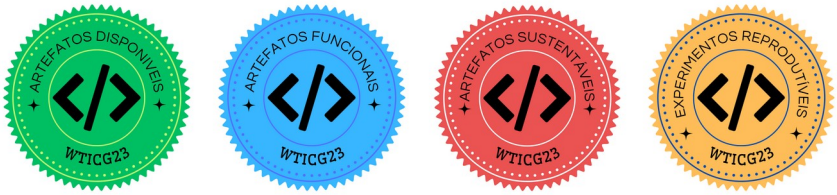


Segurança em Internet das Coisas: Uma Análise de Comportamento de Rede sob Ataque

Alexandre M. Carrer[1], **Cíntia B. Margi**[1]

[1]Departamento de Sistemas Digitais e Computação
Escola Politécnica da Universidade de São Paulo (EPUSP) – São Paulo, SP – Brazil

{alexandrecarrer,cintia}@usp.br

Abstract. *In order to provide detection and mitigation of Internet of Things (IoT) attacks, it is vital to understand how different attacks impact network performance. Literature, in general, includes network layer attacks analysis. In this work we implement attacks on the link layer (Blackhole and Greyhole) and transport layer (Flooding) and analyze the network behaviour using metrics such as server response rate to client requests and routing protocol downtime. Simulations were conducted with different densities of attackers and distances from the malicious node to the server. The results demonstrate the capacity of relating the collected metrics with the type of attack and approximate location of the attacking node.*

Resumo. *Para viabilizar mecanismos de detecção e mitigação de ataques em Internet das coisas (IoT) é vital entender como diferentes ataques afetam o desempenho da rede. A literatura em geral contém análises de ataques da camada de rede. Neste trabalho implementamos ataques de camada de enlace (Blackhole e Greyhole) e de camada de transporte (Flooding) e analisamos o comportamento da rede observando a taxa de resposta do servidor e a indisponibilidade do protocolo de roteamento. As simulações foram realizadas com diferentes densidades de atacantes e diferentes distâncias do atacante ao servidor. Os resultados demonstram a capacidade de relacionar as métricas coletadas com o tipo de ataque e localização aproximada do nó atacante.*

1. Introdução

A segurança é um requisito crítico em Internet das Coisas (ou *Internet of Things* - IoT) e garanti-la é essencial para suas mais diversas aplicações. No escopo de redes IoT temos as *Low Power and Lossy Networks* (LLNs), redes de dispositivos que possuem recursos limitados de memória, processamento e energia, com enlaces com baixa vazão de dados e sujeitos à perdas de pacotes. Estes fatores dificultam a implementação e utilização de mecanismos de segurança diretamente nos nós da rede.

Uma estratégia comum e necessária para detecção de ataques de rede, especialmente de negação de serviço (DoS - *Denial of Service*), é o uso de Sistemas de detecção de intrusão (IDS - *Intrusion Detection Systems*) [Ganapathi and D 2009]. Um IDS baseado em rede detecta anomalias no funcionamento da rede analisando os parâmetros da rede e os pacotes trocados entre os dispositivos. Cada rede possui um conjunto de protocolos em funcionamento e está sujeita a diversos ataques que podem comprometer a integridade, confidencialidade e disponibilidade dos dados coletados.

Para desenvolver um IDS para redes de computadores é necessário ter o conhecimento do funcionamento padrão da rede e como ela se comporta sob ataques. Os sistemas podem ser classificados conforme o mecanismo de detecção de intrusão implementado [Zarpelão et al. 2017]. Um fator em comum é a comparação do funcionamento atual da rede com o normal, analisado em um ambiente controlado.

Na literatura são poucas as análises de comportamento de rede que utilizam os padrões definidos pelo IETF (*Internet Engineering Task Force*) para IoT com ataques além da camada de rede. Por exemplo, o protocolo de roteamento RPL [Barthel et al. 2012] é analisado isoladamente. Tomić e McCann analisam os resultados sob a ótica de vulnerabilidades oriundas dos protocolos de camada de roteamento, investigando a reação das métricas de rede sob seis diferentes ataques de camada de rede [Tomić and McCann 2017]. Rehman et al. realizam ataques no sistema de rank de nós no protocolo RPL, protocolo de roteamento do padrão IETF [Rehman et al. 2016].

Neste trabalho são analisados três ataques em diferentes camadas da pilha de protocolos IETF para IoT com o objetivo de melhor entender o comportamento da rede sob ataque e coletar suas métricas de desempenho. Assim, foram implementados os ataques *Blackhole* e *Greyhole* de camada de enlace, e *Flooding* de camada de transporte. Foram executadas simulações variando densidade de nós atacantes e distância dos nós malicioso ao servidor.

Os resultados apresentam a reação das métricas de rede para cada tipo de ataque nas diferentes densidades de atacantes (6, 12 e 25%). Foi analisado o impacto dos ataques *Blackhole* e *Greyhole* e a possível partição da rede que eles podem causar com base na localização do nó malicioso na topologia de rede. Outro comportamento observado foi a diminuição drástica na taxa de resposta do servidor às requisições dos clientes em ataques do tipo *flooding* para as simulações acima de 12% de nós atacantes.

2. Implementação dos Ataques

IoT é um sistema complexo que permite a coleta de dados em diversos ambientes, como em aplicações de monitoramento ambiental, controle de tráfego e segurança. A IETF define uma pilha de protocolos voltada para aplicações de IoT, sendo aceita como o padrão nesta área de LLNs e IoT [Palattella et al. 2013]. No entanto, os dispositivos e protocolos estão sujeitos a vários tipos de ataques que podem comprometer a sua disponibilidade. Cada tipo de ataque pode ter diferentes impactos e requer diferentes contramedidas para proteger a rede.

Este trabalho tem como objetivo avaliar ataques ativos relacionados a protocolos IETF para IoT. Os ataques ativos são aqueles que injetam pacotes na rede, atuando em diferentes camadas na pilha de protocolos, e são classificados conforme a camada afetada em cada tipo de comportamento malicioso [Deogirikar and Vidhate 2017] [Zhou et al. 2008]. Para tanto, selecionamos os ataques *Blackhole* e *Greyhole*, implementados na camada de enlace, e *Flooding*, implementado na camada de transporte. Os três ataques foram implementados em nós utilizando o sistema operacional Contiki-NG [Oikonomou et al. 2022], usado em dispositivos e sensores de IoT [Bansal and Kumar 2020].

Blackhole Os ataques do tipo *Blackhole* são ativos, pois o atacante descarta os pacotes que deveria encaminhar na rede. Quando o protocolo de roteamento baseia-se na topologia de árvore (como no RPL que baseia-se em DODAG), o nó malicioso que implementa este tipo de ataque faz com que os nós filhos percam a conectividade com o sorvedouro da rede.

Para implementar este ataque modifica-se o *framer* do nó malicioso. O *framer* dos pacotes da rede é provido pelo sistema operacional e é diferente para cada tecnologia de acesso ao meio. Ao modificar o código que cria os quadros encaminhados pelo nó, não chamando a sub-rotina de criação de quadros, impedimos que ele transmita qualquer tipo de pacote após a ativação do comportamento malicioso. Pseudocódigo 1 ilustra esta modificação do *framer*.

Greyhole Ataques do tipo *Greyhole* são similares aos ataques *Blackhole* ao realizar o descarte de pacotes ao invés de transmiti-los. Porém, a diferença entre eles é que ataques *Blackhole* absorvem todos os pacotes recebidos e ataques *Greyhole* absorvem uma parte deles. Assim, ataques *Greyhole* são mais difíceis de serem detectados.

A implementação é similar ao ataque do tipo *Blackhole*, porém apresenta comportamento de um encaminhamento seletivo. As modificações do *framer* do nó malicioso impedem que parte das transmissões e encaminhamento de pacotes sejam feitas pelo nó atacante. Para decidir quais pacotes são descartados realiza-se o sorteio de um número aleatório de 0 a 100, e caso ele seja menor que a porcentagem definida, o pacote é descartado. O Pseudocódigo da implementação do ataque Greyhole pode ser encontrado no Pseudocódigo 2.

Pseudocódigo 1: Modificação do Framer para implementação de ataque Blackhole.

```
if iniciarAtaque and nodeID == attackerNodeID
then
    Packet Blackholed
else
    Create and Foward Frame
end if
```

Pseudocódigo 2: Modificação do Framer para implementação de Greyhole.

```
dropRatio = 30,
          = 60,
          = 90
if iniciateAttack and nodeID==attackerNodeID and rand %
100 ≤ dropRatio then
    Packet Blackholed
else
    Create and Foward Frame
end if
```

Flooding Este ataque é classificado como ativo e sua implementação se baseia em sobrecarregar a rede enviando pacotes repetidamente. Por exemplo, em um ataque de *Flooding* na camada de rede utilizando o RPL como protocolo de roteamento, um nó malicioso envia muitos pacotes de configuração de rede DIO/DAO em um curto intervalo de tempo. Na camada de aplicação, um nó malicioso pode realizar o ataque enviando muitas requisições de sua aplicação em pouco tempo.

Para a implementação do ataque de *Flooding* na camada de transporte, utilizamos como referência um programa exemplo de comunicação UDP disponível no Contiki-NG, cujo cliente envia requisições a cada 60 segundos. O nó atacante envia uma nova requisição a cada 300 milissegundos, inundando assim a rede e o sorvedouro de requisições UDP.

Além de sobrecarregar o sorvedouro de dados, o ataque afeta outros nós por fazê-los rotear as mensagens até chegar ao destino. Este comportamento malicioso gera dificuldade de acesso ao meio por outros nós da rede e gera colisões de mensagens que atrasam as requisições. O ataque também enche o *buffer* de mensagens dos nós intermediários entre o atacante e o sorvedouro da rede, causando perda de pacotes recebidos e gerados pelo próprio nó, além de rotear uma grande quantidade de pacotes vizinhos. O Pseudocódigo desta modificação pode ser encontrado no Pseudocódigo 3.

Pseudocódigo 3: Modificação do código do dispositivo para implementação de Flooding.

```
while True do
    if eTimerExpired then
        Send UDP request
        if nodeID==attackerNodeID and iniciateAttack then
            setTimer(0,3s)
        else
            setTimer(60s)
        end if
    end if
end while
```

3. Método

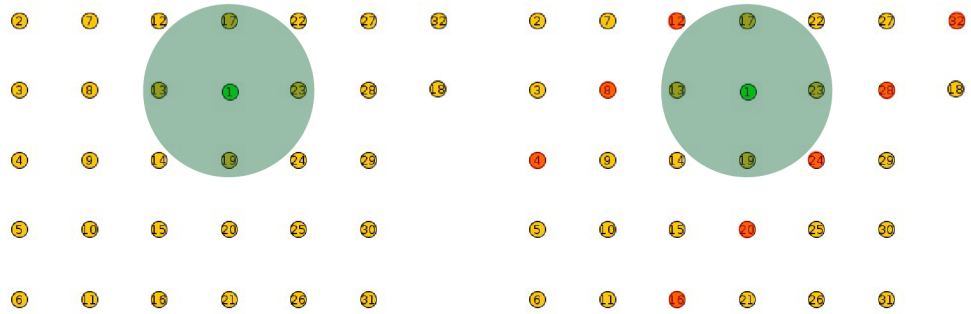
O objetivo da pesquisa é o entender o comportamento da rede em um cenário IoT sob diferentes ataques que tentam interromper seu funcionamento correto. Para isto, foram realizadas diferentes simulações variando densidade dos atacantes e distância dos nós maliciosos até o servidor. As simulações foram divididas em três densidades de nós atacantes, 6% (nós múltiplos de 13), 12% (nós múltiplos de 7) e 25% (nós múltiplos de 4). Estes múltiplos foram escolhidos para uma maior amplitude de casos abordados na simulação, melhor discutido na Seção 4.

A simulação foi realizada em uma máquina virtual com o sistema operacional Ubuntu Desktop 22.04 canônico. Para a instalação do Contiki-NG e o Simulador Cooja, foi seguido o tutorial de instalação por Docker disponível na documentação do sistema operacional [Contiki-NG 2023]. Para a simulação de rede, os sensores emulados utilizados foram os *Z1 WSN Module*, da Zolertia [Zolertia 2013].

O código dos dispositivos foi criado com base no exemplo de aplicação de protocolo UDP do sistema operacional Contiki-NG. No padrão de pilha de protocolos IETF IoT [Palattella et al. 2013] e na simulação realizada são utilizados os seguintes protocolos: para a camada física e de enlace: IEEE 802.15.4, para a camada de rede: *IPv6 over Low Power Personal Area Network* (6loWPAN) + Routing Protocol for *Low-Power and Lossy Networks* (RPL) e para a camada de transporte: *User Datagram Protocol* (UDP).

A topologia de rede em seu funcionamento padrão possui 32 nós, sendo um com a função de servidor UDP e 31 clientes. Cada cliente realiza uma requisição por minuto ao servidor, que atua como sorvedouro da rede e raiz da árvore DODAG do protocolo RPL. Cada mensagem é composta por 32 Bytes (simbolizando os dados da aplicação) e todas as requisições devem ser respondidas, ou seja, uma mensagem de 32 bytes é enviada do cliente ao servidor e vice-versa em cada requisição. A topologia de rede está ilustrada na Figura 1, onde os nós possuem contato apenas com seus vizinhos imediatamente nos

pontos cardinais, ou seja, vizinhos de cima, baixo, esquerda e direita. O alcance dos nós está indicado pelo círculo verde em volta do servidor da rede.



(a) Topologia padão

(b) Topologia de rede em ataque com 25% de densidade de atacantes

Figura 1. Topologia da rede simulada no Contiki Cooja (Verde: Servidor da rede; Vermelho: Nós atacantes).

A simulação foi executada por 2 horas e 30 minutos para a coleta dos dados que viabiliza a análise do comportamento de rede. Na simulação, os nós atacantes foram ativados no marco de uma hora de simulação. Quando os nós maliciosos realizam 60 requisições, iniciam o ataque programado como descrito na seção 2.

Durante as simulações realizadas, foram coletadas diversas métricas para avaliar o impacto dos ataques na rede. As duas métricas avaliadas foram a taxa de resposta do servidor às requisições feitas pelos clientes e o tempo que o protocolo RPL ficou indisponível para os nós da rede.

A **taxa de resposta do servidor às requisições dos clientes** foi medida para verificar o impacto do ataque de *Flooding*, *Blackhole* e *Greyhole* no acesso ao meio e no *buffer* de mensagens a serem transmitidas e roteadas pelo nó. Ao coletar essa métrica, foi possível avaliar como o ataque de *Flooding* afetou a capacidade do servidor em responder às requisições dos clientes não atacantes. Já nos ataques de *Blackhole* e *Greyhole*, a métrica foi utilizada para compreender a partição da rede causada pelos nós atacantes, bem como a adaptação da topologia de rede perante estes ataques.

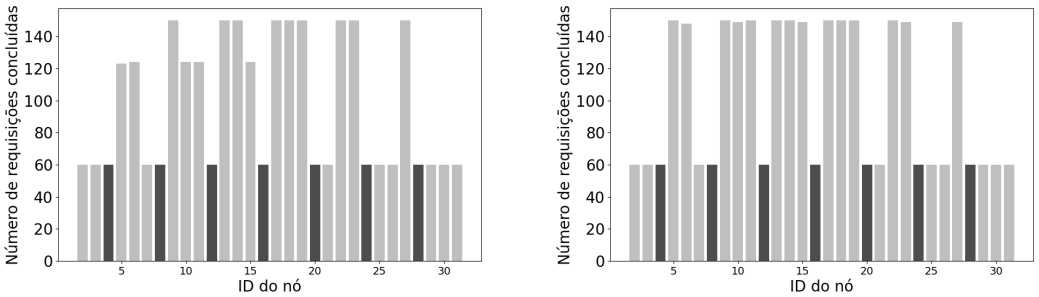
A outra métrica coletada foi **o tempo que o protocolo de roteamento ficou indisponível para os nós da rede**. O protocolo RPL é responsável pelo roteamento dos dados nas redes de sensores sem fio, LLNs e IoT. Ao medir o tempo em que o protocolo ficou indisponível durante os ataques foi possível verificar a capacidade de manutenção da rede sob ataque, o tempo de adaptação para a nova topologia, e a partição da rede causada pelos atacantes.

4. Resultados e Discussões

Nesta seção são apresentados os resultados das simulações dos três diferentes ataques (*Blackhole*, *Greyhole* e *Flooding*) em diferentes densidades de atacantes, distâncias do sorvedouro e *drop ratio* do ataque *Greyhole*.

Ao analisar o comportamento da rede, observa-se que a efetividade dos ataques em atrapalhar o roteamento de pacotes e isolar nós da rede depende de: (i) topologia da rede, (ii) localização dos atacantes, e (iii) árvore do protocolo de roteamento.

Considerando os ataques *Blackhole* e *Greyhole*, esta dependência do posicionamento dos nós da rede e as conexões com seus vizinhos faz com que os nós clientes sejam de um de três perfis: (i) os que possuem rotas com o sorvedouro que não passam por nós atacantes; (ii) aqueles cuja rota atual passa por um nó atacante, mas existe outra rota viável que contorna atacantes; e (iii) aqueles que dependem do roteamento de nós atacantes para chegar ao sorvedouro. A Figura 2(a) mostra a quantidade de requisições concluídas por nó, e os perfis mencionados são vistos como os três patamares no gráfico de barras. No primeiro caso, o nó não é afetado pelo ataque em nenhuma maneira (150 requisições concluídas), além de passar a compartilhar rotas com outros nós ou ter mais nós como filho. No segundo caso (125 requisições concluídas), após certo tempo sem resposta do sorvedouro, a árvore DODAG do protocolo RPL é refeita sem os nós atacantes. Isto ocorre pela natureza da implementação dos ataques e a incapacidade de manter uma comunicação constante com os vizinhos por não transmitir *frames*. No terceiro caso (60 requisições concluídas), ocorre a partição da rede por incapacidade de se comunicar com o sorvedouro sem passar por nós atacantes.



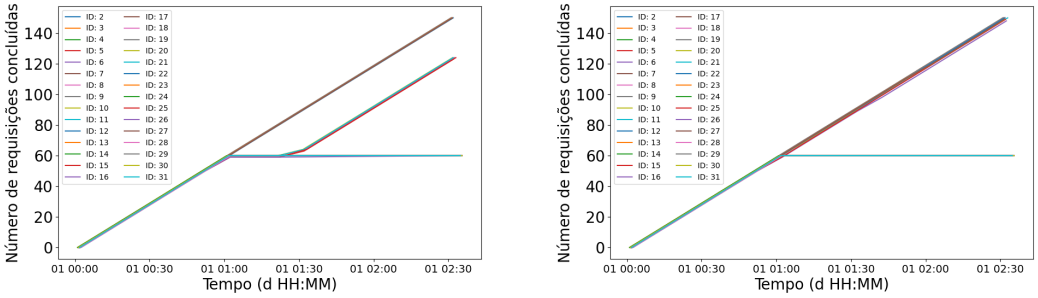
(a) Blackhole com 25% de densidade de atacantes

(b) Greyhole com 25% de densidade de atacantes com taxa de roteamento em 60%

Figura 2. Número de requisições concluídas por cada nó no final da simulação. Nós da rede estão em cinza claro e atacantes em cinza escuro.

A Figura 3 apresenta o número de requisições concluídas por cada nó ao decorrer da simulação. O tempo de readequação da rede é o intervalo entre o início do descarte de pacotes pelos nós atacantes até a recriação da árvore de roteamento para reconectar os nós afetados à rede. Este fator se mostra diferente nos dois ataques (*Blackhole* e *Greyhole*) pela reação do protocolo de roteamento. Nas simulações com o ataque de *Blackhole*, os nós com o segundo perfil apresentaram uma demora de 25 minutos (e perda de 25 pacotes) para perceberem o ataque e reconfigurar a árvore de roteamento. Nos casos de ataque *Greyhole* para a 25% de nós atacantes, o tempo de readequação foi, em média, (i) de 30s para 90% de taxa de encaminhamento; (ii) 1 minuto e 30 segundos para 60%; e (iii) 13 minutos para 30%. Estes resultados estão de acordo com o protocolo de roteamento utilizado, o RPL-Lite do Contiki-NG [Contiki-NG 2022]. O comportamento, aparentemente contraintuitivo, é observado ao comparar as imagens na Figura 3(b), onde as requisições dos nós afetados voltam a ser concluídas antes no cenário do ataque *Greyhole* 3(a).

Na implementação do RPL-Lite do Contiki-NG, os candidatos a pai para cada um dos nós é decidido por parâmeros que tentam diminuir a sobrecarga da rede e aumentar o tempo de vida da rede. O silencio parcial dos pais atacantes *Greyhole* fazem com que os nós percebem que o nó malicioso está próximo e ainda ativo, mas suas métricas estão piores que os outros candidatos à pai. Métricas como *Expected Transmissions* (ETx), taxa de confirmação das mensagens de controle do filho fazem com que a rede seja reconfigurada e as relações de roteamento são corrigidas mais cedo na rede sob ataque *Greyhole* do que *Blackhole*.



(a) Blackhole com 25% de densidade de atacantes

(b) Greyhole com 25% de densidade de atacantes com taxa de roteamento em 60%

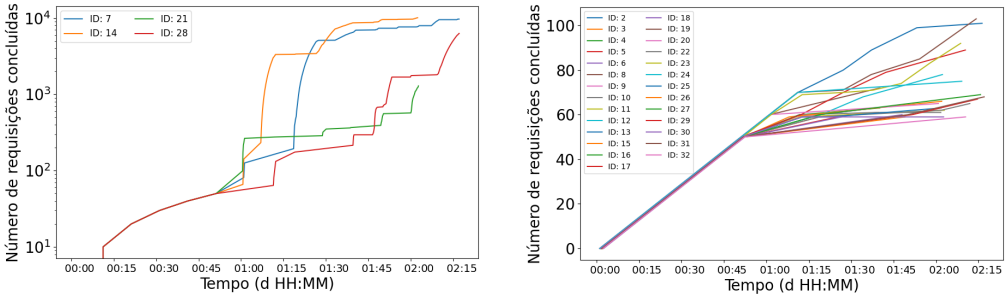
Figura 3. Número de requisições concluídas por cada nó durante a simulação.

Durante a análise das simulações, observou-se que nos dois ataques os nós maliciosos não participam da recriação da árvore de roteamento por não transmitirem nenhum tipo de mensagem de controle com constância. Assim os ataques perdem efetividade após a reestruturação da rede, o que é evidenciado nas Figuras 3 (a) e (b).

Para o ataque de *Flooding* de requisições UDP implementados, no contexto da efetividade do ataque às redes, é possível perceber o impacto da proximidade do nó com sorvedouro da rede. Observou-se que a efetividade do ataque e os impactos característicos na rede está diretamente relacionada a essa proximidade:

- Quando um nó está próximo ao sorvedouro, o ataque se assemelha a uma negação de serviço (DoS). Isso ocorre porque o nó comprometido tem acesso direto ao sorvedouro e pode impactar diretamente a comunicação e o fluxo de dados na rede. Nesse caso, o ataque tem um efeito mais severo devido à sua localização estratégica;
- Quando um nó está distante da raiz da rede ou do sorvedouro, o ataque, além de características do ataque de negação de serviço (DoS), assume características semelhantes a um ataque de *Hello Flood*. Nesse tipo de ataque as grandes quantidades de mensagens do nó atacante devem ser roteadas por outros nós para alcançar o sorvedouro. Esta propagação afeta todos os nós em rotas para o sorvedouro. A distância da raiz torna esses nós em rota mais suscetíveis a esses ataques, pois sua capacidade de comunicação e processamento pode ser sobrecarregada. Este comportamento é observado na Figura 4(a) e (b), com a análise dos nós atacantes e vítimas respectivamente. Os nós competem para utilizar o meio, terem suas mensagens retransmitidas e requisições respondidas pelo sorvedouro. A competição

afeta o desempenho geral da rede, e nós com proximidade do sorvedouro são menos afetados pela inundação da mesma. Todos nós vítimas dos ataques realizam a mesma quantidade de tentativas de envio de mensagens, mas devido a competição pelo meio físico e a necessidade de rotear pacotes de nós maliciosos, o impacto nos nós é diferente.



(a) Nós atacantes **(b)** Nós da rede

Figura 4. Requisições concluídas por tipo de nó durante a simulação (Flooding com 12% de atacantes). Obs.: Eixo y em escala Logarítmica em (a).

Outro impacto relevante foi a quantidade e densidade de nós atacantes na rede. Em uma densidade baixa, no caso de 6% de atacantes, o comportamento de rede sobrecarregada não ocorreu pois o sorvedouro e a largura de banda suportaram a inundação dos dois nós. Isto é evidenciado pela Figura 5, onde os nós atacantes e vítimas possuem uma curva que apresenta crescimento constante e linear, se diferenciando apenas na quantidade de mensagens por segundo na simulação.

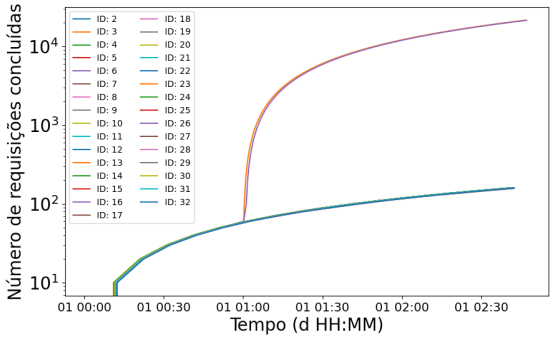


Figura 5. Número de requisições concluídas por cada nó durante a simulação (*Blackhole* com 6% de atacantes). Obs.: Eixo y em escala logarítmica.

Considerando os resultados obtidos nos três ataques podemos destacar as seguintes considerações.

No processo de criação e atualização da árvore DODAG no protocolo RPL-Lite (baseado no RPL definido pela RFC 6550 [Alexander et al. 2012]) são adotados métricas para a escolha de pais para a criação da topologia de rede. Na RFC 6551 [Barthel et al. 2012] a métrica adotada é o número de saltos até a raiz. Como as LLNs lidam com nós com restrição de energia, o protocolo contempla a redefinição da topologia da rede para adaptar a possíveis mudanças. Nós atacantes que não colaboram com

a criação da árvore do protocolo RPL, como os atacantes do tipo *Blackhole* e *Greyhole*, ficam de fora da reestruturação da rede e quando ela ocorre. Essa abordagem visa otimizar a escolha dos nós pais, mas também ajuda a evitar ataques dos tipos listados acima.

Além disso, observou-se que a efetividade dos ataques pode variar consideravelmente dependendo da localização dos nós atacantes perante o sorvedouro. Conforme ilustrado na Figura 1(b), observa-se que, no caso de múltiplos de quatro atacantes, nas partes superior esquerda e inferior direita ocorrem partições da rede. Com a partição, os nós destas regiões são impossibilitados de transmitir e receber dados do sorvedouro até o final da simulação. Com múltiplos de 13, temos um atacante vizinho ao sorvedouro e outro distante do mesmo. Este é um caso interessante para a análise do impacto da distância do atacante no funcionamento da rede. Para o caso de múltiplos de sete atacantes, temos atacantes distribuídos na rede com distância intermediária ao sorvedouro.

Conhecendo a topologia de rede e seu funcionamento padrão, ao realizar a comparação com o comportamento apresentado por uma rede comprometida é possível inferir a localização aproximada do nó malicioso e do tipo de ataque implementado. Observando a métrica de taxa de resposta do sorvedouro é possível identificar o início de qualquer um dos três ataque, quando a métrica diverge do comportamento original da rede. Dado o comportamento individual do nós da rede afetados a localização aproximada do nó atacante pode ser inferida. No ataque *Flooding*, o nó é identificado pelo número significativamente maior de requisições ao sorvedouro. Para os ataques *Blackhole* e *Greyhole*, a rede é segmentada no local do nó atacante e todos os nós que dependiam dele para se comunicar se apresentam à rede como indisponíveis até a reconfiguração da árvore de roteamento. Esta consequência apresenta uma aproximação da posição do nó malicioso, devido ao seus efeitos nos outros nós da rede. A indisponibilidade do protocolo de roteamento também é útil para a identificação das características dos ataques. Por exemplo, auxilia na depuração de tipo de ataque a qual a rede está submetida.

5. Trabalhos Relacionados

Entender como se comporta uma rede que está sobre ataque por meio de padrões de comportamento de rede é uma técnica comum no escopo de redes IoT, LLNs e RSSFs para criar sistemas capazes de identificar a ocorrência destes ataques. Nesta seção são destacadas as contribuições deste artigo e a comparação com outros trabalhos relacionados à análise de comportamento de rede sob ataque.

Tripathi et al. discutem o impacto dos ataque de *Blackhole* e *Greyhole* no protocolo LEACH em redes de sensores sem fio (RSSF) [Tripathi et al. 2013]. O ataque de *Blackhole* descarta todos os pacotes de dados, resultando em interrupção da comunicação. Já o ataque de *Greyhole* descarta seletivamente os pacotes, descartando uma porcentagem dos recebidos. O estudo busca avaliar como esses ataques afetam o desempenho do protocolo LEACH. Esta análise de comportamento de rede para identificação de padrões de funcionamento para realizar uma inferência de integridade da rede.

Ioannou e Vassiliou abordam a análise e o impacto de ataques de camada de rede em RSSF [Ioannou and Vassiliou 2016]. Os ataques estudados incluem *Blackhole*, *Greyhole* e *Flooding*, que comprometem o funcionamento e a segurança das RSSFs. O estudo utiliza simulações para coletar métricas e avaliar os efeitos desses ataques em uma rede UDP utilizando um protocolo de roteamento próprio, chamado de *Weighted Shortest*

Path (WSP). O artigo demonstra que esses ataques podem causar sobrecarga do sorvedouro e perda de pacotes por mudar o roteamento de maneira a absorver pacotes vizinhos se passando por um nó com proximidade ao sorvedouro. Sarao implementa ataques focados em redes *ad hoc* que preveem mobilidade: *Blackhole*, *Grayhole* e *Rushing*. As simulações consideram os protocolos IEEE 802.11 e AODV. Nota-se a diminuição da vazão da rede e o aumento do atraso fim-a-fim na rede sob ataque [Sarao 2022].

Após a padronização da IETF sobre *Low-power and Lossy Networks*, grande parte dos artigos passaram a utilizar a pilha de protocolos IETF como padrão. Tomić e McCann discutem as consequências de ataques do tipo *Blackhole*, *Hello Flood*, *Replay*, *Selective Forwarding*, *Sinkhole* e *Sybil* sob a ótica de vulnerabilidades dos protocolos de roteamento [Tomić and McCann 2017]. Sidhu e Sachdeva relatam a implementação e coleta as métricas dos ataques *Blackhole*, *Greyhole*, *Dropping Node* e *Drop RREQ, RREP e RERR* em um *testbed* de 15 sensores [Sidhu and Sachdeva 2020]. A análise dos ataques de camada de rede são feitas pelas métricas coletadas da rede física sob cada um dos ataques. Rehman et al. apresenta um ataque à estrutura de árvore do protocolo RPL, o ataque ao *Rank* do nó, este ataque de protocolo de roteamento [Rehman et al. 2016]. A análise do comportamento de rede é pautada na diminuição de vazão e aumento do atraso gerados pela criação de rotas falsas na rede. Estes artigos utilizam de ataques à protocolos e padrões utilizados na pilha IETF.

A Tabela 1 apresenta o resumo da seção de revisão de literatura com os trabalhos relacionados. Observa-se não só a falta de artigos que se propõe a discutir a consequência dos ataques relacionados à camada de rede, mas uma escassez deste tipo de análise para ataques em outras camadas da pilha de protocolo. Para realizar a análise de comportamento de rede visando abranger essa lacuna na literatura, foram implementados três ataques: *Blackhole* e *Greyhole* de camada de enlace e *Flooding* de camada de transporte. Os ataques foram simulados com diferentes densidades de nós atacantes e posições relativas ao servidor da rede, e foram analisados a taxa de resposta das requisições cliente-servidor e o tempo de readequação à rede após o ataque.

Os artigos indicados na Tabela 1 que implementam os ataques Blackhole, Greyhole e Flooding relatam uma diminuição na taxa de entrega de pacotes dos nós. Este fato também foi evidenciado nos resultados obtidos por esta pesquisa com a diminuição do número de requisições concluídas nos nós vítimas do ataque. Para uma posição fixa dos atacantes na rede, [Ioannou and Vassiliou 2016] analisaram como variar a posição do sorvedouro impactava as métricas de desempenho da rede. Este impacto, com diferentes consequências, também foi evidenciado nas análises deste trabalho ao variar a posição relativa do nó atacante usando o protocolo RPL na camada de rede.

6. Conclusões e Trabalho Futuro

Dada a lacuna na literatura sobre a análise de comportamento de rede, o objetivo deste trabalho foi entender o comportamento da rede em um cenário IoT sob diferentes ataques. Assim, foram realizadas diferentes simulações variando densidade dos atacantes e distância dos nós maliciosos até o servidor. Os resultados obtidos e analisados destacam as diferenças de comportamento de rede sob ataque com base em sua topologia. A compreensão da reação da rede é essencial para desenvolver estratégias de proteção e mitigação destes ataques. Utilizando as métricas de taxa de resposta do ser-

Tabela 1. Resumo comparativo de literatura relacionada em termos de contexto, ataques implementados, configuração e implementação da rede

Trabalho	Contexto	Ataques Implementados	Configuração de Rede	Plataforma de Experimentação
[Tripathi et al. 2013]	RSSF	Blackhole, Greyhole	Não define camada física e de enlace, LE-ACH	Network Simulator 2 (NS-2)
[Ioannou and Vassiliou 2016]	RSSF	Blackhole, Greyhole, Flooding	IEEE 802.15.4 + WSP	ContikiOS/Cooja
[Tomić and McCann 2017]	RSSF	Blackhole, Hello Flood, Replay, Selective Forwarding, Sinkhole, Sybil	IEEE 802.15.4 + Padrão IETF	ContikiOS/Cooja
[Sidhu and Sachdeva 2020]	RSSF	Blackhole, Greyhole, Dropping Node, Drop RREQ, RREP, RERR	IEEE 802.15.4 + Padrão IETF	Testbed
[Sarao 2022]	MANET	Blackhole, Grayhole, Rushing	IEEE 802.11 + AODV	Network Simulator 2 (NS-2)
[Rehman et al. 2016]	IoT	Rank	IEEE 802.15.4 + Padrão IETF	ContikiOS/Cooja
Este trabalho	IoT	Blackhole, Greyhole, Flooding	IEEE 802.15.4 + Padrão IETF	Contiki-NG/Cooja

vidor à requisição dos clientes foi possível encontrar o início do ataque e, comparando à organização original da rede, a localização aproximada do nó atacante. O número de pacotes perdidos pela indisponibilidade do protocolo de roteamento da rede depura o tipo de ataque a qual a rede está sendo submetida, principalmente na classificação de ataques que ocorrem na mesma camada, como o *Blackhole* e *Greyhole* deste trabalho. A implementação dos ataques está disponível no Github: `https://github.com/AleMarquis/ArtigoWTICGSBSeg23`

Pretendemos aumentar o número de métricas analisadas e coletadas nas simulações futuras visando a análise dos dados obtidos. Esta coleta se faria útil para a criação de um *dataset* público com métricas de rede padrão IETF sob ataque.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, projeto FAPESP #2022/07523-8 e Itaú Unibanco S.A. pelo programa PBI do Centro de Ciência de Dados (C2D) da Escola Politécnica da Universidade de São Paulo. 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.

Bansal, S. and Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks*, 27.

Barthel, D., Vasseur, J., Pister, K., Kim, M., and Dejean, N. (2012). Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks. RFC 6551.

Contiki-NG (2022). Rpl — contiki-ng documentation. `https://docs.contiki-ng.org/en/develop/doc/programming/RPL.html`. Acessado em: 11/jul/2023.

Contiki-NG (2023). Docker — contiki-ng documentation. https://docs.contiki-ng.org/en/develop/doc/getting-started/Docker.html. Acessado em: 11/jul/2023.

Deogirikar, J. and Vidhate, A. (2017). Security attacks in iot: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pages 32–37.

Ganapathi, P. and D, S. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security*, 4.

Ioannou, C. and Vassiliou, V. (2016). The impact of network layer attacks in wireless sensor networks. In *2016 International Workshop on Secure Internet of Things (SIoT)*, pages 20–28.

Oikonomou, G., Duquennoy, S., Elsts, A., Eriksson, J., Tanaka, Y., and Tsiftes, N. (2022). The Contiki-NG open source operating system for next generation IoT devices. *SoftwareX*, 18:101089.

Palattella, M., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L., Boggia, G., and Dohler, M. (2013). Standardized protocol stack for the internet of (important) things. *IEEE Communications Surveys 'I&' Tutorials*, 15(3):1389–1406.

Rehman, A., Khan, M., Lodhi, M., and Hussain, F. (2016). Rank attack using objective function in rpl for low power and lossy networks. In *2016 International Conference on Industrial Informatics and Computer Systems (CIICS)*, pages 1–5.

Sarao, P. (2022). Performance analysis of manet under security attacks. *J. Commun.*, 17(3):194–202.

Sidhu, N. and Sachdeva, M. (2020). Impact analysis of network layer attacks in real-time wireless sensor network testbed. *International Journal of Advanced Computer Science and Applications*, 11.

Tomić, I. and McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal*, 4(6):1910–1923.

Tripathi, M., Gaur, M., and Laxmi, V. (2013). Comparing the impact of black hole and gray hole attack on leach in wsn. *Procedia Computer Science*, 19:1101–1107. The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), the 3rd International Conference on Sustainable Energy Information Technology (SEIT-2013).

Zarpelão, B., Miani, R., Kawakani, C., and de Alvarenga, S. (2017). A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37.

Zhou, Y., Fang, Y., and Zhang, Y. (2008). Securing wireless sensor networks: a survey. *IEEE Communications Surveys 'I&' Tutorials*, 10(3):6–28.

Zolertia (2013). Z1 - zolertia. https://zolertia.sourceforge.net/wiki/index.php/Z1. Acessado em: 11/jul/2023.