

# Segurança de Computadores e Redes

Universidade Estadual Paulista Júlio de Mesquita Filho

Prof. Dr. Kelton Augusto Pontara da Costa

Aula 4

# Sumário

- 1 Abordagem da aula 4
  - Detecção baseada em mineração de dados
  - Datasets
  - KDD e Data Mining
  - O processo de KDD
  - Tarefas de Data Mining
  - Anomalia e Intrusão
  - Matriz de Confusão
  - Seminários

- As técnicas de mineração de dados são capazes de lidar com grandes quantidades de dados, buscando padrões consistentes entre estes dados e formando subconjuntos que respeitem determinadas regras de associação.
- As soluções que utilizam a mineração de dados têm um objetivo parecido com as soluções que utilizam processamento de sinais: separar em dois subconjuntos os dados considerados normais e os dados considerados anômalos durante o processamento das informações coletadas da rede.

- Técnicas relacionadas à mineração de dados como PCA (Principal Component Analysis), PSO-KM (K-Means-based on Particle Swarm Optimization) e CSI-KNN (Combined Strangeness and Isolation measure K-Nearest Neighbors) são utilizadas com bons resultados para identificar em grandes conjuntos de dados coletados da rede, quais são os dados anômalos e quais são os dados normais.

- Datasets são conjuntos de dados de tráfego coletados de uma rede, contendo ou não tráfego malicioso (KDD CUP 99, 2016). A seguir pode ser visto exemplos de datasets e suas respectivas descrições.

- KDDCup'99: O KDDCup'99 é um conjunto de dados utilizados no 3o Concurso Internacional de Descoberta de Conhecimento e Mineração de Dados. A tarefa era construir um detector de intrusão de rede, um modelo preditivo capaz de distinguir conexões maliciosas ou ataques e conexões normais. Esta base de dados contém um conjunto padrão de dados a serem auditados, que inclui uma grande variedade de intrusões simulados em ambiente militar e abrange as categorias de ataques DoS, R2L, U2R e Probing (KDD CUP 99, 2016). É o conjunto de dados mais utilizado para avaliação de sistemas de detecção de intrusão.

- Darpa: O dataset Darpa foi criado no laboratório Lincoln do MIT (Massachusetts Institute of Technology), sob patrocínio da DARPA, onde foi coletado um conjunto de dados para avaliação de sistemas de detecção de intrusão. Os dados foram coletados de uma rede com tráfego em máquinas reais e simuladas, sendo os ataques efetuados contra máquinas reais. A coleta foi efetuada durante semanas, gerando arquivos com as 4 principais categorias de ataques e tráfego normal.

- UNB ISCX 2012: O dataset UNB ISCX 2012 foi criado pelo ISCX Information Security Centre of Excellence, pertencente a Universidade de New Brunswick no Canadá. O dataset foi baseado no conceito de perfis, contendo descrições detalhadas de intrusões e modelos abstratos de distribuição para aplicações, protocolos ou entidades de rede de nível inferior. Os traços reais foram analisados para criar perfis de agentes que geram tráfego real para HTTP, SMTP, SSH, IMAP, POP3 e FTP. Então foi criado um conjunto de diretrizes para delinear conjuntos de dados válidos, que estabelecem a base para a geração de perfis. Os perfis foram utilizados em vários cenários com ataques, então capturado o tráfego e gerado os arquivos do dataset.



- Atualmente a capacidade de coletar e armazenar dados é muito maior do que nossa capacidade de analisar e compreender os mesmos. Técnicas computacionais e ferramentas são essenciais para o suporte a extração de conhecimento útil em grandes volumes de dados.
- Essas técnicas e ferramentas são do campo da KDD - Knowledge Discovery in Databases ou Descoberta de Conhecimento em Base de dados, definido por Fayyad et al. como o processo de identificação de padrões válidos, potencialmente úteis e compreensíveis em dados. Data
- Mining ou Mineração de Dados, é a etapa principal desse processo, baseando-se em técnicas estatísticas, inteligência artificial, aprendizado de máquina e outros.

- As etapas para descoberta de conhecimento são descritas:
- Compreensão do domínio: desenvolver uma compreensão do domínio (dados) e os conhecimentos prévios relevantes para identificar o objetivo do processo KDD.
- Selecionar os dados: selecionar um dataset, ou um subconjunto de variáveis ou dados de amostras no qual a descoberta é para ser realizada.
- Pré-processamento: também conhecida como etapa de limpeza, se corrige erros e inconsistências caso existam e remoção de dados com ruído.

- Redução de dados e projeção: nesta etapa se converte os dados para que possam ser reconhecidos pelo algoritmo, e reduzido o número de variáveis caso necessário, com métodos de redução ou transformação de dimensionalidade.
- Escolher o algoritmo de Mineração de Dados: inclui a seleção do método a ser usado para a busca de padrões nos dados, tais como decidir quais modelos e parâmetros mais apropriados.
- Mineração de Dados: é a parte mais importante do processo, onde os dados são aplicados a um determinado algoritmo de Mineração de Dados com a finalidade de extrair padrões de conhecimento.

- Interpretação/Avaliação dos dados: é etapa de interpretação dos padrões gerados e avaliado o retorno.
- Utilizar a descoberta de conhecimento: na última parte do processo, já é conhecido os padrões e existe a descoberta de conhecimento, então é possível a tomada de ações sobre eles, documentar ou reportar aos interessados.

- As tarefas de Data Mining são responsáveis pelas informações que serão extraídas da base de dados, para determinar qual tarefa resolver, é essencial que conheça o domínio da aplicação e o que se deseja obter. As técnicas de mineração de dados estão diretamente ligadas as tarefas que irão resolver. As principais tarefas de Data Mining são descritas Tabela.

Classificação	Descrição	Exemplos
Classificação	Consiste em construir um modelo de algum tipo que possa ser aplicado a dados não classificados visando categorizá-los em classes. Um objeto é examinado e classificado de acordo com uma classe definida.	-Classificar solicitações de pedidos de crédito. -Esclarecer fraudes na declaração do imposto de renda.
Regressão	Regressão é aprender uma função que mapeia um item de dado para uma variável de predição real estimada.	-Prever a demanda futura de um novo produto. -Estimar expectativa de vida média dos brasileiros.
Associação	Identificação de grupos de dados que apresentem concorrência entre si.	-Quais produtos são colocados juntos em carrinhos de supermercado.
Segmentação ( <i>Clustering</i> )	Processo de partição de uma população heterogênea em vários subgrupos ou grupos mais homogêneos.	-Agrupamento de clientes com comportamento de compras similar. -Comportamento de clientes em compras realizadas na web para uso futuro.
Detecção de desvios ( <i>outliers</i> )	Identificação de dados que deveriam seguir um padrão esperado, mas não o fazem.	-Detecção de intrusão em redes de computadores.

Figura 1: Principais tarefas de Data Mining

- Anomalias no tráfego em redes de computadores são comportamentos que divergem de situações normais. Intrusão (ou ataque) é um subconjunto das anomalias.
- Intrusão é qualquer ação que possa ferir a integridade, disponibilidade ou confidencialidade de recursos.

- Apesar de situações anômalas serem indesejadas, nem todas são ameaças ou ataques. Por exemplo, Loops de roteadores acontecem quando dois roteadores A e B têm acesso a uma rota R1. Imaginando que a rota de B para R1 seja perdida de alguma forma e que ainda não se tenha uma tabela de roteamento atualizada, B tentará alcançar a rota através de A. Supondo que A entenda que alcançar essa rota passando por B seja o melhor caminho, A enviará novamente os pacotes para B, que tentará novamente alcançar o destino por A e assim acontecerá um loop, onde os roteadores enviarão indefinidamente os pacotes um para o outro.



- Se não houver um apropriado Time-to-Live (TTL), que é o campo utilizado para se calcular o tempo de vida de um pacote dentro da rede, esses pacotes podem ficar por um longo tempo navegando. O Time-to-live deve então ser configurado no momento de criação do pacote. Um roteador em loop pode ser considerado uma anomalia, mas não necessariamente é proveniente de um ataque, podendo ser produto de uma topologia mal estruturada ou da queda de outro roteador, mau funcionamento do dispositivo, entre outras causas.

- Em algumas soluções de detecção de anomalias, comportamentos de usuários podem ser analisados e categorizados como anômalos ou não. Assim como outros tipos de anomalias, comportamentos anormais podem não constituir ameaças.

- Portanto, devem ser aceitos como comportamentos normais (se o problema enfrentado for o reconhecimento de ataques). A maior dificuldade nesses casos é a escolha de um bom limiar, que possa diferenciar anomalias e comportamentos normais, sem categorizar as anomalias sem importância como ataques.

- Caso a solução não seja capaz disso, pode gerar muitos falsos positivos (categorizando anomalias sem importância como ataques). Como é mostrado na Figura, a matriz de confusão do problema abordado apresenta 4 possibilidades:

		Predição		Total
		$p$	$n$	
Classe real	$p'$	Verdadeiro Positivo	Falso Negativo	$P'$
	$n'$	Falso Positivo	Verdadeiro Negativo	$N'$
Total		$P$	$N$	

Figura 2: Matriz de confusão e 4 possibilidades

- 1) Verdadeiro Positivo (VP) (True Positive), quando o classificador consegue indicar corretamente como positivo (no caso deste estudo, um ataque corretamente classificado como tal).
- 2) Falso Positivo (FP) (False Positive), quando o objeto é classificado como positivo (ataque) mas na verdade não era um.
- 3) Verdadeiro Negativo (FN) (True Negative), quando o classificador indica corretamente o objeto como tráfego normal.
- 4) Falso Negativo (VN) (False Negative), quando o classificador classifica como tráfego normal quando na verdade deveria classificar como ataque.

$$\text{Taxa de acerto} = \frac{(VP + VN)}{(VP + VN + FP + FN)}$$

$$\text{Taxa de falso alarme (FAR)} = \frac{FP}{(VN + FP)}$$

$$\text{Taxa de detecção (DR)} = \frac{VP}{(VP + FN)}$$

$$\text{Taxa de erro} = 1 - (\text{Taxa de acerto})$$

Figura 3: Fórmulas<sup>1 2</sup>

---

<sup>1</sup>As métricas mais populares são False Alarm Rate (FAR), e Detection Rate (DR). O FAR também é conhecido por False Positive Rate (FPR) e o DR é conhecido também por True Positive Rate (TPR).

<sup>2</sup>O DR é o percentual de ataques que foram detectados com base em todos os eventos e o FAR é o percentual de eventos normais que foram, erroneamente, classificados como ataques, tendo como base todos os eventos. Um IDS deve possuir alta taxa de DR e baixa de FAR, pois sistemas com altas taxas de FAR geram muitos avisos ao administrador de segurança, enquanto sistemas com baixas taxas de DR não são efetivos, gerando uma falsa sensação de segurança.

- atividade até 3 alunos;
- levantamento do estado-da-arte no contexto definido pelo grupo;
- apresentação/discussão sobre o contexto para a sala;
- proposta de artigo para desenvolvimento.
- definição das datas.