Avaliação de Conjuntos de Atributos para a Detecção de Ataques de Personificação na Internet das Coisas

Silvio E. Quincozes
Departamento de Computação
Universidade Federal Fluminense
Niterói, RJ, Brasil
sequincozes@id.uff.br

Juliano F. Kazienko
Colégio Técnico Industrial de Santa Maria
Universidade Federal de Santa Maria
Santa Maria, RS, Brasil
kazienko@redes.ufsm.br

Alessandro Copetti
Departamento de Computação
Universidade Federal Fluminense
Rio das Ostras, RJ, Brasil
alessandro_copetti@id.uff.br

***Resumo*—Os Sistemas de Detecção de Intrusão (IDS) utilizam o mecanismo de seleção de atributos durante o processo de classificação de ameaças ou eventos de intrusão. Uma seleção adequada permite que o IDS processe somente os atributos relevantes para a classificação. Atualmente, com bilhões de novos dispositivos e objetos ingressando na Internet das Coisas (IoT), o papel da seleção de atributos ganha maior relevância devido as restrições de recursos impostas nesse ambiente. Este trabalho investiga diferentes conjuntos de atributos propostos na literatura para detectar ataques de personificação, quando se falsifica entidades legítimas da rede. A avaliação de desempenho do IDS considera os requisitos impostos pela IoT, enfatizando o papel da seleção de atributos. Os resultados indicam uma variação de até 49,99% na acurácia para os diferentes conjuntos de atributos, mesmo com a escolha do melhor classificador para cada conjunto. Adicionalmente, uma oscilação de até 85,43% foi observada no tempo de processamento. A melhor acurácia obtida foi de 99,99%, com uma redução de até 65,04% do tempo necessário para processamento.**

I. Introdução

Nos últimos anos, com o surgimento do paradigma da Internet das Coisas (*Internet of Things* - IoT), além de dispositivos pessoais como *smartphones* e *notebooks*, milhões de objetos com limitações energéticas e de processamento estão ganhando conectividade com a internet. Para tanto, além das tecnologias de comunicação tradicionais, como o Wi-Fi, a comunicação pode ocorrer usando IPv6 em redes pessoais de baixa potência (6LoWPAN), ZigBee (802.15.4), *Bluetooth Low Energy* (BLE), etc.

Em alguns cenários, a confiabilidade da rede pode exigir o uso de mecanismos com a mínima sobrecarga possível [1]. Portanto, os mecanismos de segurança aplicados devem ser projetados para respeitar as capacidades computacionais dos dispositivos envolvidos. Contudo, o uso de mecanismos leves, muitas vezes, pode implicar na introdução de vulnerabilidades, as quais são exploradas para a prática de ataques, como o de personificação. Esse tipo de ataque consiste na falsificação de entidades legítimas da rede tais como usuários, estações bases ou até dispositivos de sensoriamento equipados com uma placa de rede. A sua prática, que visa a obtenção de acesso não autorizado a sistemas computacionais, possui propriedades semelhantes ao comportamento normal, incluindo os mesmos atributos. Portanto, de acordo com Aminanto et al. [2], a análise e detecção desse tipo de ataque é considerada desafiadora.

Segundo Napiah et al. [3], as ameaças na IoT podem ser originadas de nós maliciosos, infiltrados em redes específicas da IoT tais como 6LoWPAN, ou ainda, provindos de atacantes externos atavés da exploração de falhas de segurança na comunicação através do padrão IEEE 802.11 (Wi-Fi). Baseando-se nessa definição, tais abordagens são denominadas como ataques *inside* e *outside*, respectivamente. Os ataques praticados por atacantes externos a rede, usualmente, visam o acesso não autorizado aos sistemas e suas informações [4], enquanto os atacantes internos, usualmente, consistem em usuários legítimos que exploram meios de obter acesso aos recursos não autorizados para seu nível de acesso [5].

Nesse contexto, diversas técnicas vêm sendo investigadas a fim de identificar eventos de intrusões e de impedir que atacantes consigam afetar as suas vítimas [2][6][7][8]. A identificação de ameaças pode se dar através do uso de Sistemas Detectores de Intrusões (IDSs). Tais sistemas executam a análise de informações provindas de tráfego de rede ou de registros de sistemas e serviços por meio da aplicação de técnicas como o aprendizado de máquina a fim de detectar ações maliciosas ou anômalas [9][10].

Uma das etapas fundamentais de qualquer IDS consiste na definição de quais atributos que são analisados [8]. Esse processo é chamado de Seleção de Atributos, o qual tem por finalidade a redução do número de informações, de modo a processar somente aqueles atributos relevantes para a classificação [11]. A seleção de atributos define os dados de entrada para todo um processo de análise da detecção de intrusões. Desse modo, para que um IDS alcance bons resultados, é crucial a seleção adequada dos atributos mais relevantes para o problema. Ademais, além do aumento do desempenho dos algoritmos detectores, a seleção de atributos reduz o consumo dos recursos. Portanto, uma das principais vantagens do estudo dos benefícios de diferentes conjuntos de atributos consiste na desoneração do processo de análise por parte de detectores de intrusões, viabilizando-se assim a detecção de ameaças em

tempo hábil para a aplicação de contramedidas [12].

Assim, a seleção de atributos desempenha papel fundamental em cenários com restrição de recursos como a IoT, quando empregado um IDS. Os IDSs exploram os recursos computacionais e de memória para detecções precisas e rápidas. Contudo, ambos os recursos são limitados em dispositivos da IoT. Dessa forma, a detecção de intrusões ocorre, usualmente, por dispositivos centralizadores, os quais coletam e analisam os dados. Essas operações implicam em um consumo adicional de energia para processamento de amostras e também demandam o uso da rede para a coleta de informações. Na Tabela I, desenvolvemos uma relação para clarear as funcionalidades desejáveis de um IDS, face a limitação de recursos da IoT. Além de identificar desafios para os IDS na IoT, esses desafios apresentam oportunidades para a seleção de atributos impactar no desempenho dos IDS.

Tabela I
RELAÇÃO ENTRE REQUISITOS DA DETECÇÃO DE INTRUSÕES E RESTRIÇÕES DA INTERNET DAS COISAS (IOT)

Questões / **Recurso**	**Restrições da IoT**	**Requisitos de IDSs**
Uso de CPU	Processamento Limitado	*Feedback* Rápido
Memória Disponível	Altamente Reduzida	Aprendizado baseado em amostras
Disponibilidade de Energia	Eficiência Energética	Uso contínuo
Uso de Rede	Requer pouca sobrecarga	Sondagens para monitoramento

Uma vez que existem diferentes categorias de ataques, os atributos afetados pelas ações de atacantes nem sempre são os mesmos. Portanto, a relevância de um atributo deve ser medida de acordo com o nível de contribuição que o mesmo apresenta para a identificação de cada perfil de intrusão. Nesse contexto, ao passo que a seleção de atributos para ataques convencionais é amplamente discutida na literatura [12][13][14], a análise do impacto dos atributos capazes de identificar ataques atuais, tais como os que envolvem dispositivos da Internet das Coisas, ainda é pouco explorada pela comunidade acadêmica. Existem, contudo, algumas propostas que consideram a seleção de diferentes conjuntos de atributos para a detecção de intrusões por meio da análise de atributos coletados de redes Wi-Fi [2][6][7][8][15]. Não há, porém, uma consolidação na seleção dos atributos a serem analisados, de modo a explorar o máximo desempenho dos IDSs.

O objetivo deste trabalho consiste em revisar e avaliar os diferentes conjuntos de atributos utilizados na literatura aplicados à mitigação de ataques *outside* de personificação em redes sem fio, especialmente na IoT. Com isso, espera-se resolver o problema da escolha de atributos adequados para tal propósito, de modo a construir um conhecimento que exonere trabalhos futuros e IDSs de tal análise. Experimentos práticos foram executados a partir de um conjunto de dados (*dataset*) público e recente [16], o qual inclui amostras de intrusões coletadas a partir de redes padrão IEEE 802.11, pertinentes a cenários reais da atualidade.

O restante deste trabalho está organizado como segue. Na Seção II, os termos e definições relacionados à seleção de atributos e ataques de personificação são explorados. Na Seção III, os trabalhos relacionados são apresentados. Os materiais e métodos são apresentados na Seção IV. Na Seção V os atributos utilizados na literatura serão discutidos. A Seção VI descreve cenários de ataques de personificação, relata os experimentos realizados e os achados deste trabalho. Por fim, na Seção VII, as conclusões e trabalhos futuros são apresentados.

II. FUNDAMENTAÇÃO TEÓRICA

Nesta seção são discutidos os diferentes tipos de ataques de personificação. Posteriormente, é investigada a etapa de seleção de atributos no processo de classificação.

A. Ataques de Personificação

Existem diferentes formas para que atacantes consigam personificar entidades legítimas de uma rede. O ataque *Evil Twin* se baseia na clonagem de pontos de acessos (*access points* - AP) a fim de que a vítima se conecte ao AP malicioso ao invés do legítimo. Para tanto, é importante que o AP clonado ofereça um sinal superior ao AP legítimo. Desse modo, a vítima passa a se comunicar com o ponto de acesso malicioso, possibilitando ao atacante a interceptação e manipulação de toda a comunicação sem o conhecimento da vítima. Portanto, basicamente, o atacante age como um Homem-No-Meio, do inglês, *Man-In-The-Middle* (MITM) [17].

Ao executar o ataque *Cafe Latte*, o atacante não precisa estar no raio de alcance de pontos de acessos da rede alvo, pois diferentemente do *Evil Twin*, as vítimas desse ataque são clientes isolados de redes protegidas pelo protocolo *Wired Equivalent Privacy* (WEP). Isso acontece porque muitos dispositivos costumam armazenar as credenciais de acesso a fim de estabelecer conexão de forma automática quando o cliente estiver dentro do alcance do AP [18]. Assim, ao forjar requisições *Address Resolution Protocol* (ARP) para a vítima, é possível a quebra da chave WEP [19].

O ataque *Hirte* estende o *Cafe Latte* através da aplicação de técnicas de fragmentação. Assim, tanto a captura de pacotes IP quanto ARP pode permitir a quebra da chave criptográfica utilizada nas comunicações *wireless* que usam o protocolo WEP. O conceito de fragmentação é utilizado com o propósito da quebra da requisição em dois fragmentos antes do envio para a vítima, onde o comprimento do primeiro fragmento é manipulado de modo com que o IP de origem seja movido para uma posição específica durante a remontagem no cliente [20]. A execução desse tipo de ataque pode se dar através do uso de ferramentas tais como *Aircrack-ng*, a qual possui instruções públicas para tal prática[1].

O protocolo WEP, apesar de não ter como propósito específico a segurança em ambientes IoT, possui um funcionamento interessante devido a seu baixo custo de processamento

[1]https://www.aircrack-ng.org/doku.php?id=hirte

e ao número reduzido de mensagens. Conforme Tozlu et al. [21], o protocolo WEP apresenta uma sobrecarga computacional desprezível para a autenticação e a encriptação de dados, quando comparado às abordagens mais sofisticadas. Embora o protocolo tenha vulnerabilidades conhecidas, ele ainda é utilizado em 7% das redes, por mais de 32 milhões de usuários, segundo a plataforma WiGLE [22], que consolida informações de redes sem fio em todo o mundo. Assim, não podem ser desprezadas medidas de segurança para evitar invasões nesse protocolo, as quais possam atingir redes ou dispositivos IoT associados.

B. Seleção de Atributos

A detecção de intrusões consiste na análise de dados pertinentes à identificação de ameaças. Portanto, os IDSs, usualmente, são baseados em mecanismos organizados em um processo sequencial. Tipicamente, esse processo inicia a partir da extração de informações. Tal coleta pode se dar a partir da implantação de um *sniffer*, a fim de capturar pacotes transmitidos em uma determinada rede, ou ainda através da coleta de registros (*logs*) de aplicações.

Independentemente da fonte de informações observada, é comum que existam muitas informações irrelevantes dentre as que realmente possuem algum valor para a análise. Portanto, uma etapa fundamental na detecção de intrusões consiste na etapa de pré-processamento, onde ocorrem a extração e seleção de atributo. Tais operações têm como objetivo, respectivamente, a transformação de dados brutos em informações com algum valor agregado para a análise posterior e a seleção de quais desses atributos extraídos serão utilizadas pelo mecanismo detector, na etapa seguinte [16].

C. Técnicas de Seleção de Atributos

Alguns algoritmos de mineração de dados efetuam o descarte de atributos irrelevantes implicitamente, tal como é feito no algoritmo *REPTree*, por exemplo. Esse tipo de seleção é caracterizada como *embedded*, pois está embutida na implementação do método classificador. Existem, contudo, muitos outros algoritmos que não executam nenhuma técnica com a finalidade de eliminação de ruídos ou redundância nos atributos analisados. Nesses casos, técnicas de seleção de atributos pertencentes a categoria *Wrapper* ou *Filter* podem ser utilizadas. Enquanto os métodos *Wrapper* se baseiam na saída de algum algoritmo de aprendizado de máquina para iterativamente melhorar a qualidade dos atributos selecionados, os algoritmos *Filter*, que são independentes de tais algoritmos, determinam a importância de cada atributo unicamente com base em suas características [11].

Ademais, volumosos conjuntos de dados dificultam a execução de técnicas de seleção. Assim, mesmo para aqueles algoritmos que já contemplem a seleção de atributos em sua implementação, o ideal é que as informações de entrada sejam reduzidas sempre que possível através do conhecimento prévio da relevância de alguns dos atributos existentes. Existem múltiplas técnicas que podem ser aplicadas para a seleção de atributos[2], a seguir alguns dos métodos mencionados neste trabalho serão brevemente discutidos.

Uma das mais simples técnicas de seleção de atributos se baseia no Ganho de Informação (GI), obtido através do cálculo da entropia. A Equação 1 denota esse cálculo, onde p_i é a probabilidade de que uma instância no conjunto C pertença a uma determinada classe.

$$Ganho(C) = -\sum_{i=1}^{m} p_i log_2(p_i) \tag{1}$$

O GI é proporcional à redução da entropia, portanto, os atributos com menores entropia tendem a ser selecionados por apresentar um maior ganho de informação. Todavia, apesar de simples, essa abordagem pode ser inviável de ser aplicada a grandes conjuntos de dados.

O método Qui-quadrado, do inglês, *Chi Square Statistics* [23], tem por finalidade avaliar quantitativamente a associação entre atributos de duas categorias. A ideia básica desse método consiste no estabelecimento de duas hipóteses. A hipótese H_0, diz que não há associação entre o atributo analisado e a classe. Em contra partida, H_1 consiste em dizer que há associação, ou seja, o atributo possui dependência em relação à classe. A Equação 2 ilustra o teste do qui-quadrado, onde as frequências observadas F_O são calculadas a partir dos atributos das amostras e as F_E são calculadas a partir das F_O.

$$x_2 = \sum \frac{(F_O - F_E)^2}{F_E} \tag{2}$$

A abordagem de seleção de atributos baseada em correlação, do inglês, *Correlation-based Feature Selection* (CFS) consiste na construção de matrizes de correlação *Atributo x Atributo* e *Atributo x Classe*. A partir dessas matrizes, é calculado o peso de cada conjunto de atributos através da Equação 3, onde o mérito de um conjunto *S*, que contém k atributos é calculado com base na média da correlação entre atributo-classe r_{ac} e a média entre atributo-atributo r_{aa}. Com base nessa equação, é possível a obtenção da razão entre a capacidade de predição e o grau de redundância de cada conjunto.

$$Merito(S) = \frac{k \times \overline{r_{ac}}}{\sqrt{k + k(k-1)r_{aa}}} \tag{3}$$

Existem abordagens de seleção de atributos que consistem na implementação de mecanismos de aprendizado de máquina por meio de redes neurais artificiais, do inglês, *Artificial Natural Network* (ANN). Esse tipo de metodologia tem por finalidade a poda de agentes que transportam informações redundantes ou de pouca relevância para a classificação. Nesse contexto, diferentes algoritmos em particular podem ser implementados, tais como modelos cognitivos [8] ou algoritmos de aprendizado baseados em ponderação de atributo [2], onde os pesos dos atributos representam a sua importância.

[2]http://featureselection.asu.edu/algorithms.php

III. Trabalhos Relacionados

No trabalho [7], é proposta a combinação de métodos de seleção de atributos baseado em ponderação com algoritmos de aprendizado de máquina. Baseando-se no fato de que a IoT está repleta de dispositivos vulneráveis que geram grandes volumes de dados, a ideia dos autores é avaliada a partir de amostras de tráfego de rede Wi-Fi da base AWID [16], com a técnica de Redes Neurais. Nesse estudo, os autores demonstram que o método proposto apresenta resultados superiores quando comparado aos modelos de seleção de atributos baseados em filtros. No total, foram selecionados quatro conjuntos de atributos, cada um deles por um método diferente: CFS, Correlação (Coor), ANN e também por meio de um método de árvore de decisão (C4.5).

Em seu trabalho posterior [2], os autores apresentam esforços a fim efetuar a seleção de um conjunto de atributos ideal para a mitigação de ataques de personificação. Além dos métodos utilizados anteriormente, um novo conjunto baseado nos resultados alcançados pelo método de Máquina de Vetores de Suporte (SVM) é proposto.

No trabalho [8], os autores propuseram um modelo cognitivo baseado em fractal para redes neurais artificiais para extrair atributos importantes a partir de *datasets* contendo intrusões. Fractais são figuras geométricas não euclidianas que, quando criadas artificialmente comumente exibem padrões semelhantes em escalas menores. Com isso, os autores chegam à proposta de um novo conjunto de seis atributos.

Alotaibi [6] aborda técnicas voltadas à detecção de intrusões em dispositivos *wireless* em sua tese de doutorado. Com base no método de aprendizado de máquina chamado *Extra Tree*, os autores selecionam 20 atributos, os quais são ordenados por nível de importância. Tal seleção é referenciada também no trabalho [15], do mesmo autor, onde é alcançada uma acurácia de 96.32%. Para a avaliação, os autores propõem o uso de um conjunto de classificadores, baseando-se em votação majoritária entre os mesmos.

Em [24], os autores propõem um modelo multi-agente cognitivo a fim de aprender o comportamento anormal do tráfego da rede sem fio através da composição de uma ANN. Nessa rede, cada neurônio de entrada é considerado um agente. O mecanismo de aprendizado de máquina proposto ordena todos os agentes com pesos e reduz a complexidade computacional do IDS, podando todos os agentes que transportam informações redundantes ou de pouca relevância para a classificação. Desse modo, seis atributos são selecionados por meio dos seis agentes que foram classificados como significantes. Os autores relatam uma acurácia de 99.3% nos experimentos realizados.

Um outro conjunto de atributos é selecionado em [25], de modo a possibilitar a detecção de intrusões em redes *wireless* 802.11. Dado o conjunto de 154 atributos iniciais, baseadas no conjunto de dados AWID [16], os autores executam a redução de atributos com base nos seguintes critérios: primeiramente, atributos que representam valores descritivos são removidos. Assim, restando 111 atributos com valores numéricos. Posteriormente, a técnica de cálculo de ganho de informação foi aplicada. Com base nessa técnica, um novo subconjunto de 40 atributos foi selecionado. Esse subconjunto é reduzido novamente através da aplicação do método estatístico Qui-quadrado. Com isso, o resultado final é a seleção de 10 atributos, que refletem em uma redução significativa de tempo de processamento. Todavia, há uma perda de acurácia de até 3.8% por meio da seleção de atributos proposta, que foi avaliada por 5 diferentes algoritmos classificadores.

Em 2016, no trabalho [26], Aminanto e Kim propõem uma solução para mitigação de ataques de personificação. A seleção de atributos se dá por meio de uma ANN, a qual resulta em um conjunto composto por 35 diferentes atributos. A proposta é avaliada com base nas assinaturas desse tipo de ataque contidas na base de intrusões pública da AWID. Para tanto, o algoritmo de *deep learning* chamado *Stacked Auto Encoder* (SAE) foi utilizado. Dois anos depois, em 2018, Aminanto, juntamente com Choi e Tanuwidjaja, propõem uma nova abordagem de seleção de atributos [18], desta vez, baseando-se em ponderação. A proposta também visa a mitigação de ataques de personificação em redes Wi-Fi. Segundo os autores, a avaliação do conjunto de atributos proposto alcançou taxas de detecção superiores aos trabalhos existentes, onde 99.91% das intrusões experimentadas foram identificadas com sucesso através da análise de um conjunto de 8 atributos, que se apresenta em menor número em relação àquelas selecionadas em seu trabalho anterior. Portanto, menos informações foram capazes de gerar resultados mais precisos.

Com base na análise dos trabalhos anteriormente discutidos é possível constatar a clara falta de consolidação em termos de seleção de atributos, mesmo quando um tipo específico de ataque é analisado. Portanto, a principal limitação de tais trabalhos consiste na falta de consenso na definição de quais conjuntos de atributos devem ser analisados.

IV. Materiais e Métodos

Esta seção apresenta a metodologia empregada com a finalidade de analisar os conjuntos de atributos selecionados pelos autores dos trabalhos discutidos, na Seção III. Todos os experimentos foram conduzidos a partir de uma máquina com processador Intel Core i7-7500U, equipada com 16GB de memória RAM DDR4 e sistema operacional Windows 10. A seguir, os demais materiais e métodos serão apresentados.

A. Espaço Amostral

Os experimentos foram realizados a partir do *dataset* AWID [16], que contém um largo número de amostras coletadas a partir de redes Wi-Fi reais. Basicamente, existem duas versões dessa base de intrusões. Uma delas possui 210.900.113 registros e a outra, que consiste em uma versão reduzida e independente da anterior, possui outros 2.326.218 registros.

Ambas as versões são segmentadas em duas partes a fim de permitir o treinamento e teste de detectores, respectivamente. Tanto a versão completa quanto a reduzida contém amostras que abrangem 9 classes de ataques para treinamento e 17 para teste. Portanto, existem amostras presentes na etapa de teste que não fazem parte da etapa de treinamento. Dentre

tais classes, existem amostras que pertencem aos ataques de personificação dos seguintes tipos: *Cafe-Latte*, *Evil Twin* e *Hirte*. Contudo, as amostras do tipo *Hirte* estão contidas somente na segmentação destinada à teste.

Uma vez que o escopo deste trabalho limita-se à avaliação de atributos para a detecção dos ataques de personificação, as 20.079 amostras correspondente aos 3 tipos de ataques dessa categoria foram extraídas a partir da versão reduzida da AWID. A fim de manter-se a proporção 1:1, conforme sugerido por Aminato et al. [7], as amostras do tipo normal foram extraídas na mesma quantidade. A Tabela II discrimina a distribuição de ataques por classe.

Tabela II
DISTRIBUIÇÃO DE AMOSTRAS POR CLASSE (TREINAMENTO E TESTE)

Tipo	Amostras de Treinamento	Amostras de Teste
Evil Twin	2.633	611
Cafe Latte	45.889	379
Hirte	0	19.089
Normal	48.522	20.079

B. Pré-Processamento

Dentre os atributos pertencentes ao espaço amostral analisado, existe uma grande diferença entre escalas e tipos de dados. Com isso, os resultados poderiam sofrer interferências de atributos de maior escala, por exemplo, sendo assim necessário o pré-processamento de algumas informações a fim de torna-las prontas para a classificação de amostras. Seguindo o modelo experimental apresentado em [18], todos os atributos foram transformados em números inteiros, dentro de um intervalo de 1 a 100. Para este fim, primeiramente, aqueles atributos que contém caracteres alfanuméricos foram enumeradas. Uma vez que todos os atributos estão em formato numérico, os mesmos são submetidos a um processo de normalização. Tal processo se dá de acordo com a Equação 4:

$$N_i = \frac{x_i - min(x)}{max(x) - min(x)} \quad (4)$$

Onde, N_i representa o valor normalizado do atributo x_i e os valores de $min(x)$ e $max(x)$ correspondem aos valores mínimo e máximo daquele atributo em todo o conjunto de dados analisado. Com isso, um arquivo com valores separados por vírgula (CSV) foi gerado, contendo 66 atributos normalizados (dentro de intervalos de 0 a 100). Além disso, cada amostra contém sua respectiva classe, na posição 67, para fins de treinamento supervisionado.

V. AVALIAÇÃO E DISCUSSÕES

Os conjuntos apresentados na Tabela III contêm os índices dos atributos da base de dados AWID, os quais foram selecionados pelos trabalhos relacionados. Os 15 conjuntos analisados somam 188 atributos que se repetem, onde 67 deles são únicos. Portanto, a partir dos 154 atributos contidos nesse conjunto, 88 deles são descartados. A partir dessa análise, a Tabela IV lista os 15 atributos mais selecionadas nesta revisão da literatura. Além desses, outros 52 atributos estão contidos em pelo menos um dos conjuntos propostos pela comunidade acadêmica com o propósito de detecção de intrusões em redes Wi-Fi. Apesar da maioria dos trabalhos analisarem diferentes classes de ataques, incluindo a personificação, existem também trabalhos que focam apenas nessa classe [2] [18] [26].

Tabela III
CONJUNTO DE ATRIBUTOS SELECIONADOS NA LITERATURA

Ref.	Conjunto	Atributos Selecionados
[7]	C_1	4, 8, 47, 68, 71
[7]	C_2	8, 9, 47, 50, 51, 67, 71, 75, 145, 154
[7]	C_3	4, 7, 14, 31, 38, 64, 66, 67, 68, 70, 73, 75, 79, 82, 83, 90, 93, 94, 107, 112, 118, 120, 131, 134, 136, 140
[7]	C_4	1, 2, 3, 4, 8, 38, 61, 67, 70, 75, 76, 77, 78, 79, 80, 82, 107, 108, 109, 110, 111, 112, 119
[8]	C_5	4, 8, 77, 79, 82, 154
[2]	C_6	5, 38, 70, 71, 154
[2]	C_7	47, 50, 51, 67, 68, 71, 73, 82
[2]	C_8	4, 7, 38, 77, 82, 94, 107, 118
[2]	C_9	47, 64, 82, 94, 107, 108, 122, 154
[2]	C_{10}	11, 38, 61, 66, 68, 71, 76, 77, 107, 119, 140
[6] e [15]	C_{11}	8, 47, 50, 61, 66, 67, 68, 71, 73, 75, 76, 77, 78, 79, 80, 82, 110, 140, 141, 142
[24]	C_{12}	4, 8, 77, 79, 82, 154
[25]	C_{13}	4, 5, 6, 7, 8, 9, 38 ,75, 81, 82
[18]	C_{14}	47, 64, 82, 94, 107, 108, 122, 154
[26]	C_{15}	4, 7, 8, 29, 38, 47, 62, 66, 67, 68, 70, 72, 73, 77, 79, 80, 82, 88, 93, 94, 98, 104, 107, 108, 112, 113, 122, 125, 126, 127, 140, 141, 142, 144, 148

Tabela IV
OS 15 ATRIBUTOS MAIS USADOS DENTRE OS CONJUNTOS ANALISADOS.

Índice	Nomenclatura	Seleções	%
82	wlan.seq	11	68,75
107	wlan_mgt.fixed.timestamp	8	50
8	frame.len	8	50
38	radiotap.mactime	7	43,75
4	frame.time_epoch	7	43,75
77	wlan.da	7	43,75
79	wlan.sa	6	37,5
154	data.len	6	37,5
47	radiotap.datarate	6	37,5
68	wlan.fc.ds	6	37,5
71	wlan.fc.pwrmgt	5	31,25
75	wlan.duration	5	31,25
67	wlan.fc.subtype	5	31,25
94	wlan_mgt.fixed.capabilities.preamble	5	31,25
108	wlan_mgt.fixed.beacon	5	31,25

O atributo mais escolhido pelos autores dos trabalhos analisados consiste no número de sequência (*wlan.seq*), que acompanha todos quadros transmitidos na comunicação 802.11, exceto os quadros de controle. Usualmente, o número de sequência é incrementado de 0 a 4.095 a cada quadro consecutivo. A verificação de adulterações neste parâmetro é capaz de identificar ações oriundas de atacantes [6]. Por esse motivo, essa informação faz parte de 11 dos 16 conjuntos de atributos selecionados pelos trabalhos analisados.

Em segundo lugar, os atributos mais selecionados costumam ser aqueles que se referem ao carimbo de tempo (*wlan_mgt.fixed.timestamp*) e o comprimento dos quadros transmitidos (*frame.len*). A relevância desses atributos se dá pela capacidade de representar a disposição temporal e o tamanho de pacotes que trafegam nas redes Wi-Fi [6].

VI. Experimentação

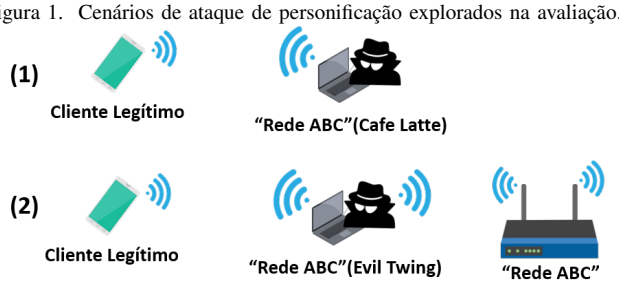
A fim de avaliar o desempenho em termos de precisão e de tempo total de processamento, esta Seção apresenta uma experimentação prática. Tal experimentação é realizada a partir da classificação de amostras extraídas do conjunto de dados AWID, o qual é composto por amostras com 155 diferentes atributos. Desses atributos, 83 não utilizados por nenhum trabalho analisado, portanto, foram excluídos da experimentação.

Os seguintes algoritmos classificadores foram utilizados na avaliação: *K-Nearest Neighbours* (KNN), textitREPTree, *Random Tree*, *Naive Bayes*, *JRip*, *KStar* e *Locally Weighted Learning* (LWL). Esses algoritmos foram escolhidos considerando os requisitos de acurácia, tempo de treinamento, tempo de classificação e clareza da solução final [9].

A. Cenários de Ataque de Personificação

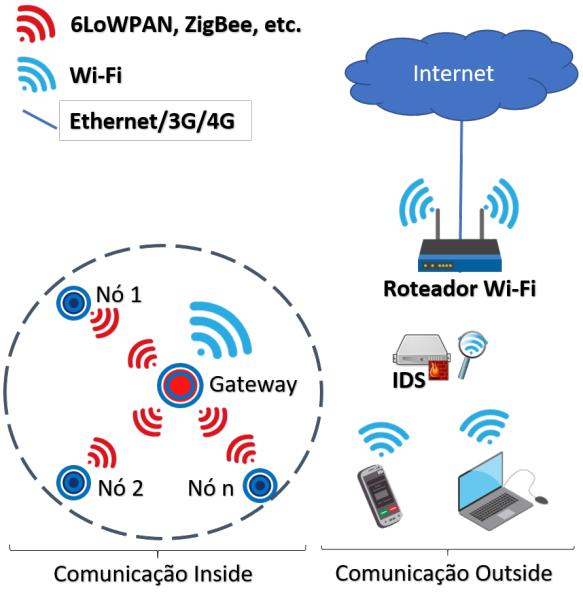
Conforme discutido na Seção II-A, existem diferentes categorias de ataques com a finalidade de personificar dispositivos em redes Wi-Fi. Nesta seção, alguns cenários de ataques serão apresentados. No cenário 1, assume-se que o atacante está dentro da área de cobertura da vítima mas não necessariamente na área de cobertura de um AP legítimo. O cenário 2, por sua vez, parte da premissa que o atacante está dentro da área de cobertura tanto da vítima quanto do AP legítimo a qual a vítima tenta se conectar. A Figura 1 ilustra tais cenários.

Figura 1. Cenários de ataque de personificação explorados na avaliação.



Cenário 1: suponha que um atacante que tem como recurso tecnológico um *laptop* com a distribuição *Kali Linux*, do sistema operacional *Linux*, instalada. Tal indivíduo mal intencionado deseja atacar uma rede legítima que é protegida pela criptografia WEP. O objetivo desse atacante consiste na obtenção indevida da chave criptográfica utilizada. Portanto, o atacante pode configurar o ambiente através da utilização das ferramentas *Airodump-ng* e *Airbase-ng*, as quais permitirão a captura de pacotes transmitidos no meio sem fio e a criação de uma rede falsa, respectivamente. Em seguida, quando a vítima se conecta à rede falsa, a ferramenta *Airodump-ng* será capaz de obter os dados necessários para a decodificação da chave WEP, que ocorre por meio de uma terceira ferramenta chamada *Aircrack-ng*. Todas as ferramentas utilizadas para esse ataque estão pré-instaladas na distribuição *Kali Linux*. Por fim, a consequência desse ataque implica na quebra da confidencialidade da informação transmitida no meio sem fio pela vítima. Em outras palavras, o atacante passa a ser capaz de espionar toda informação transmitida pela vítima.

Figura 2. Escopo explorado na avaliação.



Cenário 2: suponha que neste cenário o atacante tem posse de um um notebook com as mesmas ferramentas disponíveis no cenário (1). Adicionalmente, assume-se que esse atacante está dentro da área de cobertura do ponto de acesso legítimo e através da criação de uma nova rede, passa a emitir um sinal mais forte do que o AP legítimo o que influencia a vítima a optar por conectar-se na rede criada pelo atacante. Tal rede maliciosa deve possuir o mesmo identificador de conjunto de serviços, do inglês, *Service Set Identifier* (SSID) que o AP legítimo. Uma vez que o cliente conecta-se à rede falsa, o atacante é capaz de interceptar toda a informação antes de efetuar a retransmissão para o AP legítimo. Assim, informações sigilosas tais como senhas e dados bancários serão expostas ao atacante sem o conhecimento da vítima.

No contexto da Internet das Coisas, existem *gateways* que suportam tanto a comunicação por meio de tecnologias específicas para a IoT (e.g. 6LoWPAN), quanto a comunicação Wi-Fi tradicional. Tais *gateways* são responsáveis pela comunicação *Inside*, que ocorre entre dispositivos da IoT (e.g. sensores e atuadores), com os dispositivos *outside*, que se situam fora da rede de sensores (e.g. pontos de acessos Wi-Fi). Segundo Zarpelão [4], um IDS pode ser implantado em cada um dos dispositivos ou em uma entidade centralizadora, como o *gateway*. A vantagem de se implantar o IDS na comunicação *outside* é a detecção de ataques provindos da Internet contra os objetos no domínio físico. Além disso, a implantação de IDSs nos próprios nós da rede IoT pode ser um problema devido

a sobrecarga de processamento, armazenamento e energia. Portanto, o objeto de estudo deste trabalho concentra-se na comunicação *outside*, conforme ilustrado na Figura 2.

B. Métricas de Avaliação

Existem múltiplas maneiras de avaliar a precisão de uma classificação de dados. Uma delas consiste no computo da taxa de detecção, que se dá através da Equação 5, onde o número de ataques detectados é dividido pelo total de ataques.

$$Tx.Deteccao = \frac{VP}{VP + FN} \tag{5}$$

Entretanto, tal métrica não considera o número de Falsos Positivos (FP), limitando a avaliação. Por outro lado, o cálculo da acurácia leva em consideração a quantidade total de classificações corretas, tanto para Verdadeiros Positivos (VP) quanto Verdadeiros Negativos (VN). Então, a soma desses valor é dividida pelo número total de amostras. Nessa equação, Falsos Negativos (FN) afetam negativamente a acurácia obtida na classificação. Portanto, a acurácia é considerada como a principal métrica de avaliação neste trabalho. A Equação 6 denota esse cálculo:

$$Acuracia = \frac{VP + VN}{VP + FP + VN + FN} \tag{6}$$

Segundo Buczak [9], o tempo necessário para a classificação de novas amostras é um fator importante, pois deve viabilizar a reação contra possíveis ameaças. Portanto, outra métrica adotada é a quantidade de amostras processadas por segundo.

C. Resultados e Discussão

Os resultados dos experimentos são resumidos nos gráficos exibidos nas Figuras 3 e 4. Tais gráficos dizem respeito, respectivamente: a acurácia máxima (alcançada pelo melhor classificador) para cada um dos conjuntos de atributos, a acurácia média para cada conjunto e a quantidade média de amostras processadas por segundo. As duas últimas métricas são baseadas na média aritmética simples dos resultados de acurácia e tempo obtidos pelos 7 algoritmos classificadores.

A partir da análise dos conjuntos de atributos utilizados na literatura para a detecção de intrusões, é possível constatar que somente a escolha do melhor algoritmo de aprendizado de máquina não é suficiente para que bons resultados sejam alcançados. Os resultados demonstram que o impacto dos conjuntos de atributos selecionados é bastante significativo em termos de tempo e acurácia. A Figura 4 ilustra a quantidade de amostras processadas por segundo para cada um dos conjuntos, onde os conjuntos C_1 e C_{12}, os quais contêm 5 e 6 atributos, respectivamente, demonstraram a maior capacidade de processamento de amostras por segundo: 103 e 92, respectivamente. Por outro lado, os conjuntos C_{13} e C_{10} computaram, em média, 15 amostras por segundo. Com base nessa informação, é possível constatar que conjuntos com números reduzidos de atributos foram processados em pelo menos 15,45% do tempo utilizado para o processamento de conjuntos maiores.

O conjunto C_2, gerado a partir do método de correlação de atributos (*Coor*), apresentou o potencial mais promissor para a detecção de ataques de personificação. Além desse conjunto apresentar superioridade em relação as médias das acurácias obtidas pelos 7 classificadores experimentados (92,66%), dois desses classificadores atingiram a mais alta acurácia geral (99.99%) através dos classificadores *REPTree* (árvore de decisão) e *JRip* (regras de associação). Por outro lado, identificaram-se também conjuntos tais como C_{10} e C_{13} que apresentam atributos incapazes de permitir a detecção desse tipo de ataque em redes *Wi-Fi*. O conjunto C_{10} foi gerado a

Figura 3. Acurácia média ($\overline{x}$) e máxima obtida para cada conjunto de atributos.

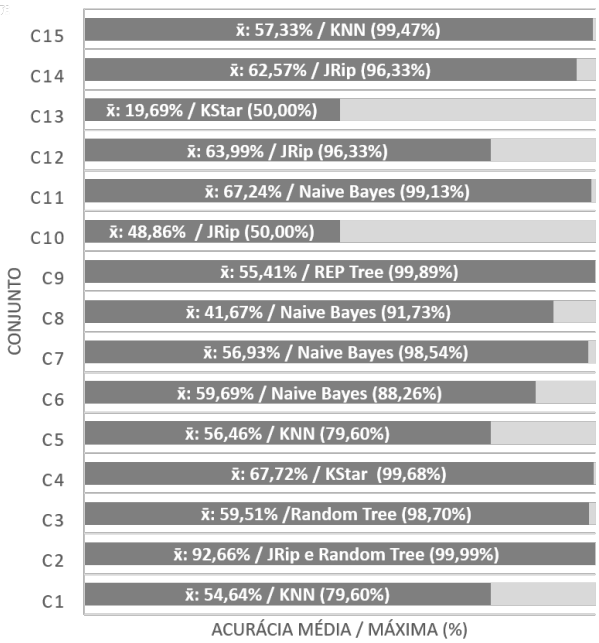
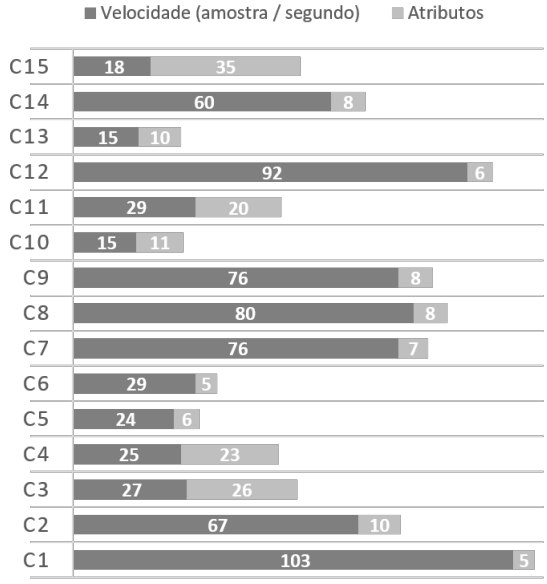


Figura 4. Relação entre a quantidade de amostras analisadas por segundo e o número de atributos selecionados para cada conjunto.



partir do uso de SVM, enquanto C_{13} foi gerado a partir da combinação dos métodos GI com Qui-Quadrado, após uma exclusão manual de atributos. Acredita-se que o não uso de técnicas de aprendizado de máquina na filtragem de atributos possa justificar os baixos resultados alcançados.

Finalmente, foi avaliado o impacto da redução de atributos, por meio da filtragem, na escalabilidade de detectores. Para tanto, foram medidos os tempos gastos exclusivamente para treinamento do menor conjunto (C2) e do maior (C15), em um cenário contendo um milhão de amostras de treinamento. Os resultados demonstram que o tempo gasto para treinamento do conjunto C2 (1417ms), com 8 atributos, consiste em apenas 33,08% do tempo necessário para treinar o conjunto C15 (4284ms), que possui 35 atributos. Cabe ressaltar que sistemas inteligentes, que possuem a capacidade de aprendizado em tempo de execução, o modelo de treinamento deve ser atualizado sempre que houverem novas assinaturas.

VII. Conclusões e Trabalhos Futuros

Este trabalho analisou 15 conjuntos de atributos utilizados pela comunidade acadêmica por meio de 7 diferentes algoritmos classificadores. Tal análise se deu a partir de um conjunto de dados pertinente a cenários reais. Com isso, constatou-se que os conjuntos de atributos analisados apresentaram uma variação de 19,69% à 92,66% na acurácia média para a detecção de ataques de personificação. A partir dos resultados obtidos com o melhor algoritmo de classificação para cada conjunto, há um impacto de até 49,99% na classificação, ocasionado pela seleção de atributos. As análises revelam que o conjunto C_2, que contém os 10 atributos denotados na Tabela III, apresenta maior potencial para a representação dos ataques de personificação: *Hirte*, *Evil Twin* e *Cafe Latte*. Portanto, este trabalho conduz projetistas de IDSs à escolha de atributos que ofereçam rapidez e alta precisão nas análises.

Como trabalhos futuros pretende-se expandir a análise a fim de definir as melhores técnicas de seleção de atributos para a detecção de outros tipos de ataques praticados na IoT, tais como, negação de serviço, sondagem, injeção, escalada de privilégios, força bruta, etc. Em outra iniciativa, abordar as possibilidades de ataques que tem como alvo a comunicação *inside*, a qual ocorre por meio de tecnologias específicas da IoT como 6LoWPAN e ZigBee.

Referências

[1] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of MQTT communication protocol in IoT system," in *Electrical Engineering, Computer Science and Informatics (EECSI), 2017 4th International Conference on*. IEEE, 2017, pp. 1–6.

[2] M. E. Aminanto, H. Tanuwidjaja, P. Yoo, and K. Kim, "Weighted feature selection techniques for detecting impersonation attack in Wi-Fi networks," in *Proc. Symp. Cryptogr. Inf. Secur.(SCIS)*, 2017, pp. 1–8.

[3] M. N. Napiah, M. Y. I. Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol," *IEEE Access*, 2018.

[4] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[5] P. Nespoli, D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Communications Surveys & Tutorials*, 2017.

[6] B. Alotaibi, "Empirical techniques to detect rogue wireless devices," Ph.D. dissertation, University of Bridgeport, 2016.

[7] M. E. Aminanto, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Wi-Fi intrusion detection using weighted-feature selection for neural networks classifier," in *Big Data and Information Security (IWBIS), International Workshop on*. IEEE, 2017, pp. 99–104.

[8] D. Kaleem and K. Ferens, "A cognitive approach for attribute selection in internet dataset," in *Cognitive Informatics & Cognitive Computing (ICCI* CC), IEEE 16th International Conference on*. IEEE, 2017, pp. 319–328.

[9] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[10] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to snort system," *Future Generation Computer Systems*, vol. 80, pp. 157–170, 2018.

[11] J. Li, K. Cheng, S. Wang, F. Morstatter, R. P. Trevino, J. Tang, and H. Liu, "Feature selection: A data perspective," *ACM Computing Surveys (CSUR)*, vol. 50, no. 6, p. 94, 2017.

[12] S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, and A. Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 271, 2013.

[13] N. Hoque, D. Bhattacharyya, and J. K. Kalita, "MIFS-ND: a mutual information-based feature selection method," *Expert Systems with Applications*, vol. 41, no. 14, pp. 6371–6385, 2014.

[14] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE transactions on computers*, vol. 65, no. 10, pp. 2986–2998, 2016.

[15] B. Alotaibi and K. Elleithy, "A majority voting technique for wireless intrusion detection systems," in *Systems, Applications and Technology Conference (LISAT), IEEE Long Island*. IEEE, 2016, pp. 1–6.

[16] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2016.

[17] D. A. Dai Zovi and S. A. Macaulay, "Attacking automatic wireless network selection," in *Proceedings from the Sixth Annual IEEE SMC. Information Assurance Workshop. IAW'05.* IEEE, 2005, pp. 365–372.

[18] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, 2018.

[19] M. S. Ahmad and V. Ramachandran, "Cafe latte with a free topping of cracked wep retrieving wep keys from road warriors," in *Proc. Conf. ToorCon*, 2007.

[20] C. Buchanan and V. Ramachandran, *Kali Linux Wireless Penetration Testing Beginner's Guide: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack*. Packt Publishing, 2017. [Online]. Available: https://books.google.com.br/books?id=jsxPDwAAQBAJ

[21] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: A practical approach," *IEEE Communications Magazine*, vol. 50, no. 6, 2012.

[22] Wireless network mapping. Acessed 25th July 2018. [Online]. Available: http://wigle.net

[23] H. O. Lancaster and E. Seneta, *Chi-square distribution*. Wiley Online Library, 1969.

[24] D. Kaleem and K. Ferens, "A cognitive multi-agent model to detect malicious threats."

[25] U. S. K. P. M. Thanthrige, J. Samarabandu, and X. Wang, "Machine learning techniques for intrusion detection on public dataset," in *Electrical and Computer Engineering (CCECE), IEEE Canadian Conference on*. IEEE, 2016, pp. 1–4.

[26] M. E. Aminanto and K. Kim, "Detecting impersonation attack in WiFi networks using deep learning approach," in *International Workshop on Information Security Applications*. Springer, 2016, pp. 136–147.