ELSEVIER

CrossMark

Disponível online em www.sciencedirect.com

ScienceDirect

Procedia Computer Science 167 (2020) 636-645

Procedia Computer Science

www.elsevier.com/locate/procedia

Conferência Internacional sobre Inteligência Computacional e Ciência de Dados (ICCIDS 2019)

Uma revisão do avanço dos conjuntos de dados de detecção de intrusão

Ankit Thakkar, Ritika Lohiya*

aDepartamento de Informática e Engenharia, Instituto de Tecnologia, Universidade Nirma, Ahmedabad - 382 481, Gujarat, Índia.

Abstrato

A pesquisa no campo da Cyber Security levantou a necessidade de abordar a questão dos cibercrimes que causaram a requisição das propriedades intelectuais, tais como quebra de sistemas de computador, comprometimento de dados importantes, comprometendo a confidencialidade, autenticidade e integridade do usuário. Considerando estes cenários, é essencial proteger os sistemas informáticos e o usuário usando um Sistema de Detecção de Intrusão (IDS). O desempenho do IDS estudado através do desenvolvimento de um conjunto de dados IDS, que consiste
de recursos de tráfego de rede para aprender os padrões de ataque. A detecção de intrusão é um problema de classificação, onde várias técnicas de Machine Learning (ML) e Data Mining (DM) são aplicadas para classificar os dados da rede em tráfego normal e de ataque. Além disso, os tipos de ataques de rede mudaram ao longo dos anos e, portanto, existe a necessidade de atualizar os conjuntos de dados usados para avaliar o IDS. Este documento lista os diferentes conjuntos de dados IDS usados para a avaliação do modelo IDS. O documento apresenta uma visão geral das técnicas ML e DM usadas para IDS, juntamente com a discussão sobre CIC-IDS-2017 e CSE-CIC-IDS-2018. Estes são conjuntos de dados recentes que consistem em
de características de ataque de rede e incluir novas categorias de ataques. Este documento discute os recentes avanços nos conjuntos de dados IDS que podem ser usados por várias comunidades de pesquisa como o manifesto para usar os novos conjuntos de dados IDS para o desenvolvimento eficiente e eficaz do ML e DM baseado no IDS.

Palavras-chave: Sistema de detecção de intrusão; Conjunto de dados de detecção de intrusão; Classificação de ataques; Avaliação de desempenho; Técnicas de aprendizagem de máquinas; Conjunto de dados CIC-IDS-2017; Conjunto de dados CSE-CIC-IDS-2018

1. Introdução

De acordo com as estatísticas reportadas pela Cyber Security, espera-se que os danos causados pelos ataques cibernéticos atinjam até três trilhões até 2021 com a probabilidade de executar explorações de um dia por dia [1]. Além disso, a quantidade de informações armazenadas em nuvens públicas e privadas operadas por empresas de dados como a Amazon Web Services, Facebook e Twitter, será aumentada cem vezes até 2022 [2]. Assim, um aumento na demanda de dados para sistemas de segurança mais proficientes. Os sistemas de computador com brechas, mecanismos de segurança com políticas de segurança incompetentes e falta de conhecimento sobre os ataques e crimes aumentaram os alvos para a colocação de ataques na rede. Ataques à rede, tais como resgate, roubo de identidade, roubo de dados, negação de serviço e

* Autor correspondente.

Endereço de e-mail: ankit.thakkar@nirmauni.ac.in (Ankit Thakkar), 18ftphde30@nirmauni.ac.in (Ritika Lohiya).

Revisão por pares sob responsabilidade do comitê científico da Conferência Internacional sobre Inteligência Computacional e Ciência de Dados (ICCIDS 2019).
10.1016/j.procs.2020.03.330

Tabela 1. Comparação de diferentes sistemas de detecção de intrusão [4]

Assinatura baseada em	Baseado em anomalias
Eficaz na identificação de ataques conhecidos através da realização de análises contextuais	Detecta ataques desconhecidos e vulnerabilidades juntamente com ataques conhecidos.
Depende do software do sistema e do sistema operacional para identificar os ataques e vulnerabilidades.	Ela é menos dependente do sistema operacional, e mais do exame - ines os padrões de rede para identificar ataques.
O banco de dados de assinaturas de ataque deve ser atualizado.	Ele constrói perfis da comunicação em rede observada para identificar os padrões de ataque.
O IDS baseado em assinatura tem um conhecimento mínimo de protocolos.	O IDS baseado na anomalia realiza a análise do protocolo para estudar os detalhes do pacote.

Os ataques de dia zero são difíceis de rastrear usando os mecanismos de segurança padrão como firewall e software anti-vírus [3]. Portanto, um Sistema de Detecção de Intrusão (IDS) usado para examinar as informações que fluem pela rede e para gerar um alarme para as prováveis atividades maliciosas geradas pelos intrusos. Um IDS detecta as intrusões

seja extraindo as assinaturas dos pacotes da rede ou analisando os padrões de ataque. Um IDS que detecta a intrusão através do estudo das assinaturas é denominado IDS baseado em Assinaturas. O IDS baseado em assinatura gera um alerta para os padrões de assinatura correspondentes armazenados no banco de dados de assinaturas. Em contraste, um IDS que detecta ataques com base no

Os padrões de ataque são chamados de IDS baseados na Anomalia. Uma tabela comparativa dos diferentes IDS é apresentada na Tabela 1. Independentemente do tipo de IDS, a arquitetura básica do IDS consiste em quatro etapas, como mostrado na Figura 1. Os pacotes de rede são capturados usando sensores de rede ou ferramentas de farejamento de rede. Os dados capturados são então filtrados e examinados.

A filtragem é realizada com base nas regras de filtragem, e depois os padrões de assinatura são combinados com os já disponíveis

banco de dados de assinaturas. Um alerta é gerado pelo IDS quando uma correspondência é encontrada com o banco de dados de assinaturas armazenadas.

A avaliação de um modelo IDS pode ser realizada pela implementação de técnicas de Machine Learning (ML) e Data Mining (DM) para classificar o tráfego de rede em fluxo de tráfego benigno e malicioso. As técnicas ML e DM implementadas nos conjuntos de dados IDS contêm dados etiquetados e características de tráfego de rede. Elas ajudam o classificador a aprender diferentes padrões de ataque para detectar um determinado ataque. As características do conjunto de dados ajudam o classificador a aprender os padrões normais de tráfego, bem como os padrões de ataque através dos quais o classificador é capaz de classificar os dados de entrada [5]. O conjunto de dados utilizado para o treinamento do classificador é construído monitorando o tráfego da rede por um determinado intervalo de tempo. O conjunto de dados consiste no tráfego normal da rede e no tráfego anômalo da rede que ajuda o classificador a identificar os padrões dos dados com uma quantidade suficiente de exemplos. Os dados coletados são divididos em um conjunto de treinamento e um conjunto de testes para treinamento e teste do classificador, respectivamente. Assim, várias técnicas de ML e DM utilizadas para o desenvolvimento de um IDS [6].

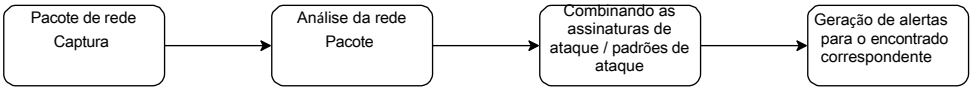

Fig. 1. Arquitetura do IDS

Os conjuntos de dados IDS consistem de etiquetas derivadas da observação dos padrões dos dados de tráfego da rede e, portanto, estes conjuntos de dados não funcionam bem com explorações de dia-zero [7]. Junto com o conjunto de dados, aplicando uma técnica apropriada

para a classificação dos ataques também é importante. Há uma infinidade de técnicas variadas que têm sido utilizadas com sucesso no IDS [8], [9], [10]. Entretanto, cada um dos algoritmos usados para o IDS treina e testa o conjunto de dados de uma maneira diferente. Os algoritmos usados para o IDS implementados no DARPA [11], KDD CUP 99 [12], ou conjunto de dados NSL-KDD [13] tendo as instâncias da rede agrupadas como conjunto de trens e conjunto de testes. A eficiência do sistema desenvolvido pode ser testada e comparada com base em fatores tais como otimização de parâmetros, otimização de características e variabilidade no tamanho do

conjunto de dados.

Além do desempenho dos conjuntos de dados disponíveis e das técnicas utilizadas para o IDS, a escolha de uma métrica de desempenho adequada é também um dos fatores cruciais que devem ser levados em consideração. A métrica mais comumente utilizada para mostrar a eficácia do sistema é a precisão [14]. A exatidão é calculada

considerando
a pequena porção do conjunto de teste ou a precisão média em muitos conjuntos de teste é avaliada, precisão para um
a categoria dos ataques é medida, ou é apresentada a precisão das amostras corretamente classificadas do conjunto de
treinamento

[15] , [16], [17]. Portanto, uma única métrica de desempenho não é suficiente para medir a eficiência do algoritmo. É necessário considerar a matriz de confusão e encontrar o número de falsos positivos e falsos negativos para derivar outras métricas de desempenho, tais como Taxa de Detecção (DR), Taxa de Falso Positivo (FPR), precisão e recall [13]. A precisão
de um determinado tipo de ataque é também um aspecto crítico, pois o classificador pode dar maior precisão para um tipo de ataque, mas pode falhar na classificação do outro [18].

A contribuição do documento pode ser resumida como:

- Visão geral das técnicas ML e DM usadas para IDS.
- Revisão dos conjuntos de dados de detecção de intrusão para avaliação do desempenho do IDS.
- Discussão sobre o CIC-IDS-2017 e CSE-CIC-IDS-2018 com características e limitações dos conjuntos de dados.

O roteiro do documento é o seguinte: a seção 2 discute as técnicas para o IDS. A seção 3 é uma discussão sobre os conjuntos de dados do IDS e a seção 4 apresenta um estudo sobre os conjuntos de dados CIC-IDS-2017 e CSE-CIC-IDS-2018. Concluímos o trabalho com o escopo de pesquisa futura na seção 5.

2. Técnicas para o Sistema de Detecção de Intrusão

Vários métodos ML e DM implementados para o desenvolvimento de um IDS são mostrados na Figura 2. Por exemplo, uma visão geral dos métodos ML usados para o IDS é apresentada em [19]. O documento descreve diferentes métodos híbridos e de conjunto, juntamente com técnicas de seleção de características. A pesquisa bibliográfica destaca os métodos homogêneos e heterogêneos de conjunto.
ods implementados para o IDS. Uma pesquisa dos métodos ML e DM apresentados em [6], na qual o documento discute o algo- rithms implementado para o IDS usando diferentes subconjuntos do conjunto de dados KDD CUP 99 [12].

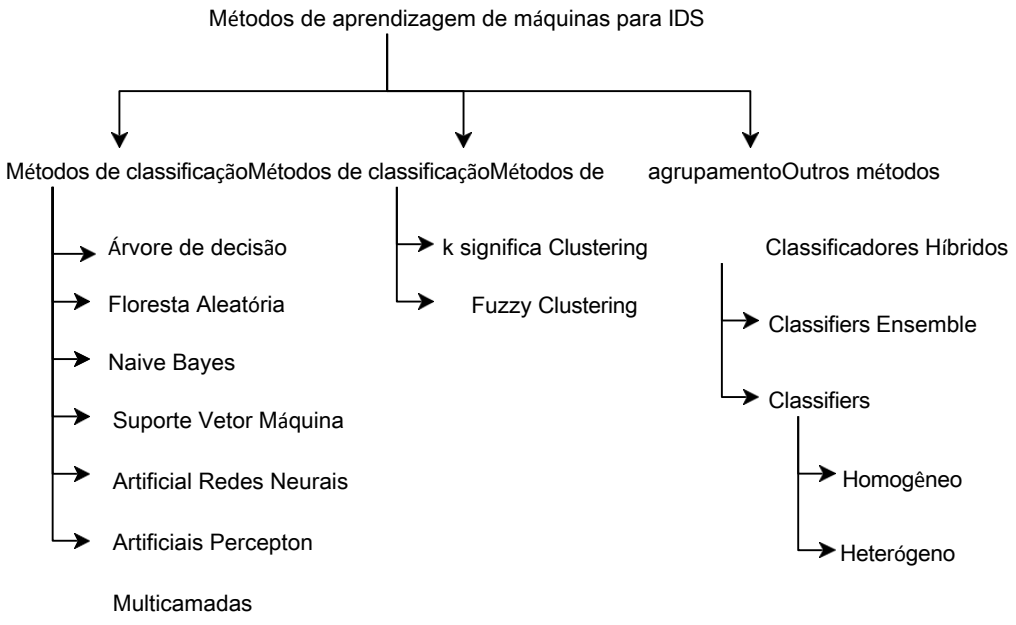

Fig. 2. Taxonomia das técnicas utilizadas para o IDS

Um estudo sobre o conjunto de dados NSL-KDD discutido em [13], onde os algoritmos ML implementados no conjunto de dados NSL-KDD [12]. Entretanto, o estudo se concentra em medir a eficiência do conjunto de dados através da implementação de algoritmos ML. Os experimentos foram conduzidos usando a ferramenta WEKA [20] e o desempenho do conjunto de dados para diferentes classificadores foi registrado. O trabalho concluiu que não é necessário considerar todas as características para treinamento e classificação de ataques e
O NSL-KDD é claramente uma versão refinada do conjunto de dados KDD CUP 99 [13]. Um tipo similar de questão foi abordado em [5] onde algoritmos ML comuns foram pesquisados, e desafios para comparar a eficiência de várias técnicas foram declarados para o conjunto de dados KDD CUP 99. O documento afirmava que uma grande preocupação para realizar a análise comparativa é a falta de um banco de testes eficaz. O documento listou as

questões comuns com o conjunto de dados KDD CUP 99 e sugeriu o uso de

o mesmo tamanho de amostras do mesmo conjunto de dados para a realização de uma análise comparativa de diferentes técnicas de classificação de ataques.

Um conjunto de diretrizes foi introduzido em [7] para preencher a lacuna entre as exigências atuais dos conjuntos de dados IDS e suas deficiências. O documento também discute técnicas para construir conjuntos de dados usando essas diretrizes. Além dos conjuntos de dados disponíveis publicamente, conjuntos de dados simulados também foram usados para medir o desempenho do IDS em redes com e sem fio. Em [21], um conjunto de dados simulado foi criado para redes móveis ad-hoc e algoritmos ML foram aplicados para detectar anomalias nas redes sem fio.

Uma abordagem híbrida é proposta em [16], combinando o classificador Na¨ıve Bayes (NB) com o método de redução baseado em funcionalidade e vitalidade. As simulações foram realizadas no conjunto de dados NSL-KDD e um conjunto reduzido de recursos foi usado para a classificação de ataque. O conjunto de dados NSL-KDD consiste em 41 características que foram reduzidas a 25 características usando o método de redução de características. O método proposto mostrou 98% de precisão. Técnicas ML sem supervisão, como o agrupamento de meios *k*- é usado em [22] para analisar o conjunto de dados do NSL-KDD. Aqui, 20% das instâncias do conjunto de dados NSL-KDD agrupadas em quatro clusters.

Além dos métodos de aprendizagem supervisionada e não supervisionada, a aprendizagem semi-supervisionada também é utilizada para a intrusão de técnicas. Um método ML semi-supervisionado de base difusa proposto em [23], no qual instâncias não rotuladas são consideradas para avaliação de desempenho. Aqui, uma rede neural de alimentação de camada única é usada para treinar o modelo para fornecer um vetor de afiliação difuso para aprender cada categoria de ataque separadamente. Os experimentos realizados no conjunto de dados NSL-KDD revelam que instâncias não rotuladas com baixo e alto valor de imprecisão contribuem mais para melhorar a precisão do sistema.

Os classificadores de conjunto também estão sendo utilizados para a classificação de ataque. Uma abordagem de agrupamento para classificação binária e multi-classe é apresentada em [24]. Ela é baseada em uma busca adaptativa gananciosa e aleatória combinada com classificadores florestais aleatórios. A abordagem proposta utilizou um procedimento de busca aleatória adaptável e gananciosa para a construção de árvores de decisão aleatórias. Os experimentos realizados no conjunto de dados NSL-KDD usando três métodos de seleção de características, a saber, Ganho de Informação (IG), Incerteza Simétrica (SU) e Método de Seleção de Característica Baseada em Correlação (CFS) [24]. Os resultados mostraram que a abordagem proposta superou o desempenho das técnicas ML como classificador florestal aleatório, perceptron multicamadas, e NB e métodos de seleção de características melhoraram a precisão do sistema.

Os classificadores ML extremos também são utilizados no estudo dos perfis de tráfego da rede para classificar os ataques. Os perfis de tráfego de rede são examinados em [25], onde o ML extremo online se aplica para detectar intrusões. A proposta
A estrutura utiliza o perfil alfa para minimizar o tempo computacional, o perfil beta para minimizar o conjunto de dados de treinamento, e as características são reduzidas utilizando a abordagem combinada de filtro, correlação e consistência. Os experi- mentos realizados no conjunto de dados NSL-KDD que deram 98,6% de precisão com 1,7% de FPR para classificação binária e 97,6% de precisão e 1,7% de FPR para classificação multiclasse. Os experimentos também foram realizados com o conjunto de dados da Universidade de Kyoto, com 96,37% de exatidão e 5,7% de FPR. Um resumo das técnicas utilizadas para o IDS é apresentado na Tabela 2.

3. Revisão dos conjuntos de dados de detecção de intrusão

Um conjunto de dados de detecção de intrusão pode ser desenvolvido coletando informações de fontes variadas, como fluxos de tráfego de rede que contém informações sobre o host, comportamento do usuário e configurações do sistema [26]. Estas informações são necessárias para estudar os padrões de ataque e a atividade anormal de vários ataques à rede. A atividade da rede é coletada através de um roteador ou switch de rede. Após a coleta do tráfego de entrada e de saída da rede, a rede
A análise do fluxo é realizada para estudar o tráfego da rede. A análise do fluxo pode ser descrita como o processo de análise do
informações sobre pacotes de rede, como endereço IP de origem, endereço IP de destino, número da porta de origem, porta de destino
número, tipo de serviços de rede, para citar alguns [27]. O host de rede fornece as configurações do sistema e as informações do usuário que não podem ser extraídas da análise do fluxo da rede. Por exemplo, informações obtidas através de tentativas falhadas de login, observando a atividade de intrusão.

Os analistas de segurança de rede podem detectar intrusões observando as informações obtidas dos pacotes de rede através da análise do fluxo da rede. Algumas categorias de ataque, como descritas no conjunto de dados DARPA [11], podem ser listadas como segue:

- Negação de Serviço (DoS): É um ataque de intrusão realizado ao tornar os recursos da rede ocupados e indisponíveis para os usuários legítimos.
- User to Root (U2R): É um ataque de intrusão causado por impedir a autenticidade do usuário causado pela permissão de acesso à raiz do intruso.

Tabela 2. Resumo das Técnicas para o IDS

Ref	Técnica	Característica Selec...	Dataset	Análise de resultados
[16]	NB	Caracter ística baseada na vitalidade	A abordagem híbrida	NSL-KDDA é proposta combinando NB com o método de seleção de características baseado na vitalidade para alcançar uma precisão de 98%.
[22]	k grupos...	significa	Não usado	NSL-KDDD As instâncias do conjunto de dados estão agrupadas em ters representando quatro classes de ataque junto com o tráfego normal.
[13]	J48, SVM, NB	Correlação - sediada em		NSL-KDDO desempenho do classificador é melhorado por usando o método de seleção de características. Dos três classificadores utilizados, o J48 tem um desempenho superior em termos de precisão de classificação (99,8%).
[25]	Sequencial ex- treme ML	Abordagem combinada no filtro, corre- lação, e consistência	NSL-KDD, Kyoto	Os experimentos são conduzidos no NSL-KDD dá 98,6% de precisão para classificação binária e 97,6% de precisão para classificação multiclasse. Os experimentos realizados com o conjunto de dados de Kyoto proporcionam uma precisão de 96,37%.
[24]	Floresta de tamanho aleatório e ganancioso Adap- tive Random- izado	IG, SU, e CFS	NSL-KDD	Os resultados experimentais são apresentados tanto para a classificação binária como para a multiclasse. Os resultados mostram que a abordagem proposta atinge a maior precisão com o método de seleção de características baseado em SU tanto para a classificação binária (85,05%) como para a classificação multiclasse (77,6%), em comparação com outros métodos.
[23]	Rede Neural Fuzzy	Não	usado	NSL-KDDO conjunto de treinamento é dividido em baixo e alto fuzzi- ness grupos e vetor de filiação fuzzy é usado para estudar as instâncias. O modelo proposto dá a taxa de precisão de 84,12%.

- Remota para Local (R2L): É um ataque de intrusão causado pela quebra da integridade da rede e que permite o acesso da rede local ao intruso.
- Sonda: É uma atividade de intrusão realizada pela varredura da rede e coleta de todas as informações relacionadas à rede sobre as atividades da rede realizadas na rede.

Os conjuntos de dados de detecção de intrusão gerados a partir dos traços reais de tráfego na rede são apresentados na Tabela **???**. Estes conjuntos de dados foram utilizados para a avaliação do desempenho do IDS por muitos pesquisadores. Para citar alguns, o primeiro conjunto de dados de detecção de intrusão foi criado pelo Laboratório MIT Lincoln em 1998 e foi nomeado como DARPA no âmbito do DARPA
projeto financiado [11]. Mais tarde, em 1999, os arquivos tcpdump da DARPA foram refinados e processados pelos pesquisadores da Universidade da Califórnia para formar o conjunto de dados KDD CUP 99 [12]. O conjunto de dados KDD CUP 99 foi formado com um grande número de registros duplicados e redundantes que foram removidos para formar o conjunto de dados NSL-KDD [13]. Para avaliar as técnicas de correlação de alerta IDS, um conjunto de dados foi criado capturando os detalhes da bandeira dos pacotes da rede. Isto
O conjunto de dados foi nomeado como DEFCON e definiu categorias de ataque tais como varredura de portas e estouro de buffer [28]. Os conjuntos de dados CAIDA e LBNL IDS são formados pelo exame dos traços do fluxo da rede e dos pacotes da rede. A CAIDA foi

desenvolvido pelo Center of Applied Internet Data Analysis [29] e LBNL foi desenvolvido pelo Lawrence Berkeley National Laboratory [30]. A academia militar dos Estados Unidos gerou um conjunto de dados chamado CDX baseado na competição de guerra em rede e este conjunto de dados foi usado para avaliar as regras de alerta do IDS [31]. O conjunto de dados de Kyoto [32] e Twente [33] foram desenvolvidos através da análise das atividades dos honeypots implantados em suas respectivas áreas universitárias. O conjunto de dados UMASS foi formado pelo exame dos arquivos de rastreamento dos pacotes de rede e aplicações sem fio [34] e ISCX IDS 2012 pela observação do perfil alfa e beta dos pacotes de rede [7], enquanto o conjunto de dados AFDA consiste de características que mostram o padrão de ataque e traços de chamadas do sistema [35]. Os conjuntos de dados CIC-IDS-2017 e CSE-CIC-IDS-2018 são

os recentes conjuntos de dados que foram desenvolvidos pelo Instituto Canadense de Segurança Cibernética, realizando a caracterização do tráfego de intrusão. Estes conjuntos de dados consistem em sete categorias de ataque que descrevem os cenários de ataque recentes [36].

A maioria das pesquisas realizadas no campo do IDS tem usado o KDD CUP 99 e o NSL-KDD para medir o desempenho de diferentes classificadores [13]. Estes conjuntos de dados consistem em 41 características e quatro categorias de ataque. As características extraídas são categorizadas em quatro classes como se segue:

- Básico: Estas características extraídas da conexão *TCP/IP* aberta estabelecida entre os laços par-comunicantes.
- Anfitrião: Estas características extraídas das conexões do host com base no protocolo utilizado e no tipo de serviço.
- O tráfego: Estas características extraídas das conexões tendo o mesmo serviço.
- Conteúdo: Estas características extraídas dos padrões seqüenciais dos dados para detectar intrusões.

O conjunto de dados KDD CUP 99 e NSL-KDD lista algumas categorias de ataque, enquanto os conjuntos de dados CIC-IDS-2017 e CSE-CIC-IDS- 2018 listam uma nova gama de ataques gerados a partir de recursos reais de tráfego de rede, tais como Negação de Serviço Distribuída, Negação de Serviço, força bruta, XSS, Injeção SQL, Botnet, Ataque Web e Infiltração. Estes conjuntos de dados têm rotulado instâncias com mais de 80 características.

Tabela 3: Resumo dos conjuntos de dados IDS gerados a partir do traço real da rede - traços de ficção

Nome do conjunto de dados	desenvolvido por	características	Tipos de ataque	Descrição
DARPA	Laboratório MIT Lincoln	41	Dos, R2L, U2R, Sonda	Ela não representa tráfego real da rede, ausência de instâncias falso-positivas, irregularidades em instâncias de dados de ataque.
KDD CUP 99	Universidade de Califórnia	41	Dos, R2L, U2R, Sonda	Consiste em dados redundantes e duplicados mesmo- ples.
NSL-KDD	Universidade de Califórnia	41	Dos, R2L, U2R, Sonda	Versão refinada do conjunto de dados KDD CUP 99 e con- sist de um número limitado de tipos de ataque.
Grupo	DEFCONShmoo Bandeira	traços	Protocolo Telnet Attacks	As características são capturadas através da competição "Capture the Flag".
CAIDA	Centro de Análise de Dados da Internet Applied	20	DDoSIt	consiste de instâncias que são muito específicas para um tipo particular de ataque ou atividade na Internet.
LBNL	Laboratório Nacional Lawrence Berkeley	Traços da Internet	atividade especificando o	Traços maliciosos Consiste em 100 horas de vestígios de cabeçalho de pacote para identificar o tráfego malicioso.
	CDXUnited States Military Academy	5Buffer Overflow Nikto e Nessus		Este conjunto de dados utilizou ferramentas de rede para capturar o tráfego e foi usado para avaliar as regras de alerta do IDS.
Kyoto	Kyoto Universidade	24Sessões	Normais e de Ataque	Foi desenvolvido através da implantação de honeypots na rede, mas não descreve nenhum detalhe sobre os tipos de ataque.
	TwenteTwente Uni- versity		ISCX2012	Universidade de Novo

	Brunswick	IP fluxos	Malicioso tráfego, Efeito colateral tráfego, tráfego desconhecido, e alertas não relacionados a DoS, DDoS, força bruta, Infiltração	O tamanho do conjunto de dados é pequeno e o escopo dos tipos de ataque é limitado.	
		IP fluxos		Este conjunto de dados consiste em cenários de rede com atividades de confiança e instâncias de dados etiquetadas.	

Continua na próxima página

Tabela 3 - *Continuação da página*

anterior Dataset Name		Desenvolvido		ByFeatures
Tipos de ataque	Descrição			
AFDA de	Universidade	Sistema	Zero-dia ataques,	Este conjunto de dados consiste em 10 vetores de ataque ao longo
	Novo Sul País de Gales	ligue para traços	Ataque furtivo, C100 tem ataques.	com os traços das outras instâncias de dados, mas Ataque à concha da web uma gama limitada de
CIC-IDS-2017	Canadense em... stitute de Cy- segurança ber	80	Bruto força, de dados Cana portuária, Dos, DDoS, Web, Infiltração	Os perfis de rede são usados para gerar o conjunto Botnet, de uma maneira específica.
CSE-CIC-IDS-2018	Canadense em... stitute de Cy- segurança ber	80	Bruto força, de dados Cana portuária, Dos, DDoS, Web, Infiltração	Os perfis de rede são usados para gerar o conjunto Botnet, de uma maneira específica.

4. Discussão sobre o conjunto de dados recentes do IDS: CIC-IDS-2017 e CSE-CIC-IDS-2018

Os padrões de comportamento dos ataques de rede mudam gradualmente e, portanto, é necessário atualizar os conjuntos de dados conven- tionais no ambiente dinâmico. Isto ajudará a manifestar diferentes cenários de tráfego de rede e padrões de ataque que são fáceis de adaptar, aprender e redefinir [37]. Além disso, a escolha de um conjunto de dados apropriado também é uma tarefa crítica.

Alguns conjuntos de dados são desenvolvidos por organizações específicas para seu propósito de pesquisa e não estão disponíveis publicamente, enquanto os conjuntos de dados que estão disponíveis publicamente contêm registros que podem não corresponder à demanda tecnológica atual. De fato, estes conjuntos de dados disponíveis ao público são estatisticamente deficientes [38] e, portanto, a não disponibilidade de um conjunto de dados ideal é uma questão que precisa ser levada em consideração [38].

Para desenvolver e avaliar a estrutura dos conjuntos de dados IDS, poucas características críticas foram derivadas para construir um conjunto de dados IDS completo e eficiente [37]. Estas características são listadas como diversidade de ataques, anonimato, protocolos disponíveis, captura do tráfego completo da rede, captura da interação completa da rede, definição da configuração completa da rede, conjunto de características, amostras de dados rotuladas, heterogeneidade e metadados [37]. O CIC-IDS-2017

e conjuntos de dados CSE-CIC-IDS-2018 são desenvolvidos mantendo estas características em consideração. Estes conjuntos de dados têm usado o conceito de perfis para gerar os conjuntos de dados de uma forma bem ordenada. Ambos os conjuntos de dados apresentam um conhecimento profundo dos ataques realizados e conhecimento conceitual sobre os diferentes modelos de aplicação, rede

dispositivos, e protocolos. O tráfego de rede foi capturado usando o CICFlowMeter que atribuiu um

rotular o fluxo e também fornecer detalhes sobre o endereço de origem e destino e número do porto, carimbo da hora e ataque. As simulações do ambiente de teste consistem no tráfego de rede gerado a partir de protocolos como HTTP, HTTPS, SSH e protocolos de e-mail como SMTP e POP3.

4.1. Características do Dataset

A formação dos conjuntos de dados CIC-IDS-2017 e CSE-CIC-IDS-2018 atraiu muitos pesquisadores para implementar diferentes classificadores usando esses novos conjuntos de dados [39], [40], [41]. As especificações dos conjuntos de dados estão listadas na Tabela 4. Os arquivos presentes no conjunto de dados são usados para classificação binária, bem como para classificação multiclasse. Um IDS ideal pode ser descrito como aquele que é capaz de detectar com precisão cada tipo de ataque e, portanto, para construir um IDS eficiente, os arquivos do conjunto de dados devem ser fundidos para ter uma ampla gama de categorias de ataque [42]. Além disso, estes conjuntos de dados são desenvolvidos

levando em consideração as onze características de um conjunto de dados ideal apresentado em [43] e que estão listadas

na Tabela 5.

4.2. Limitações dos conjuntos de dados

As observações dos conjuntos de dados CIC-IDS-2017 e CSE-CIC-IDS-2018 têm poucas limitações em relação às amostras de dados e aos arquivos criados pela análise de fluxo de rede que podem ser listados como:

- As amostras de dados geradas pela análise do fluxo da rede são armazenadas em arquivos e processar esses arquivos é uma tarefa muito tediosa, pois esses arquivos têm um grande número de instâncias de dados em cada arquivo.

Tabela 4. Especificações dos conjuntos de dados do CIC-IDS-2017 e CSE-CIC-IDS-2018 [36]

Nome do conjunto de dados	CIC-IDS-2017	CSE-CIC-IDS-2018
Tipo de conjunto de dados	Multi-classe	Multi-classe
Ano de formação	2017	2018
Duração da Captura	5 dias	10 dias
Infra-estrutura de ataque	4 PCs, 1 roteador, 1 switch	50 PCs
Infra-estrutura da vítima	3 servidores, 1 firewall, 2 interruptores, 10 PCs	420 PCs, 30 servidores
Características	80	80
Número de classes	15	18

Tabela 5. Características para a construção de um conjunto de dados ideal [43]

Característica	Descrição
Configuração de rede	Refere-se a ter conhecimento completo sobre a topologia de rede de como os dispositivos de rede são conectados no ambiente de teste para que cenários de ataque realistas sejam capturados.
Network Traffi	Refere-se à captura de todos os pacotes de rede do host, destino, firewall e aplicações web para análise de fluxo e geração de conjuntos de dados.
Dataset	Refere-se à marcação das instâncias de dados capturadas do tráfego da rede para ter uma compreensão completa da interação da rede.
Network Interaction	Refere-se a ter o registro completo da comunicação da rede ocorrendo dentro e fora da rede
Capturar o Traffi	Refere-se à captura do tráfego funcional e não funcional da rede para medir o DR e FPR do IDS.
Protocolos	Um conjunto de dados ideal deve incluir toda a comunicação utilizando diferentes protocolos, sejam eles nem maliciosos ou mal-intencionados.
Ataques	O conjunto de dados deve consistir em uma ampla gama e categorias de ataques atualizadas
Anonimato	O conjunto de dados deve incluir informações do cabeçalho do pacote, bem como a carga útil do pacote.
HeterogeneidadeO	conjunto de dados deve ser coletado de fontes variadas para cobrir todos os detalhes do procedimento realizado para detectar os ataques.
Características	O conjunto de dados deve manter um conjunto completo de características bem definidas para classificar o ataque.
Metadados	Um conjunto de dados deve ter documentação adequada descrevendo o ambiente de teste, o sistema de ataque...
	infra-estrutura do tem, infra-estrutura do sistema de vítimas e cenários de ataque.

- Os arquivos do conjunto de dados podem ser fundidos para incluir cada uma das etiquetas de ataque para processamento. Mas a combinação das instâncias de cada tipo de ataque aumenta o tamanho do conjunto de dados, o que resulta em mais tempo de computação e processamento.
- O conjunto de dados também consiste em alguns registros de dados ausentes e redundantes.
- Os conjuntos de dados CIC-IDS-2017 e CSE-CIC-IDS-2018 são propensos à questão do desequilíbrio de alta classe que pode resultar em baixa precisão e alta FPR do sistema [42].

Estas questões podem ser tratadas através do pré-processamento das amostras de dados, pela aplicação da engenharia de recursos ou pela eliminação dos registros que faltam. O desequilíbrio de alta classe pode ser tratado por meio de re-rotulagem ou amostragem das amostras de dados e isto, por sua vez, aumentaria a probabilidade de ocorrência de amostras de dados de todas as classes.

5. Conclusão

O estudo revisa os conjuntos de dados desenvolvidos no campo do Sistema de Detecção de Intrusão (IDS). Estes conjuntos de dados têm sido usados para avaliação do desempenho do IDS baseado em ML e DM. O estudo revelou que há necessidade de atualizar o conjunto de dados subjacentes para identificar os ataques recentes no campo do IDS com melhor desempenho. Isto se deve ao fato de que
os atacantes executam os ataques utilizando processos e tecnologias variadas. Além disso, o padrão de execução de diferentes ataques simula a necessidade de ter conjuntos de dados com cenários de rede realistas. Para cumprir a exigência de construir um conjunto de dados de detecção de intrusão com tráfego de rede realista e ataques de rede atualizados, foram introduzidos os conjuntos de dados CIC-IDS-2017 e CSE-CIC- IDS-2018. Este documento revisa as características destes conjuntos de dados e também discute
algumas falhas. No futuro, nos concentramos no estudo do desempenho desses conjuntos de dados com várias técnicas ML e DM, juntamente com a incorporação de engenharia de características e amostragem de dados para solucionar as deficiências desses conjuntos de dados.

Referências

[1] Stevens T. Cyber segurança e a política do tempo. Imprensa da Universidade de Cambridge; 2016.
[2] Miller NJ, Aliasgari M. Benchmarks para avaliar soluções de detecção de intrusão baseadas em anomalias. Universidade Estadual da Califórnia, Long Beach; 2018.
[3] Scaife N, Carter H, Traynor P, Butler KR. Cryptolock (e solte-o): parando os ataques de resgate aos dados dos usuários. Em: 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2016. p. 303-312.
[4] Gupta B, Agrawal DP, Yamaguchi S. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global; 2016.
[5] Garcia-Teodoro P, Diaz-Verdejo J, Macia'-Ferna'ndez G, Va'zquez E. Detecção de intrusão de rede baseada em anomalias: Técnicas, sistemas e desafios. computadores e segurança. 2009;28(1-2):18–28.
[6] Buczak AL, Guven E. Uma pesquisa sobre mineração de dados e métodos de aprendizagem de máquinas para detecção de intrusão de segurança cibernética. IEEE Communications Surveys & Tutorials. 2016;18(2):1153–1176.
[7] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA. Rumo ao desenvolvimento de uma abordagem sistemática para gerar conjuntos de dados de referência para detecção de intrusão. computadores e segurança. 2012;31(3):357–374.
[8] Agrawal S, Agrawal J. Levantamento sobre detecção de anomalias utilizando técnicas de mineração de dados. Procedia Computer Science. 2015;60:708–713.
[9] Belavagi MC, Muniyal B. Avaliação de desempenho de algoritmos de aprendizagem supervisionada de máquinas para detecção de intrusão. Procedia Computer Science. 2016;89:117–123.
[10] Ektefa M, Memar S, Sidi F, Affendey LS. Detecção de intrusão usando técnicas de mineração de dados. Em: 2010 International Conference on Information Retrieval & Knowledge Management (CAMP). IEEE; 2010. p. 200-203.
[11] Cunningham RK, Lippmann RP, Fried DJ, Garfinkel SL, Graf I, Kendall KR, et al. Avaliar sistemas de detecção de intrusão sem atacar seus amigos: A avaliação de detecção de intrusão DARPA 1998. Laboratório Lexington Lincoln do Instituto de Tecnologia de Massachusetts; 1999.
[12] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. Uma análise detalhada do conjunto de dados da KDD CUP 99. Em: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. IEEE; 2009. p. 1-6.
[13] Dhanabal L, Shantharajah S. Um estudo sobre o conjunto de dados NSL-KDD para sistema de detecção de intrusão baseado em algoritmos de classificação. International Journal of Advanced Research in Computer and Communication Engineering. 2015;4(6):446–452.
[14] Tavallaee M, Stakhanova N, Ghorbani AA. Para uma avaliação confiável dos métodos de detecção de intrusão baseados em anomalias. IEEE Transactions on Systems, Man, and Cybernetics, Parte C (Applications and Reviews). 2010;40(5):516–524.
[15] Deshmukh DH, Ghorpade T, Padiya P. Sistema de detecção de intrusão através de melhores métodos de pré-processamento e Na¨ıve Bayes classificadora usando NSL-KDD 99 Dataset. Em: 2014 International Conference on Electronics and Communication Systems (ICECS). IEEE; 2014. p. 1-7.
[16] Mukherjee S, Sharma N. Detecção de intrusão usando o classificador Bayes ingênuo com redução de características. Tecnologia de Procedimentos. 2012;4:119–128.
[17] Pervez MS, Farid DM. Seleção de características e classificação de intrusão no conjunto de dados NSL-KDD Cup 99 empregando SVMs. In: A 8ª Conferência Internacional sobre Software, Conhecimento, Gerenciamento de Informação e Aplicações (SKIMA 2014). IEEE; 2014. p. 1-6.
[18] Farid DM, Harbi N, Rahman MZ. Combinando baias ingênuas e árvore de decisão para detecção de intrusão adaptativa. arXiv preprint arXiv:10054496. 2010;.
[19] Aburomman AA, Reaz MBI. Um levantamento dos sistemas de detecção de intrusão baseados em classificadores de conjuntos e híbridos. Computadores e Segurança. 2017;65:135–152.
[20] Srivastava S. Weka: uma ferramenta para pré-processamento de dados, classificação, conjunto, agrupamento e mineração de regras de associação. International Journal of Computer Applications. 2014;88(10).
[21] Damopoulos D, Menesidou SA, Kambourakis G, Papadaki M, Clarke N, Gritzalis S. Avaliação do IDS baseado em anomalias para dispositivos móveis que utilizam classificadores de aprendizagem de máquinas. Redes de Segurança e Comunicação. 2012;5(1):3–14.
[22] Kumar V, Chauhan H, Panwar D. K significa abordagem de agrupamento para analisar o conjunto de dados de detecção de intrusão NSL-KDD. International Journal of Soft Computing and Engineering (IJSCE). 2013;.

[23] Ashfaq RAR, Wang XZ, Huang JZ, Abbas H, He YL. Abordagem de aprendizagem semi-supervisionada baseada em imprecisão para sistema de detecção de intrusão. Ciências da Informação. 2017;378:484–497.

[24] Kanakarajan NK, Muniasamy K. Melhorando a precisão da detecção de intrusão usando o GAR-Forest com seleção de características. In: Anais da 4ª Conferência Internacional sobre Fronteiras em Computação Inteligente: Teoria e Aplicações (FICTA) 2015. Springer; 2016. p. 539-547.
[25] Singh R, Kumar H, Singla R. Um sistema de detecção de intrusão usando perfil de tráfego de rede e máquina de aprendizagem online sequencial extrema. Sistemas especialistas com aplicações. 2015;42(22):8609–8624.
[26] Koch R. R. Rumo à detecção de intrusão de próxima geração. Em: 2011 3rd International Conference on Cyber Conflict. IEEE; 2011. p. 1-18.
[27] Rajahalme J, Conta A, Carpenter B, Deering S. RFC 3697: Especificação da etiqueta de fluxo IPv6. In: The Internet Society; 2004. .
[28] Nehinbe JO. Um método simples para melhorar as detecções de intrusão em redes corporativas. In: Conferência Internacional sobre Segurança da Informação e Forense Digital. Springer; 2009. p. 111-122.
[29] Shannon C, Moore D. O conjunto de dados da caida sobre o verme espirituoso. O suporte para o Witty Worm Dataset e o UCSD Network Telescope são fornecidos pela Cisco Systems, Limelight Networks, o Departamento de Segurança Nacional dos EUA, a National Science Foundation. 2004;.
[30] Nechaev B, Allman M, Paxson V, Gurtov A. Lawrence berkeley laboratório nacional (lbnl)/projeto de rastreamento de empresas. Berkeley, CA: LBNL/ICSI. 2004;.
[31] Sangster B, O'Connor T, Cook T, Fanelli R, Dean E, Morrell C, et al. Rumo às competições de instrumentos de guerra em rede para gerar Datasets etiquetados. In: CSET; 2009. .
[32] Song J, Takakura H, Okabe Y, Eto M, Inoue D, Nakao K. Análise estatística dos dados do honeypot e construção do conjunto de dados de Kyoto 2006+ para avaliação do NIDS. In: Anais do Primeiro Workshop de Análise de Construção de Conjunto de Dados e Retornos da Experiência de Coleta de Dados para Segurança. ACM; 2011.
p. 29–36.
[33] Barbosa RRR, Sadre R, Pras A, van de Meent R. Simpleweb/universidade de dados de traços de tráfego twente. Centro de Telemática e Tecnologia da Informação da Universidade de Twente, Enschede, Relatório Técnico. 2010;.
[34] Liberatore M, Shenoy P. Umass repositório de vestígios. Acessado: Maio; 2017.
[35] Creech G, Hu J. Geração de um novo conjunto de dados de teste IDS: Hora de aposentar a coleção KDD. Em: 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE; 2013. p. 4487-4492.
[36] Sharafaldin I, Lashkari AH, Ghorbani AA. Para a geração de um novo conjunto de dados de detecção de intrusão e caracterização do tráfego de intrusão. In: ICISSP; 2018. p. 108-116.
[37] Sharafaldin I, Gharib A, Lashkari AH, Ghorbani AA. Rumo a um conjunto de dados de referência confiável de detecção de intrusão. Software Networking. 2018;2018(1):177–200.
[38] Koch R, Golling M, Rodosek GD. Rumo à comparabilidade dos sistemas de detecção de intrusão: Novos conjuntos de dados. In: TERENA Networking Conference. vol. 7; 2014. .
[39] Nicholas L, Ooi SY, Pang YH, Hwang SO, Tan SY. Estudo da memória de longo prazo em sistema de detecção de intrusão de rede baseado em fluxo. Journal of Intelligent & Fuzzy Systems. 2018;(Preprint):1–11.
[40] Radford BJ, Richardson. SequenceAggregation Rules for Anomaly Detection in Computer Network Traffi. arXivpreprint arXiv:180503735. 2018;.
[41] Vijayanand R, Devaraj D, Kannapiran B. Sistema de detecção de intrusão para rede de malha sem fio usando múltiplos suportes vetoriais de classificação de máquinas com seleção de características baseadas em genético-algoritmo. Computadores e Segurança. 2018;77:304–314.
[42] Panigrahi R, Borah S. Uma análise detalhada do conjunto de dados do CICIDS2017 para o projeto de Sistemas de Detecção de Intrusão. International Journal of Engi- neering & Technology. 2018;7(3.24):479–482.
[43] Gharib A, Sharafaldin I, Lashkari AH, Ghorbani AA. Uma estrutura de avaliação para o conjunto de dados de detecção de intrusão. Em: Conferência Internacional 2016 - Ence on Information Science and Security (ICISS). IEEE; 2016. p. 1-6.