência de comportamento não usual. Além disso, o arcabouço também é um método distribuído, pois todos os dispositivos executam o algoritmo de detecção. Contudo é importante mencionar que essa detecção não é totalmente distribuída dado que a decisão final sempre depende de um dispositivo centralizado, que no caso do IDIT-SDN é o modulo de segurança central. A abordagem distribuída evita uma sobrecarga de transmissão de pacotes presente em abordagens totalmente centralizadas. Os resultados obtidos mostraram que o arcabouço detecta ataques *False Data Flow Forwarding* (FDFF) com uma probabilidade entre 0,93 e 1,00, semelhantes a propostas totalmente centralizadas [Segura et al. 2021].

O IDIT-SDN baseia-se na versão 0.41 do IT-SDN[1] para a sua implementação. O IT-SDN é um arcabouço de SDWSN (Redes de Sensores Sem Fio Definidas por Software) de código aberto, projetado para o sistema operacional *Contiki OS*. Os ataques de negação de serviço implementados relacionam-se aos protocolos de controle que fazem

[1]Disponível em `https://sites.google.com/usp.br/cintia/it-sdn`

parte do IT-SDN. No ataque FDFF [Segura et al. 2019], o atacante envia um pacote de dados para um de seus vizinhos com identificadores aleatórios. Como os vizinhos não tem esse destino na tabela de fluxo, eles solicitam ao controlador a regra de fluxo para tal destino. Assim, ocorre uma sobrecarga de transmissão de pacotes, principalmente nas proximidades do controlador e dos atacantes.

3. Método

Para realizar as implementações necessárias para a detecção por duas métricas simultâneas no IDIT-SDN é necessário um dispositivo com mais armazenamento do que o originalmente usado (*sky mote* com 48 kB de memória *flash*). Assim, escolhemos o dispositivo *Z1 mote*, equipado com o mesmo microcontrolador MSP430 e com maior capacidade de armazenamento, a memória *flash* é de 92 kB.

Em [Segura et al. 2021], a construção da série temporal no dispositivo ocorria a partir da coleta de uma só métrica selecionada em tempo de compilação, cuja análise de CP era realizada. Neste trabalho, cada nó constrói e analisa duas séries temporais concorrentemente, sendo uma para cada métrica a ser usada para a detecção de comportamento não usual. Para a métrica de tempo de transmissão de pacotes, monitora-se o tempo que o módulo de rádio permanece ligado em estado de transmissão usando o *Energest* [Dunkels et al. 2007]. A segunda métrica relaciona-se ao plano de controle do IT-SDN, então monitora-se o número de pacotes de controle [Alves et al. 2019] que o nó recebe.

Parâmetros da Simulação	
Topologia	*Grid* 6x6 e 10x10
Número de nós	36 e 100
Duração da simulação (s)	36000
Número de Sorvedouros	2
Número de atacantes	3 e 10
Posição dos Sorvedouros	No meio da borda da grade
Distância entre vizinhos (m)	36,7 (36 nós) e 45 (100 nós)
Alcance de transmissão do rádio (m)	45 (36 nós) e 55 (100 nós)
Número de iterações	10
Início dos ataques após (s)	14000
Parâmetros da detecção distribuída	
Série de Monitoramento	200 amostras
Série de Detecção	50 amostras
Período de amostragem (s)	60
Sensibilidade	0
Valor crítico	2.82

Tabela 1. Parâmetros da Simulação

Conforme os trabalhos anteriores relacionados ao IDIT-SDN, o experimento consiste em simulações de duas topologias em grade, com 36 e 100 nós, usando o simulador COOJA [Osterlind et al. 2006]. O algoritmo de detecção baseia-se na construção de duas series temporais. A primeira série, chamada de Série de Monitoramento, é composta por 200 amostras e é utilizada para extrair as estatísticas necessárias durante a fase online do

algoritmo. Nela, as novas amostras são armazenadas em outra série, chamada de Série de Detecção. A cada iteração dessa rotina, é feita a verificação de CP. Se a Série de Detecção acumular 50 amostras sem CP, as primeiras 50 amostras da Série de Monitoramento são descartadas, e o conteúdo da Série de Detecção é adicionado a ela. Dessa forma, novas estatísticas são extraídas e a Série de Detecção é reiniciada. A Tabela 1 exibe os parâmetros de configuração dos experimentos. Os valores dos parâmetros de detecção distribuída usados no experimento, aumentam a taxa de detecção de CP em relação à outros valores experimentados em [Segura et al. 2022].

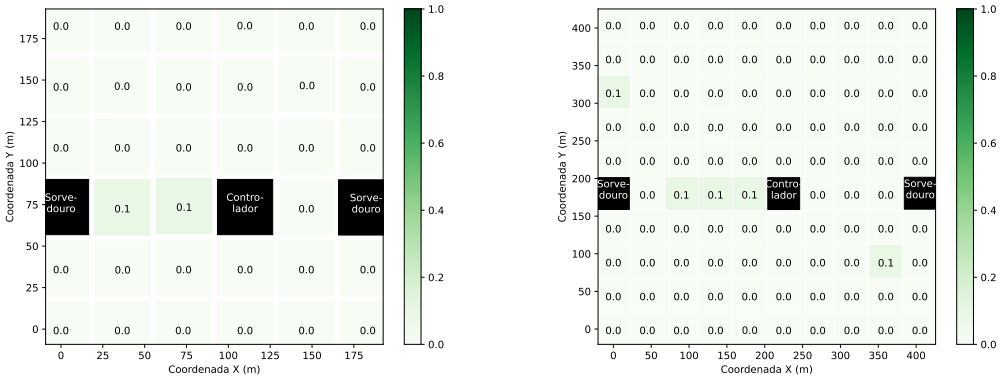
A partir do tamanho das séries temporais, definimos o tempo total da simulação e o tempo de início dos ataques, levando em consideração o período de amostragem. Como uma amostra é coletada a cada 60 segundos, para obter as primeiras 200 amostras são necessários pelo menos 12000 segundos. Além disso, as amostras durante a configuração da rede devem ser descartadas das estatísticas, já que não representam o comportamento normal da rede. Para considerar esses fatores e poder testar a detecção, o tempo de início do ataque foi configurado em 14000 segundos.

4. Resultados e Discussão

Esta seção apresenta os resultados e análises dos experimentos. A Seção 4.1 abrange a detecção de CP via tempo de transmissão, enquanto a Seção 4.2 abrange a detecção via pacotes de controle recebidos, e Seção 4.3 faz a análise conjunta.

4.1. Tempo de transmissão

A Figura 1 apresenta o percentual de detecção de CP em relação ao total de iterações da simulação. Nesse cenário não há atacantes, exibindo assim, o comportamento da rede em condições estáveis com nós estáticos, que não mudam de posição e continuam em operação durante toda a simulação. Em tal contexto, o índice de falso positivo foi de 0,6% com 36 nós e 0,5% com 100 nós respectivamente.

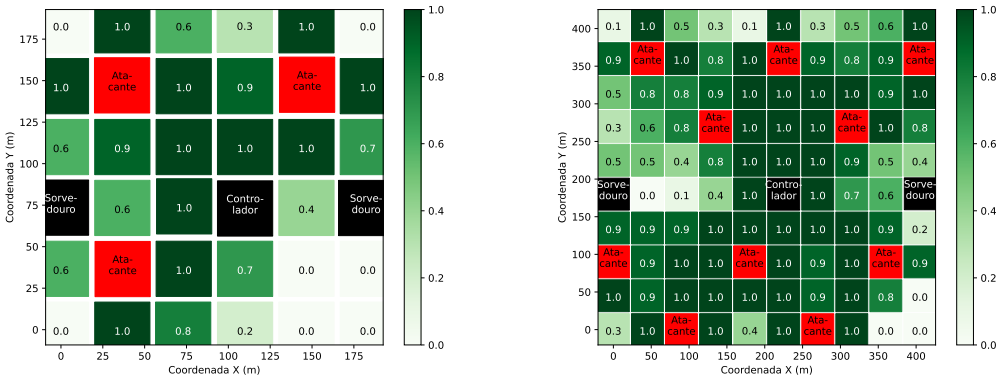


(a) 36 nós **(b)** 100 nós

Figura 1. Taxa de detecção de CP a partir de tempo de transmissão de pacotes para simulações sem ataques (Índice de falsos positivos)

No cenário similar com 10% de atacantes, a taxa média de detecção de CP avança para 61% dos dispositivos para 36 nós conforme ilustrado na Figura 2(a). A taxa média de detecção é o percentual médio de ocorrências de CP em nós sensores, excluindo-se assim,

o controlador e os Sorvedouros. Já na topologia de 100 nós, com atacantes espalhados por toda a rede, a média de registros de CP é 76,7% conforme mostrado na Figura 2(b).



(a) 36 nós **(b)** 100 nós

Figura 2. Taxa de detecção de CP a partir de tempo de transmissão de pacotes para simulações com 10% dos nós como atacantes.

Observa-se também que os nós mais próximos ao controlador detectam mais CP a partir da métrica de tempo de transmissão. Na rede de 36 nós, enquanto o percentual de detecção entre todos os nós é de 61%, nós que estão a um salto do controlador apresentam percentual de detecção de CP de 77,5% e nós que estão a dois saltos apresentam 67,2% de CP. Esse comportamento ocorre também na topologia de 100 nós, visto que os vizinhos do controlador apresentam 100% de detecção e nós a dois saltos 88,8%, enquanto a média global é de 76,7%. Isso ocorre devido ao aumento do fluxo de mensagens entre o controlador e o restante da rede causado pelo ataque, fazendo com que os nós mais próximos ao controlador passem mais tempo transmitindo pacotes.

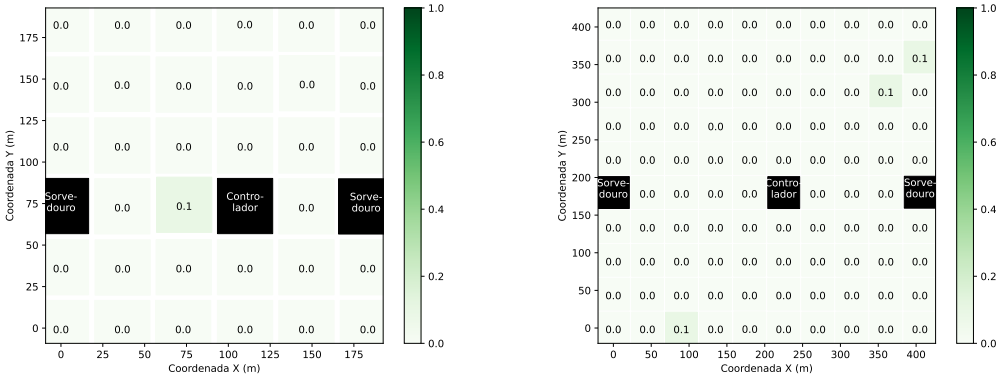
4.2. Pacotes de controle recebidos

A Figura 3 exibe apenas a detecção de CP baseada em número pacotes de controle recebidos sem ataques. Assim, atribui-se ao ataque a mudança nas taxas de detecção de CP pelos nós nas simulações com ataques. Nos cenários com 36 ou 100 nós, o índice de falso positivo foi inferior a 0,5%, e mais de 95% dos nós não detectaram CP nas iterações.

A mudança de comportamento devido à presença de ataques, observada nas Figuras 4(a) e (b) ocorre nos vizinhos dos atacantes. Considerando apenas vizinhos de atacantes, a taxa de detecção é de 100% nas duas topologias. Contudo, para mais de um salto do nó malicioso, o ataque nessa métrica não é percebido, pois não há detecção nesses nós. Esse comportamento é consequência do ataque FDFF, no qual o controlador envia um pacote de controle para o nó atacado, ou seja, o nó que recebeu um pacote com destinatário desconhecido. Assim, o nó solicita ao controlador o caminho até o referido destinatário, e o controlador responde enviando um pacote de controle de volta ao nó.

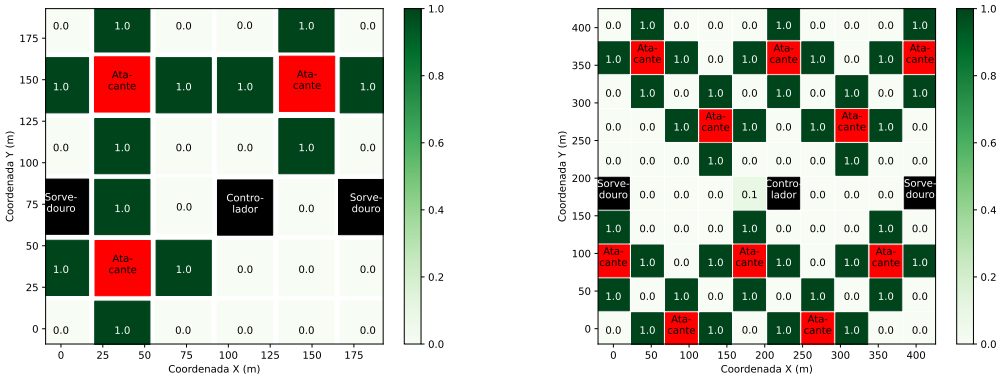
4.3. Análise conjunta

Durante o experimento, executa-se o algoritmo de detecção em duas instâncias separadamente, o que permite a comparação das métricas em termos de taxa de detecção e tempo



(a) 36 nós **(b)** 100 nós

Figura 3. Taxa de detecção de CP a partir de pacotes de controle para simulações sem ataques (Índice de falsos positivos)



(a) 36 nós **(b)** 100 nós

Figura 4. Taxa de detecção de CP a partir de pacotes de controle para simulações com 10% dos nós como atacantes.

para detecção. Conforme a Tabela 2, observa-se que a análise de CP via pacotes de controle é a mais rápida. Em ambos os cenários, a primeira detecção por essa métrica ocorre, em média, após 40 segundos do início dos ataques. Como o período de amostragem é de 60 segundos, o CP é detectado logo na primeira amostra sob ataque. Observando a diferença de tempo entre as primeiras detecções de cada métrica em cada iteração, são necessárias duas ou três amostras a mais para que ocorra a primeira detecção por tempo de transmissão. Caso o período de amostragem fosse outro, o tempo poderia mudar, dado que a detecção ou não de CP depende da chegada de novas amostras à série de detecção.

Outro resultado que pode distinguir as duas métricas é o desvio padrão observado ao longo das iterações, cujos valores estão apresentados na Tabela 2, onde σ_{RxCtrl} representa o desvio padrão da métrica de pacotes de controle, e o desvio padrão da outra métrica é representado por σ_{TxTime}. Ao compará-los nota-se que σ_{TxTime} apresenta valores maiores que o da outra métrica, mas também existe uma disparidade entre o σ_{TxTime} de cada cenário (número de nós). No cenário com atacantes em maior número e dispostos por toda a rede, o tempo médio apresenta queda assim como o seu desvio padrão,

indicando maior rapidez e estabilidade. Isso sugere que o número de atacantes e a sua distribuição na rede exercem influência sobre a rapidez de detecção. Do mesmo modo, o σ_{Dif} representa o desvio padrão da diferença de tempo de detecção entre as métricas ao longo das iterações. Tal estatística, devido à flutuação apresentada pela detecção de CP via tempo de transmissão, teve seu valor próximo à σ_{TxTime}.

Número de nós	Pacotes de controle		Tempo de Transmissão		Diferença entre métricas	
	Média (s)	σ_{RxCtrl} (s)	Média (s)	σ_{TxTime} (s)	Média (s)	σ_{Dif} (s)
36	40,14	0,28	166,41	49,84	126.26	49,85
100	40,25	0,06	142,56	27,37	102,32	27,36

Tabela 2. Tempo transcorrido do início do ataque até o primeiro alerta de detecção de CP a partir de cada métrica.

É possível analisar a eficiência da utilização de cada métrica, verificando a taxa média de detecção de ataques. Essa análise é dividida em três grupos: vizinhos dos atacantes, vizinhos do controlador e o restante dos nós (aqueles que estão a pelo menos dois saltos do controlador e dos atacantes). A Tabela 3 apresenta os valores de cada grupo separadamente. Ao utilizar o tempo de transmissão como métrica para as amostras, obtém-se maior eficiência na detecção dos sensores próximos ao controlador e nos sensores que fazem parte do fluxo dos nós atacados em direção ao controlador. Por outro lado, quando se extrai as amostras do número de pacote de controle recebidos por cada sensor, verifica-se a maior eficiência em termos de tempo (detecção mais rápida) e uma maior acurácia para nós adjacentes ao dispositivo atacante.

Ao ignorar a métrica analisada para o CP e ao considerar apenas a sua detecção ou não por parte do dispositivo, temos que o índice de detecção geral foi de 78,7% no cenário com 100 nós e de 64,3% no cenário com 36 nós, respectivamente. Por fim, com 36 nós, 36,7% dos dispositivos apresentaram dupla detecção, ou seja, verificaram CP a partir das duas métricas. Tal valor foi de 39,3% no maior cenário.

Métrica	Número de nós	Vizinhos do Controlador	Vizinhos dos atacantes	Outros	Geral
Tempo de transmissão	36	77,5%	91,7%	30,0%	61,0%
	100	100%	95,0%	60,6%	76,7%
Pacotes de Controle	36	0%	100%	0%	40,0%
	100	2,5%	100%	0%	41,5%

Tabela 3. Taxa de detecção segregada por características topológicas.

5. Conclusão

Em [Segura et al. 2021], a taxa de detecção para os vizinhos imediatos de um atacante e do controlador eram entre 93% e 100%. Ao utilizar duas métricas simultâneas, a detecção aumenta para 100% pois a métrica de tempo de transmissão maximiza a detecção nos vizinhos do controlador ao passo que a métrica de pacotes de controle maximiza a detecção nos vizinhos do atacante. O uso da métrica de pacote de controle reduz o tempo de detecção, mas se for a única utilizada, há perda na taxa de detecção para os vizinhos do controlador. Porém, ao usar ambas as métricas, temos os benefícios de ambas.

Além disso, a utilização de duas métricas simultâneas abre múltiplas possibilidades para a utilização de informações variadas na detecção de ataques, o que pode resultar

em estratégias mais robustas e adaptáveis contra ameaças. Os resultados sugerem que a combinação de métricas para detecção de ataques DDoS pode ser uma estratégia promissora para melhorar a segurança de redes. Pretendemos testar o IDIT-SDN com outras métricas e diferentes formas de combiná-las, além de mensurar a utilização do hardware com as novas implementações em termos de memória e consumo de energia.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, projetos FAPESP #2022/07523-8, #2023/08828-0 e #2020/09850-0. Cintia B. Margi é bolsista de produtividade do CNPq #311687/2022-9.

Referências

Alexander, R., Brandt, A., Vasseur, J., Hui, J., Pister, K., Thubert, P., Levis, P., Struik, R., Kelsey, R., and Winter, T. (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550.

Alves, R. C., Oliveira, D. A., Segura, G. A. N., and Margi, C. B. (2019). The cost of software-defining things: A scalability study of software-defined sensor networks. *IEEE Access*, 7:115093–115108.

Carrer, A. and Margi, C. (2023). Segurança em internet das coisas: Uma análise de comportamento de rede sob ataque. In *Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 189–200.

Dunkels, A., Osterlind, F., Tsiftes, N., and He, Z. (2007). Software-based on-line energy estimation for sensor nodes. In *Proceedings of the 4th workshop on Embedded networked sensors*, pages 28–32.

Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., and Voigt, T. (2006). Cross-level sensor network simulation with cooja. In *Proceedings. 2006 31st IEEE conference on local computer networks*, pages 641–648. IEEE.

Segura, G. A. N., Chorti, A., and Margi, C. B. (2020). Multimetric online intrusion detection in software-defined wireless sensor networks. In *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6. IEEE.

Segura, G. A. N., Chorti, A., and Margi, C. B. (2021). Distributed dos attack detection in SDN: Tradeoffs in resource constrained wireless networks. In *2021 IEEE Statistical Signal Processing Workshop (SSP)*, pages 131–135. IEEE.

Segura, G. A. N., Chorti, A., and Margi, C. B. (2022). Centralized and distributed intrusion detection for resource-constrained wireless SDN networks. *IEEE Internet of Things Journal*, 9(10):7746–7758.

Segura, G. A. N., Chorti, A., and Margi, C. B. (2023). IDIT-SDN: Intrusion detection framework for software-defined wireless sensor networks. In *Anais Estendidos do XLI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 56–63.

Segura, G. A. N., Margi, C. B., and Chorti, A. (2019). Understanding the performance of software defined wireless sensor networks under denial of service attack. *Open Journal of Internet Of Things (OJIOT)*, 5(1):58–68.