Análise de Vazamentos Temporais *Side-Channel* no Contexto da Internet das Coisas

Nelson G. Prates Jr.[1], **Andressa Vergütz** [1], **Ricardo T. Macedo**[2], **Michele Nogueira**[1]

[1]Centro de Ciência de Segurança Computacional (CCSC) – UFPR
[2]Depto. de Tecnologia da Informação - Campus Frederico Westphalen – UFSM

{ngpjunior,michele,avergutz}@inf.ufpr.br, rmacedo@inf.ufsm.br

Abstract. *The Internet of Things (IoT) enables common objects to be equipped with sensors, motivating new forms of applications. These objects collect data from users and the environment, making them interesting targets for attackers who want to access or manipulate them. However, even with the encrypted data, side-channel attacks exploit the devices characteristics in order to infer information that can compromise the security of the network structure. In the literature, most of the works that exploit these attacks do not consider scenarios composed of standard protocols for IoT, which exploit do not consider the identification of identical devices. This work presents a way of characterizing the identical IoT devices by exploring only the time information. For this, activities were carried out such as structuring an experimental scenario, collecting the traffic, extracting statistical characteristics and finally identifying devices. The results show that even identical devices can be identified with 100% accuracy.*

Resumo. *A Internet das Coisas (IoT) possibilita que objetos comuns sejam equipados com sensores, motivando novas formas de aplicações. Estes objetos coletam dados dos usuários e do ambiente, o que os tornam alvos interessantes para atacantes que almejam acessá-los ou manipulá-los. Entretanto, mesmo com os dados criptografados, os ataques side-channel exploram as características dos dispositivos, a fim de inferir informações que podem comprometer a segurança da estrutura da rede. Na literatura, a maior parte dos trabalhos que exploram estes ataques, não consideram cenários compostos por protocolos padronizados para a IoT, os que exploram, não consideram a identificação de dispositivos idênticos. Este trabalho apresenta uma forma de caracterizar os dispositivos IoT idênticos explorando unicamente a informação tempo. Para isso, foram realizadas atividades como estruturar um cenário experimental, coletar o tráfego, extrair características estatísticas e, por fim identificar os dispositivos. Os resultados apontam que mesmo dispositivos idênticos podem ser identificados com até 100% de precisão.*

1. Introdução

A IoT tem proporcionado a criação de ferramentas a exemplo de redes de comunicação seguras para monitorar a saúde de pessoas em suas atividades do cotidiano, informando transeuntes próximos sobre sua situação emergencial, ou ainda dispositivos capazes de predizer se há a iminência de um ataque cardíaco e assim acionar médicos ou serviços de socorro [Vergütz et al. 2017]. Com a IoT nesse processo de expansão é gerado um

significativo volume de dados sobre diversos aspectos. Como exemplo didático, a coleta de temperatura do ambiente, associada à intensidade do trânsito e a pressão arterial ou ritmo cardíaco de um motorista podem ser avaliados em tempo real e assim confirmar ou refutar correlações. Dessa forma, a IoT proporciona novos serviços, disponibiliza novos recursos, possibilita a criação de cidades mais inteligentes, além de ser atraente para os negócios devido ao volume de dados gerados que permite a melhor compreensão do comportamento de consumo, interesses pessoais, entre outros.

Todavia, devido ao volume e tipo de informação proporcionado pela IoT, ela se torna alvo dos ataques *side-channel* que se aproveitam de todo ou qualquer dado trafegado mesmo que criptografados (vazamentos *Side-Channel*) [Sayakkara et al. 2019]. Os atacantes, mediante *sniffers* que capturam o tráfego de rede, sondam os vazamentos *side-channel* como o tempo de resposta e o tamanho dos pacotes [Yan et al. 2017]. Tais vazamentos *side-channel* consistem de informações, que muitas vezes vazados de forma não intencional, podem ser classificados a fim de inferir informações que revelam características da rede e até mesmo o comportamento dos dispositivos e/ou protocolos. Além disso, a quebra da privacidade causada por esses ataques pode revelar informações e comportamento dos usuários e dos dispositivos. Por exemplo, [Srinivasan et al. 2008] inferiram informações sobre os usuários por meio de análises do tráfego em um cenário de casa inteligente (*smart-home*). Essas informações são adquiridas através da similaridade do tempo de resposta das transmissões realizadas pelos dispositivos IoT. Isso possibilita a identificação de cômodos, quantidade de residentes e até mesmo possíveis visitantes. Também, os dispositivos IoT tendem a transmitir informações cada vez mais pessoais/privadas dos usuários, como dados vitais, de posicionamento, de operações/serviços empresariais, entre outros. Entretanto, a maioria dos estudos da literatura que abordam este tipo de ataque não consideram os protocolos específicos para IoT, como 6LoWPAN e o CoAP.

Na literatura existem estudos que exploram o vazamento temporal *side-channel*. Todavia, a maioria dos trabalhos que realizam análises temporais sobre o tráfego de rede consideram os protocolos de rede tradicionais, como TCP/IP, IEEE 802.11 e HTTPs [Veysset et al. 2002, Srinivasan et al. 2008, Feghhi and Leith 2016]. Existem estudos que mencionam os dispositivos IoT [Apthorpe et al. 2017, Conti et al. 2018]. Entretanto, tais estudos também seguem os protocolos das redes tradicionais. O estudo de [Selis and Marshall 2017], apesar de considerar outro tipo de ataque, apresentou uma forma de caracterizar o comportamento de dispositivos IoT através do tempo de resposta de forma eficiente. Porém, os autores consideraram apenas o comando PING do protocolo ICMP. Finalmente, encontrou-se apenas um trabalho que considera os protocolos desenvolvidos para a IoT [Yan et al. 2017], onde os autores exploraram o comportamento de diferentes dispositivos IoT através das informações sobre o tamanho dos pacotes e tempo de resposta. No entanto, nenhum dos trabalhos encontrados na literatura diferenciam dispositivos IoT que apresentam características idênticas, *i.e.*, mesma marca, modelo, protocolos e programas em execução, através de análises temporais do tráfego de rede.

Neste sentido, este trabalho apresenta uma análise sobre o vazamento temporal *side-channel*, a fim de caracterizar e identificar dispositivos idênticos em uma rede IoT. Através desta análise pretende-se motivar o desenvolvimento de sistemas de gerência de monitoramento e segurança que necessitem da identificação de dispositivos. Além disso, motivado pela violação de privacidade e consequências causadas por tais ataques,

pretende-se destacar a relevância das informações *side-channel* na caracterização do tráfego de dispositivos mesmo idênticos. Para este fim, a análise proposta compreende a coleta do tráfego empírico de dispositivos IoT, a extração das informações *side-channel* para criação dos cenários e a identificação dos dispositivos. As informações *side-channel* consideradas englobam o `timestamp` e o tempo de resposta, bem como suas medidas estatísticas. Por meio desse conjunto de informações, esta análise apresenta um comportamento único e específico de cada dispositivo considerado.

A avaliação da caracterização e identificação propostas empregam tráfego de dados empíricos gerados e capturados através de um cenário experimental executando os principais protocolos IoT, como 6LoWPAN e CoAP. Para isso, gera-se tráfego de três dispositivos IoT Memsic Iris idênticos embarcados com sensores de iluminação e de temperatura ambiente. Na ferramenta de monitoramento de redes Wireshark[1] realiza-se a coleta do tráfego e o monitoramento da conexão do cliente CoAP. Na ferramenta de análises estatísticas RStudio[2] selecionam-se e extraem-se as características sobre as capturas de rede, como `timestamp` e tempo de resposta. Embasado nessas características, analisa-se o comportamento único de cada dispositivo IoT. Na ferramenta de mineração de dados WEKA[3], aplicam-se classificadores de aprendizagem de máquina para identificar os dispositivos. Além disso, analisa-se a eficiência de cada classificador através de métricas como acurácia e *F-Score*. Os resultados observados nas análises apontam que é possível caracterizar e classificar dispositivos idênticos, alcançando taxas de precisão de até 100%.

O restante do artigo está organizado como segue. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha a análise do vazamento *side-channel*. A Seção 4 descreve a metodologia de avaliação. A Seção 5 apresenta e discute os resultados obtidos. Por fim, a Seção 6 conclui o trabalho e apresenta as direções futuras.

2. Trabalhos Relacionados

Na literatura existe uma vasta quantidade de trabalhos que analisam vazamentos *side-channel* em diferentes contextos, porém poucos consideram os protocolos padronizados para a IoT. Entretanto, os dispositivos IoT possuem características específicas como mobilidade e escassez de recursos energéticos. Devido a isso, implementar os protocolos já padronizados pela Internet, que foram projetados para dispositivos mais robustos e conexões confiáveis, se torna inviável na maioria dos cenários IoT. Em vista disso, a IETF (*Internet Engineering Task Force*), através da RFC 4944 [Montenegro et al. 2007a], RFC 4919 [Montenegro et al. 2007b], RFC 7252 [Shelby et al. 2014] e RFC 6347 [Rescorla and Modadugu 2012], padronizou os protocolos IEEE 802.15.4 (Física), 6LoWPAN (Rede), CoAP (Aplicação), DTLS (Segurança fim-a-fim), respectivamente, com o objetivo de atender aos dispositivos com recursos limitados da IoT [Prates et al. 2018]. Neste contexto, [Chen et al. 2010] e [Yan et al. 2017] apresentaram as características que podem ser extraídas através do vazamento e os potenciais ataques *side-channel* direcionados para protocolos de redes tradicionais e para o protocolo *6LoWPAN*, respectivamente. Contudo, [Yan et al. 2017] provam a existência dos Vazamentos *Side-Channel* e quais características eles podem revelar sobre a estrutura. Além disso, destacaram a carência

[1]Wireshark, https://www.wireshark.org/. Último acesso em Mar/2019.

[2]RStudio, https://www.rstudio.com/. Último acesso em Mar/2019.

[3]WEKA, https://www.cs.waikato.ac.nz/ml/weka/. Último acesso em Mar/2019.

de trabalhos que exploram este tipo de ataque considerando os protocolos para IoT. A justificativa para tal carência consiste da recente padronização destes protocolos.

Por outro lado, existem estudos que analisam o vazamento *side-channel* para inferir informações sobre os tipos de dispositivos, aplicações, sistemas operacionais, etc. [Sivanathan et al. 2018] coletaram os dados de diferentes dispositivos IoT e analisaram as características que auxiliam na descrição do comportamento dos mesmos, como números de portas e padrões de atividades. Além disso, os autores utilizaram algoritmos de classificação para identificar os dispositivos. Entretanto, os autores consideraram informações de entrada de alto nível, como a incidência de palavras chaves e o tráfego de pesquisas em servidores DNS. Em outro contexto, [Saltaformaggio et al. 2016] analisaram informações do cabeçalho IP para classificar sistemas operacionais móveis. Nas análises os autores caracterizaram o tráfego de dados por meio de métodos estatísticos e *clusterizadores*. No entanto, estes estudos consideraram somente o tráfego *web* do protocolo HTTP. [Taylor et al. 2018] exploraram as informações sobre o tamanho e a direção dos pacotes por meio de vazamento *side-channel* a fim de identificar aplicativos móveis. Para isso, os autores mitigaram o efeito de tráfego ambíguo (tráfego comum entre os aplicativos) como anúncios. Apesar dos esforços dos estudos na análise de informações sobre o tráfego de dados, eles não consideraram os protocolos específicos para IoT, focando somente nos protocolos desenvolvidos para as redes tradicionais da arquitetura TCP/IP.

Além do mais, os estudos supracitados analisam o comportamento de dispositivos, sistemas e/ou aplicações por meio de diferentes informações e características do tráfego, como tamanho dos pacotes e expressões regulares. [Yan et al. 2017] observaram as características de tamanho dos pacotes e o tempo de resposta em um cenário composto por diferentes dispositivos, onde destacaram a importância da característica tempo. A informação sobre o tempo de resposta apresenta menor quantidade de ruído quando comparada ao tamanho do pacote, e com isso, alcança uma precisão maior na classificação do tráfego. Esta importância é reforçada através do trabalho de [Srinivasan et al. 2008], onde os autores, através de análises estatísticas, utilizaram o tempo coletado do tráfego de sistemas RFID para inferir informações pessoais dos usuários. Contudo, existem estudos que apontam a possibilidade de avaliar tal comportamento considerando apenas as informações relacionadas ao tempo do pacote. Por exemplo, [Veysset et al. 2002] caracterizaram sistemas operacionais através de análises sob o tempo RTT dos pacotes do tráfego TCP. [Feghhi and Leith 2016] classificaram páginas *web* utilizando somente a informação de tempo capturada através do tráfego de dados. [Malik et al. 2017] identificaram diferentes características dos sistemas operacionais móveis para classificar as aplicações ativas. Os testes seguiram uma série de requisições do tipo PING, onde os intervalos de tempo entre as respostas foram analisados para identificar as aplicações.

Também existem estudos que exploram as informações sobre o tempo de resposta para auxiliar na defesa contra ataques de redes. [Selis and Marshall 2017] propuseram um modelo de detecção que identifica máquinas virtuais intrusas falsificando o tempo de resposta. Entretanto, apesar de ser no contexto IoT, tal estudo não emprega os protocolos IoT. Desse modo, de acordo com o melhor do nosso conhecimento, não existem estudos que analisam o comportamento de dispositivos IoT, considerando as características e protocolos específicos da IoT. Além disso, não existem estudos que diferenciem o comportamento de dispositivos IoT idênticos (mesma marca, modelo e protocolos IoT). Neste

sentido, o diferencial deste trabalho consiste em caracterizar dispositivos IoT idênticos apenas utilizando informações sobre o tempo de resposta, ou seja, apenas considerando características do vazamento temporal *side-channel*.

3. Análise de Vazamentos Temporais *Side-Channel*

Esta seção descreve a análise de vazamento temporal *side-channel* no contexto de redes IoT, a fim de auxiliar na melhoria das técnicas de gerência de monitoramento e segurança. Em particular, explora-se a informação relacionada ao tempo, adquirida através da captura do tráfego de redes IoT. Além disso, caracteriza-se e identifica-se dispositivos da mesma marca e modelo, com os mesmos protocolos e programas em execução. Para isso, as próximas subseções discutem os efeitos que as informações inferidas através do tempo podem causar no contexto da privacidade dos dados dos usuários, apresentam o cenário experimental de rede e por fim, detalham a caracterização dos dispositivos.

3.1. Discussão sobre a Informação Tempo

A informação tempo pode revelar o comportamento dos dispositivos em rede, levando a violação da privacidade dos dados. Devido ao comportamento do dispositivo se tratar de uma informação extremamente valiosa, os atacantes buscam encontrar padrões para inferir informações sobre cada dispositivo presente na rede. Estes padrões, na maioria das vezes, são explorados através do tempo de execução de toda a pilha de programas dos dispositivos. Com base na literatura, as análises sobre o vazamento temporal *side-channel* de fato revelam informações tanto das camadas inferiores no nível de *hardware* (por exemplo, sobre os sensores embarcados), como sobre as camadas superiores no nível de *software* (por exemplo, sobre os aplicativos em execução) [Yan et al. 2017].

Programas de computador contêm ramificações e laços de repetições condicionais para manipular entradas e produzir a saída pretendida. Dependendo dos valores de entrada, o caminho de execução de um programa pode diferir, resultando em um tempo de execução de programa diferente [Sayakkara et al. 2019]. Em um cenário composto por dispositivos IoT estes padrões podem se destacar, pois a escassez de recursos exige que os programas desenvolvidos sejam compostos por blocos de código menores e que envolvam operações mais específicas. Além disso, o tempo de execução desses códigos podem ser diferentes de um dispositivo para o outro devido à divergência de capacidade computacional, como poder de processamento, memória, bateria, entre outros. Alguns parâmetros estruturais dos cenários de redes também podem ser explorados, como a portabilidade dos dispositivos que motivam a geração de novas características no decorrer do tempo. Estas características também podem servir como informação para identificar dispositivos. A variável mais explorada pela literatura para este fim é o tempo de resposta.

As especificações definidas pelo protocolo 6LoWPAN exigem que os dispositivos estejam conectados a uma estação base (*gateway*). Esta configuração pode ser explorada pelos atacantes, pois o *gateway* possibilita que conexões externas à estrutura de rede sejam realizadas através de um ponto central. Entretanto, a captura do tráfego deste dispositivo, mesmo que criptografado, pode gerar brechas através da exploração do tempo de resposta. Este tempo pode ser explorado com o objetivo de inferir informações sobre o posicionamento e o comportamento dos dispositivos. No entanto, as informações capturadas também podem ser exploradas para auxiliar a gerência de monitoramento das redes.

Um exemplo prático é a necessidade de identificar sensores de monitoramento de saúde para oferecer prioridade de transmissão na rede.

Entretanto, existe um questionamento sobre a possibilidade de diferenciar dispositivo idênticos da mesma marca, modelo e com os mesmos protocolos e aplicações em execução por meio unicamente do vazamento temporal *side-channel*. Em vista disso, este trabalho propõem uma análise sobre os vazamentos temporais *side-channel*, a fim de diferenciar e caracterizar dispositivos idênticos estruturalmente. Para este fim, foi estruturada uma rede experimental para simular um cenário IoT, realizar capturas do tráfego de rede e caracterizar dispositivos. Esta coleta compreende a comunicação direta entre dois dispositivos, incluindo os atrasos e as falhas que podem ocorrer durante a troca de mensagens. O cenário compreende três dispositivos idênticos, agindo como servidores de dados. Onde nos quais, recebem requisições de um cliente que acessa a estrutura de rede através de um roteador de borda. O tráfego é capturado e a partir dele são extraídas as informações para a criação de cenários, obtidos através de características estatísticas. Por fim, a identificação dos dispositivos é realizada através do uso de classificadores.

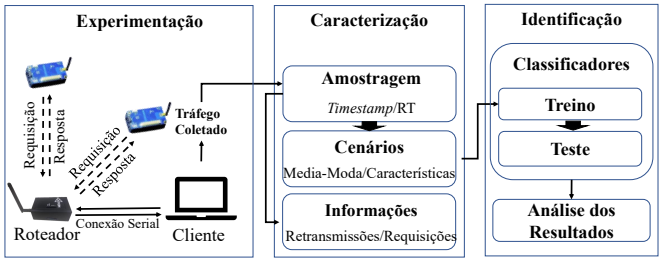


Figura 1. Etapas da Análise dos Vazamentos

Figura 2. Cenário Experimental

3.2. Cenário Experimental de Rede

A experimentação visa simular uma aplicação IoT, utilizando os principais protocolos padronizados pela IETF. Para isso, o cenário experimental é composto por quatro dispositivos IoT Memsic Iris e um computador. Os dispositivos IoT realizam diferentes operações, três deles agem como servidores e o último como estação base. Estes dispositivos IoT são equipados com *chips* Atmel's AT86RF230 compatíveis com as especificações IEEE 802.15.4 [Montenegro et al. 2007a]. Além disso, nos dispositivos podem ser acoplados placas proprietárias de sensores. As utilizadas neste cenário são as placas *MTS300CB* equipadas com sensores de iluminação e temperatura. A estação base, por sua vez, atua como um *gateway* e roteador de borda, ou seja, recebe e encaminha as requisições externas. Todos os dispositivos IoT executam o Contiki SO, com os protocolos de rede 6LoWPAN [Montenegro et al. 2007b], RPL [Thubert et al. 2017] e UDP. Para a aplicação, o protocolo CoAP [Shelby et al. 2014]. Por fim, o computador simula um cliente CoAP gerando requisições e capturando o tráfego gerado. A simulação do cliente é feita através do *framework* Californium[4] e as capturas são realizadas através da ferramenta Wireshark. O computador e o roteador de borda são interconectados através de uma interface serial/USB. A Figura 2 apresenta o cenário experimental. Considerando este cenário, também é importante afirmar que os servidores só realizam a captura dos sensores a partir do recebimento de uma requisição.

[4]Californium (Cf) https://www.eclipse.org/californium/. Último acesso em Mar/2019

3.3. Detalhamento da Caracterização e Identificação

Esta subseção detalha as fases de caracterização e identificação dos dispositivos IoT. A caracterização dos dispositivos é dividida em três etapas: *(i)* amostragem dos dados coletados, *(ii)* extração de características estatísticas para criação dos cenários e *(iii)* extração de informações extras (exemplo, taxa de retransmissões), conforme apresentado na Figura 1. A partir das coletas de tráfego da fase experimental, a amostragem desses dados segue a extração das informações sobre o `timestamp` e o tempo de resposta. Assim, cada amostra criada contém o `timestamp` de envio da requisição, o `timestamp` de recebimento da resposta e o tempo de resposta. Em seguida, extraem-se as medidas estatísticas, como média e mediana, para a criação de dois cenários de análises: um que engloba um subconjunto de medidas estatísticas e outro que envolve todas as medidas estatísticas, sendo elas média, moda, mediana, limite superior e inferior, e correlação. A entrada para a computação dessas medidas estatísticas compreende os dados extraídos na amostragem, ou seja, o `timestamp` e o tempo de resposta. Além das medidas estatísticas, a partir das amostragens de dados obtêm-se informações acerca da taxa de retransmissão e quantidade de requisições de cada dispositivo. Assim, todas essas informações em conjunto auxiliam na caracterização dos dispositivos. Em seguida, submetem-se os cenários criados com as medidas estatísticas para a fase de identificação dos dispositivos. Nesta fase, cria-se o conjunto de dados de treino e teste, para então realizar a identificação de cada dispositivo. Por fim, computam-se as métricas de desempenho para avaliação da identificação.

4. Avaliação de Desempenho

Neste estudo é analisado o vazamento de informações *side-channel* e o comportamento do tráfego considerando um cenário experimental. Particularmente, no cenário base foi coletado o tráfego de rede através da ferramenta de monitoramento de redes Wireshark. Neste cenário, um cliente realiza requisições para três dispositivos IoT Memsic Iris, que agem como servidores CoAP. A partir da captura, na ferramenta de análises estatísticas RStudio foram extraídas as características relevantes em relação ao tráfego, como tempo de resposta e tempo de envio dos dispositivos. Além disso, foram computadas as medidas estatísticas como média, mínima e moda. Tais características serviram como entrada para a caracterização do comportamento específico de cada dispositivo e para a identificação do tráfego dos mesmos. Na ferramenta de mineração de dados WEKA foram identificados os dispositivos IoT por meio de classificadores, como *Naive Bayes* e KNN. Neste sentido, as próximas subseções apresentam a metodologia de avaliação e os cenários de avaliação.

Seleção e Extração das Características

O conjunto de dados empregado nessa análise foi coletado a partir de três servidores que possuem sensores de monitoramento de iluminação e de temperatura ambiente, como detalhado na Seção 3.2. Os dados estão distribuídos em seis subconjuntos, intitulados de *Nó 1-l*, *Nó 2-l* e *Nó3-l* para os sensores de iluminação, e *Nó 1-t*, *Nó 2-t* e *Nó 3-t* para os sensores de temperatura. Cada subconjunto de dados contém uma coleta de 100.000 requisições, as quais foram divididas em 1.000 amostras de 100 requisições. A captura do tráfego foi realizada na perspectiva do **cliente**, que registrou um total de 1.226.428 pacotes transmitidos divididos em 626.428 requisições e 600.000 respostas. Além disso, como o objetivo deste estudo consiste em analisar o vazamento de informações *side-channel* de

dispositivos IoT, os dados coletados consistem de gravações normais, sem possuir nenhum tipo de ataque ou variação significante.

Na caracterização do tráfego de cada dispositivo foram considerados os dados referentes ao `timestamp` (T) e tempo de resposta (P) dos pacotes. O `timestamp` consiste do instante em que o pacote foi enviado. Enquanto o tempo de resposta se refere a diferença entre o `timestamp` de envio e o `timestamp` de resposta. Outras características dos dados de tráfego não foram consideradas, como o tamanho do pacote, pois a literatura é pobre em relação a informação tempo para os protocolos da IoT. Além do mais, a possibilidade de caracterizar o comportamento do tráfego de um dispositivo IoT apenas usando a informação tempo aponta ser um vazamento de informação *side-channel* crucial. Técnicas de gerência de monitoramento podem se beneficiar dessas informações para desenvolver novas medidas de segurança.

A fim de refinar a caracterização, foram extraídas medidas estatísticas dos dados selecionados, *i.e.,* `timestamp` de envio e tempo de resposta. Conforme a Tabela 4, as medidas estatísticas consideradas englobam a mínima (min), soma (sum), média (μ), limiar inferior (LI), limiar superior (LS), moda ($mode$), mediana (Md) e coeficiente de correlação de Pearson (r). Para algumas medidas estatísticas os valores de entrada consistem do `timestamp`, enquanto outras medidas seguem o tempo de resposta. Essas definições se embasaram no estudo de [Selis and Marshall 2017]. Para a medida do coeficiente de correlação de Pearson, foi estimado o grau de correlação entre o `timestamp` e o tempo de resposta. Com base nessas medidas, cada subconjunto possui um conjunto específico de informações que contém o tempo de resposta, `timestamp`, medidas estatísticas e rótulo. O rótulo se refere a classe alvo necessária para identificar dispositivos por meio de algoritmos supervisionados. A informação verdadeira (*ground-truth information*) sobre qual tráfego pertence a cada dispositivo foi extraída durante a coleta do tráfego no cenário experimental, o que auxiliou na rotulação da base.

Medida Estatística	**Equação**
Mínima (P)	$min = min(x_i)$
Soma (P e T)	$sum = \sum_{i=1}^{N} x_i$
Média (P)	$\mu = \frac{1}{N} \sum_{i=1}^{N} x_i$
Limiar Inferior (T)	$LI = \mu - 1.96\sigma$
Limiar Superior (P)	$LS = \mu + 1.96\sigma$
Moda (P e T)	$mode = freq(X)$
Mediana (P e T)	$Md = \frac{1}{2}(X_{\frac{N}{2}} + X_{\frac{N}{2}+1})$ de $sort(X)$
Coef. Correlação de Pearson (P e T)	$r = \frac{\sum_{i=1}^{N}(x_i-\mu_x)(y_i-\mu_y)}{\sqrt{\sum_{i=1}^{N}(x_i-\mu_x)^2 \sum_{i=1}^{N}(y_i-\mu_y)^2}}$

X = conjunto de dados; x_i = amostra i dos dados; N = quantidade de amostras; σ = variância; $freq$ = valor mais frequente; $sort$ = valores ordenados.

Tabela 1. Medidas Estatísticas para Caracterização do Tráfego

Cenários de Avaliação

Dois cenários de avaliação (**C1** e **C2**) foram considerados nas análises de vazamento *side-channel* dos dispositivos IoT. Nestes cenários variou-se a quantidade de medidas estatísticas do tráfego de rede utilizadas nas análises. Para isso, foi criado um subconjunto das características estatísticas apresentadas na Tabela 4, o qual engloba apenas a média e a moda do tempo de resposta. Assim, no primeiro cenário (**C1**) foi submetido o tempo

de resposta e o subconjunto de características estatísticas criado. Enquanto, no segundo cenário (**C2**) foram utilizadas todas as características estatísticas, tanto do `timestamp`, quanto do tempo de resposta. Dessa forma, é possível analisar o impacto das medidas estatísticas na caracterização do tráfego de dispositivos idênticos.

Detalhes da Identificação dos Dispositivos

A identificação dos dispositivos IoT engloba cinco algoritmos de aprendizagem de máquina amplamente utilizados e bem conhecidos na literatura [Pacheco et al. 2018]. Tais algoritmos compreendem o algoritmo clássico não paramétrico *K Nearest Neighbors* (KNN), os algoritmos baseados em árvores de decisão *Random Forrest* e *J48* (também conhecido como C4.5), a rede neural *Multilayer Perceptron*, e por fim, o algoritmo embasado na classificação bayesiana *Naive Bayes*. Esses algoritmos são aplicados em problemas de multi-classificação, ou seja, em situações que várias classes de dados precisam ser identificadas. Esta análise segue um problema de multi-classificação, pois objetiva-se identificar o tráfego de dados dos três dispositivos IoT considerados, o que justifica a escolha de tais algoritmos de classificação.

Para validar os algoritmos de classificação seguiu-se a abordagem tradicional que emprega um conjunto de dados de treino (70% dos dados) e teste (30% dos dados), a fim de treinar os modelos de classificação e computar as métricas de desempenho [Pacheco et al. 2018]. O conjunto de dados de treino possui uma captura de 100.000 requisições de dados para cada um dos seis subconjuntos, totalizando 600.000 requisições. As capturas de cada dispositivo com seu respectivo sensor foram divididas em conjuntos de 1.000 amostras, a fim de calcular as características estatísticas da Tabela 4. Assim, após pré-processamento, foi criado um conjunto de treino para ambos os sensores (temperatura e luz) com 3.000 exemplos de dados em cada, incluindo o rótulo dos três dispositivos IoT. O conjunto de dados de teste possui uma captura de 10.000 requisições de dados para cada subconjunto dos dispositivos IoT. Cada captura foi dividida em 100 amostras para computação das características estatísticas. Dessa forma, o conjunto de teste totalizou 300 exemplos de dados para cada sensor.

As métricas de desempenho consideradas envolvem a acurácia, precisão, *recall* e *F-Score* (também conhecida como *F-Measure*). Tais métricas consideram a taxa de verdadeiro positivo (VP), verdadeiro negativo (VN), falso positivo (FP) e falso negativo (FN). Dessa forma, estatisticamente a acurácia se refere a proporção de tráfego de dados classificados corretamente em relação a todas as amostras de tráfego. A precisão (p) estima a porcentagem de verdadeiros positivos dentre todos os exemplos de tráfego classificados como positivos ($VP/(VP + FP)$). O *recall* (r) ou revocação consiste da porcentagem de verdadeiros positivos dentre todos os exemplos cuja classe esperada é a positiva ($VP/(VP + FN)$). Por fim, o *F-Score* faz uma relação entre as medidas de precisão e *recall* através da estimação da média harmônica ($2rp/(r + p)$). Portanto, os resultados dos classificadores se embasam nessas quatro métricas.

5. Resultados

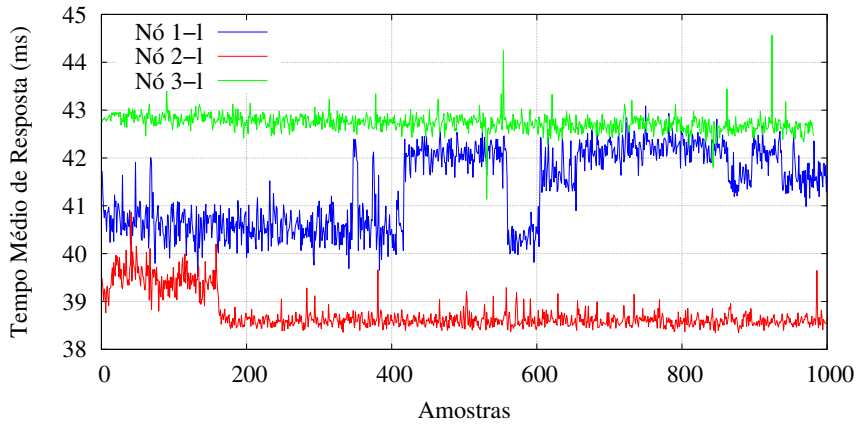
Esta seção apresenta os resultados de caracterização e identificação do tráfego de dispositivos IoT por meio do vazamento temporal *side-channel*. Os resultados seguem dois cenários de avaliação **C1** e **C2**, descritos na Seção 4. Além disso, os resultados se embasam no tráfego de três dispositivos idênticos IoT coletado em um cenário experimental.

Tais dispositivos possuem dois tipos de sensores: um sensor que monitora a iluminação e outro que monitora a temperatura ambiente. Assim, os resultados são apresentados e discutidos seguindo uma análise crítica para cada dispositivo com seu respectivo sensor.

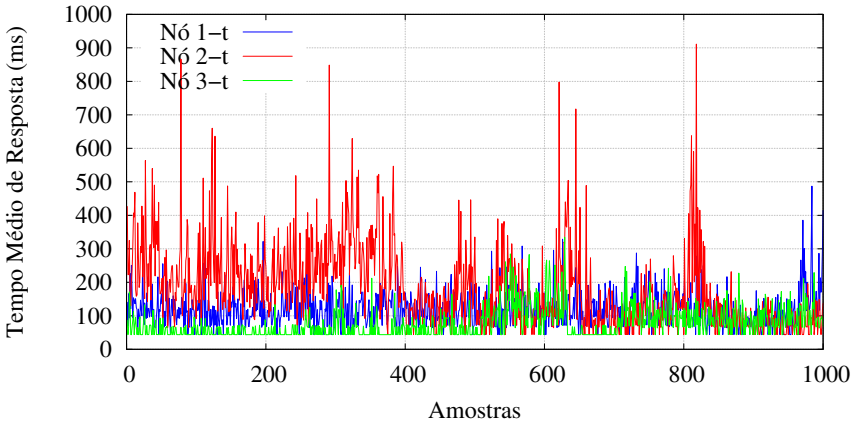
Em relação a caracterização do tráfego, a Figura 3 apresenta o comportamento do tráfego de dados dos três dispositivos IoT Memsic Irirs considerados em nossas análises. A Figura 3(a) mostra o tempo médio de resposta dos três dispositivos com sensores que monitoram a iluminação do ambiente. Enquanto, a Figura 3(b) apresenta o comportamento do tempo médio de resposta dos dispositivos com sensores de temperatura. Para cada dispositivo o tráfego de dados foi dividido em conjuntos de 1.000 amostras a fim de obter o tempo médio de resposta das requisições. Dessa forma, é possível observar um comportamento característico de cada dispositivo com seu respectivo sensor em relação ao seu tempo de resposta. Entretanto, vale observar que os dispositivos com sensores de temperatura possuem um tempo médio de resposta maior do que os de iluminação.

Mais especificamente, na Figura 3(a) o dispositivo *Nó 1* alcançou uma variação maior em seu tempo médio de resposta, atingindo valores em torno de 39 a 43ms. Em contrapartida, o dispositivo *Nó 2* apresentou uma leve queda no seu tempo médio de resposta em torno da amostra de número 200, diminuindo de 40ms para 37ms. Após essa queda, o dispositivo estabilizou com valores próximo a 37ms. Por fim, o dispositivo *Nó 3* apresentou um comportamento estável ao longo de todas as amostras de tráfego, onde seu tempo médio de resposta ficou em torno de 42 e 43ms. Desse modo, pode-se observar uma diferença clara no comportamento de cada dispositivo. Por outro lado, os dispositivos com sensores de temperatura da Figura 3(b) apresentaram um comportamento mais semelhante alcançando picos de valores de tempo médio de até 900ms para o *Nó 5*. Por se tratarem de dispositivos idênticos da mesma marca, modelo e com os mesmos protocolos e aplicações em execução, esperava-se um comportamento semelhante para ambos os sensores. Entretanto, através dos resultados observados é possível notar um comportamento específico para cada sensor. A justificativa para o sensor de temperatura alcançar valores maiores consiste do tipo de fenômeno monitorado, pois além das características dos dispositivos serem iguais, a geração e a coleta do tráfego seguiram os mesmos passos.

A Tabela 2 apresenta maiores detalhes sobre cada dispositivo com seu respectivo sensor. Como durante a geração e a coleta de tráfego de dados foi aplicado o mesmo tamanho de pacote de dados, bem como o mesmo número de requisições, a taxa de retransmissão e a média de pacotes por segundo apresentaram comportamentos similares para os três dispositivos com seus sensores. Contudo, a quantidade de requisições aumentou devido às taxas de retransmissões dos dispositivos, como por exemplo o *Nó 1-l* atingiu uma taxa de retransmissão de 7.84%. Assim, através dos resultados sobre o comportamento do tráfego de cada dispositivo observou-se que mesmo dispositivos IoT idênticos possuem um comportamento único que os diferencia no que tange o tempo médio de resposta. Tal comportamento pode ser analisado apenas considerando a característica sobre o tempo de resposta dos dispositivos. Todavia, essa informação não possui nenhuma proteção ou técnica de criptografia, o que facilita a execução de ataques *Traffic Side-Channel*. A maioria dos administradores de rede utilizam técnicas de gerenciamento de segurança que criptografam apenas o conteúdo do pacote e outras informações do cabeçalho do pacote, se abstendo de informação consideradas não tão relevantes como o tempo de reposta. Entretanto, por meio dos resultados apresentados é possível observar



(a) Dispositivos com Sensores de Iluminação



(b) Dispositivos com Sensores de Temperatura

Figura 3. Comportamento do Tempo de Resposta dos Dispositivos IoT

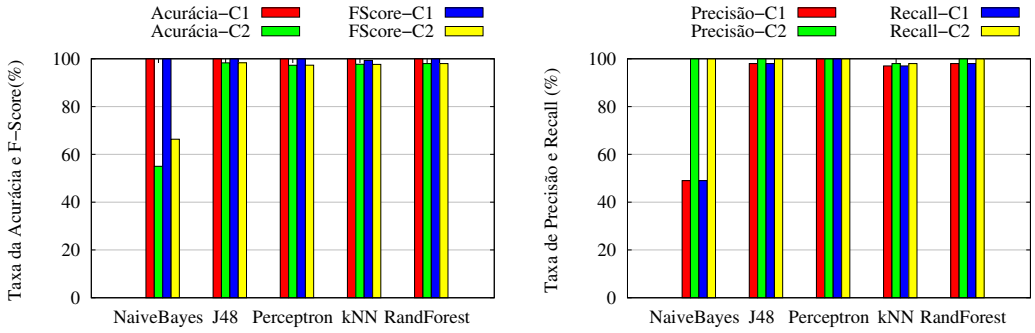
que o vazamento *side-channel* possui informações básicas que permitem caracterizar os dispositivos conectados na rede.

	Sensor de iluminação			**Sensor de temperatura**		
	Nó 1-l	*Nó 2-l*	*Nó 3-l*	*Nó 1-t*	*Nó 2-t*	*Nó 3-t*
Taxa de Retransmissão	7.84%	6.19%	3.18%	2.91%	4.98%	1.3%
Média de Pacotes/s	4.5	5.1	6.1	6.33	5.33	7.2
Tempo de Resposta Médio	41.36	38.74	46.11	119.47	182.87	77.21

Tabela 2. Detalhes dos Dispositivos IoT

Em relação a identificação do tráfego de dados de cada dispositivo IoT, os gráficos da Figura 4 apresentam os resultados referentes ao desempenho dos cinco classificadores para os sensores de iluminação. Tais resultados seguiram dois cenários de avaliação, **C1** e **C2** (detalhados na Seção 4). De acordo com o gráfico da Figura 4(a), a maioria dos classificadores alcançaram taxas de acurácia e *F-Score* próximo a 97%. Apenas o classificador *Naive Bayes* apresentou um resultado pobre para o cenário **C2**, pois neste cenário foi utilizado apenas os valores sobre a moda e a média do tempo de resposta. Porém, no cenário **C1** foram utilizadas todas as medidas estatísticas, melhorando assim o desempenho do *Naive Bayes* e dos demais classificadores. O que comprova que quanto maior o nível de detalhamento dos dados, melhor será o resultado de identificação. Um desempenho semelhante dos classificadores pode ser visto na Figura 4(b). Conforme as taxas de

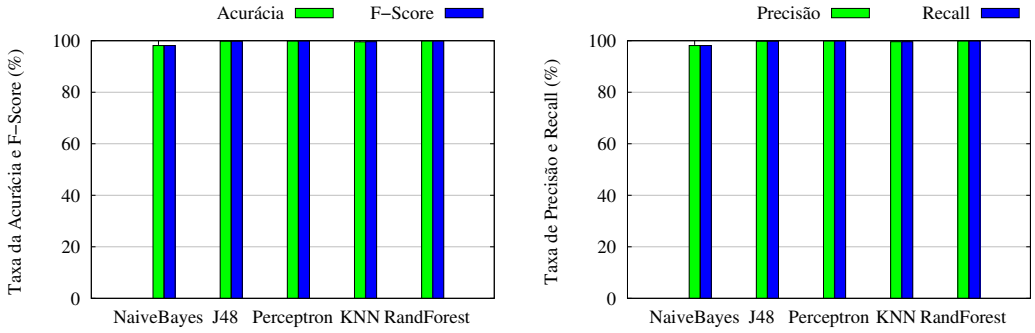
precisão e *recall*, a proporção de dispositivos classificados corretamente é extremamente alta. Dessa forma, com base no desempenho obtido por meio dos cinco classificadores comprova-se a possibilidade de identificar dispositivos IoT idênticos apenas utilizando informações relacionadas ao tempo de resposta e `timestamp` dos pacotes de dados.



(a) Acurácia e *F-Score* (b) Precisão e *Recall*

Figura 4. Desempenho dos Classificadores com Sensores de Iluminação

Para os dispositivos IoT com sensores de temperatura os resultados dos cinco classificadores também atingiram um desempenho altamente satisfatório, como pode ser observado nas Figura 5(a) e Figura 5(b). Devido aos resultados anteriores alcançarem valores ótimos para o cenário **C1**, que emprega todas as medidas estatísticas do tempo de resposta e `timestamp`, esta segunda análise considerou apenas este cenário. Nesta análise todos os classificadores alcançaram valores em torno de 90% e 99% de acurácia, *F-Score*, precisão e *recall*. Esses resultados observados reforçam as análises anteriores, o que comprova a identificação de dispositivos idênticos por meio de vazamento *side-channel*. No sentido de ataques *Traffic Side-Channel*, os atacantes podem identificar os dispositivos e assim, se passar por eles e roubar informações privadas dos usuários. Dessa forma, os resultados obtidos apontam a importância da informação tempo e a necessidade do desenvolvimento de técnicas de gerência e segurança que considerem tais informações.



(a) Acurácia e *F-Score* (b) Precisão e *Recall*

Figura 5. Desempenho dos Classificadores com Sensores de Temperatura

A Figura 6 apresenta os resultados de uma terceira análise, onde foi aplicado os dados dos três dispositivos tanto com sensores de temperatura, quanto com sensores de iluminação. Esta análise também seguiu apenas o cenário **C1**. Além disso, o tamanho do conjunto de dados de treino iniciou em 5% e aumentou gradativamente até 30%. O uso de diferentes tamanhos para o conjunto de dados de treino se embasou em um cenário que o administrador de rede precisará coletar o tráfego *online* e identificar os dispositivos o mais

rápido possível para atuar, por exemplo, contra algum ataque de rede. Assim, por meio dessa análise pode-se avaliar o desempenho dos classificadores com menor quantidade de dados de treino. Com base nos resultados, os cinco classificadores apresentaram resultados próximos a 100% de dispositivos classificados corretamente. Com isso, conclui-se a possibilidade de identificar os dispositivos mesmo com pouca quantidade de dados.

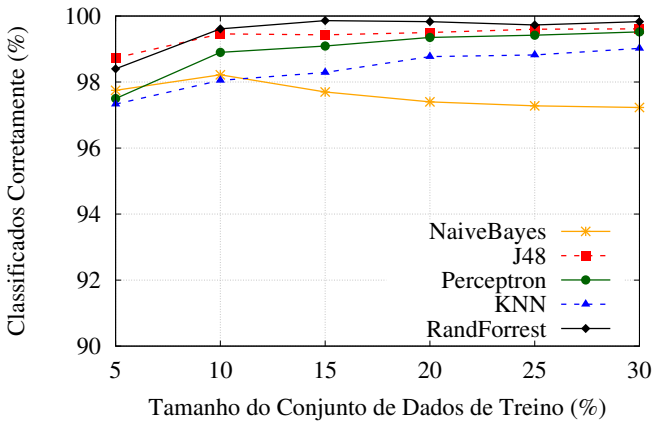


Figura 6. Taxa de Classificação considerando os Sensores de Iluminação e Temperatura

6. Conclusão

O presente artigo analisou o vazamento temporal *side-channel* no contexto de redes IoT a fim de auxiliar na melhoria das técnicas de gerência de monitoramento e segurança. Esta análise observou o comportamento de três dispositivos IoT Memsic Iris idênticos em questões de modelo, marca, protocolos e programas executados. Tal análise se embasou unicamente nas informações relacionadas ao `timestamp` e ao tempo de resposta dos dispositivos. Além disso, o tráfego de dados utilizado foi capturado por meio de um cenário de rede experimental, onde foram realizadas duas etapas de 100.000 requisições de dados por sensor. Através de profundas análises do comportamento do tráfego de dados de cada dispositivo, este trabalho confirmou a existência de características únicas e específicas mesmo de dispositivos idênticos. Além disso, este estudo mediu o desempenho de cinco classificadores na identificação do tráfego de cada dispositivo. Os resultados observados nessas análises apresentaram altas taxas de acurácia e precisão, comprovando assim uma grande eficiência em distinguir os dispositivos. Como direções futuras, pretende-se explorar outras características e com isso, desenvolver uma ferramenta de defesa que auxilie na ocultação dos vazamentos *side-channel*.

Referências

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., and Feamster, N. (2017). Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic. *arXiv:1708.05044*.

Chen, S., Wang, R., Wang, X., and Zhang, K. (2010). Side-channel leaks in web applications: A reality today, a challenge tomorrow. In *IEEE Symposium on Security and Privacy*, pages 191–206. IEEE.

Conti, M., Li, Q. Q., Maragno, A., and Spolaor, R. (2018). The dark side (-channel) of mobile devices: A survey on network traffic analysis. *IEEE Commun. Surveys & Tuts.*, 20(4):2658–2713.

Feghhi, S. and Leith, D. J. (2016). A web traffic analysis attack using only timing information. *IEEE Trans. Inf. Forensics Security*, 11(8):1747–1759.

Malik, N., Chandramouli, J., Suresh, P., Fairbanks, K., Watkins, L., and Robinson, W. H. (2017). Using network traffic to verify mobile device forensic artifacts. In *2017 14th IEEE Annual Consum. Commun. & Netw. Conference (CCNC)*, pages 114–119. IEEE.

Montenegro, G., Kushalnagar, N., Hui, J., and Culler, D. (2007a). Transmission of ipv6 packets over ieee 802.15. 4 networks. Technical report, IETF.

Montenegro, G., Schumacher, C., and Kushalnagar, N. (2007b). IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. Technical Report 4919, IETF.

Pacheco, F., Exposito, E., Gineste, M., Baudoin, C., and Aguilar, J. (2018). Towards the deployment of machine learning solutions in network traffic classification: A systematic survey. *IEEE Commun. Surveys & Tuts,*.

Prates, N., Pelloso, M., Macedo, R., and Nogueira, M. (2018). Ameaças de segurança, defesas e análise de dados em iot baseada em sdn. In *Minicursos SBSeg 2018*, chapter 1, pages 1–50. SBC.

Rescorla, E. and Modadugu, N. (2012). Datagram Transport Layer Security Version 1.2. Technical Report 6347, IETF.

Saltaformaggio, B., Choi, H., Johnson, K., Kwon, Y., Zhang, Q., Zhang, X., Xu, D., and Qian, J. (2016). Eavesdropping on fine-grained user activities within smartphone apps over encrypted network traffic. In *USENIX Workshop on Offensive Technologies)*.

Sayakkara, A., Le-Khac, N.-A., and Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*.

Selis, V. and Marshall, A. (2017). A fake timing attack against behavioural tests used in embedded iot m2m communications. In *Cyber Security in Netw. Conference*, pages 1–6. IEEE.

Shelby, Z., Hartke, K., and Bormann, C. (2014). The Constrained Application Protocol (CoAP). Technical Report 7252, IETF.

Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., and Sivaraman, V. (2018). Classifying iot devices in smart environments using network traffic characteristics. *IEEE Trans. on Mobile Comput.*

Srinivasan, V., Stankovic, J., and Whitehouse, K. (2008). Protecting your daily in-home activity information from a wireless snooping attack. In *Proceedings of the 10th international conference on Ubiquitous computing*, pages 202–211. ACM.

Taylor, V. F., Spolaor, R., Conti, M., and Martinovic, I. (2018). Robust smartphone app identification via encrypted network traffic analysis. *IEEE Trans. on Informat. Forensics Security*, 13(1):63–78.

Thubert, P., Bormann, C., Toutain, L., and Cragie, R. (2017). Ipv6 over low-power wireless personal area network (6lowpan) routing header. Technical report, IETF.

Vergütz, A., da Silva, R., Nacif, J. A. M., Vieira, A. B., and Nogueira, M. (2017). Mapping critical illness early signs to priority alert transmission on wireless networks. In *IEEE Latin-American Conference on Commun.*, pages 1–6. IEEE.

Veysset, F., Courtay, O., Heen, O., Team, I., et al. (2002). New tool and technique for remote operating system fingerprinting. *Intranode Software Technologies*, 4.

Yan, Y., Oswald, E., and Tryfonas, T. (2017). Exploring potential 6LoWPAN traffic side channels. *IACR Cryptology ePrint Archive*, 2017:316.