Proposta de um Mecanismo Inteligente baseado em Machine Learning e no melhor Parâmetro K no KNN para Detectar ataques Botnet em Internet das Coisas

Antonio Deivid Santos Costa[1], **Antonia Raiane Santos Araujo Cruz**[1]

[1]Instituto Federal de Educação, Ciência e Tecnologia do Ceará - campus Boa Viagem (IFCE) - Boa Viagem - CE, Brasil

Abstract. *The learning algorithms aim to optimize the performance in the execution of a given task through pattern recognition. Thus, the use of techniques such as k-Nearest-Neighbour (KNN) brings great advantages, besides being a simpler approach that can be used in applications focused on Information Security and anomaly detection. The objective of this work is to propose a mechanism that applies an Machine Learning (ML) approach based on the best value of the KNN parameter k for botnet detection in the Internet of Things.*

Resumo. *Os algoritmos de aprendizagem visam otimizar o desempenho na execução de uma determinada tarefa através de reconhecimento de padrões. Desta forma, a utilização de técnicas como k-Nearest-Neighbour (KNN) traz grandes vantagens, além de ser uma abordagem mais simples e que pode ser utilizada em aplicações voltadas para Segurança da Informação e detecção de anomalias. O objetivo deste trabalho é propor um mecanismo que aplique uma abordagem de Machine Learning (ML) baseada no melhor valor do parâmetro k do KNN para detecção de botnet em Internet das Coisas.*

1. Introdução

Por vários anos a sociedade vem acompanhando uma grande e intensa evolução computacional que vem proporcionando máquinas cada vez menores e com mais robustez. De acordo com [Kurose et al. 2007] a infraestrutura da rede tradicional possui em sua composição uma grande variedade de equipamentos, como switches e roteadores.

Todavia, com a implementaçãao do paradigma Internet das Coisas (*Internet of Things* - IoT), surge a preocupação em relação à segurança dos dados que trafegam através dos canais de comunicação gerados a partir da interconexão de objetos à rede mundial de computadores. A IoT apresenta grandes diferenças em relação as redes de computadores tradicionais, inclusive em relação a abrangência em termos de número de nós possíveis a se conectar [Atzori et al. 2010].

Estima-se que cerca de 70% dos dispositivos IoT são vulneráveis a ataques, e a grande maioria de aplicações nesse âmbito não são imposta a testes de segurança da informação [Rawlinson 2014], consequentemente, é necessário implementar mecanismos de segurança, destaca-se as ferramentas como, firewall, *Intrusion Detection System* (IDS) e métodos de segurança, como *Virtual Private Network* (VPN).

Neste trabalho, propõe-se desenvolver um mecanismo para a detecção de ataques botnet em IoT, que aplique uma abordagem de Machine Learning e baseada no algoritmo

KNN, de forma a selecionar o melhor valor do parâmetro *K* para o problema. Com a finalidade de prover maior nível de segurança para os dispositivos IoT e suas aplicações, bem como possibilitar avanços das pesquisas de sistemas de detecção de intrusões.

2. Fundamentação Teórica

Os atuais paradigmas emergem de uma realidade automatizada que está sempre buscando formas e métodos para preconizar mais facilidades, por exemplo, os paradigma Internet das Coisas e Computação em Nuvem (*Cloud Computing*).

Para tanto, conceitualmente, IoT descreve uma relação de presença difusa de uma variedade de dispositivos fısicos embarcados nomeadamente sensores e atuadores, que através de conexões e tecnologias como IEEE 802.15.4, *Bluetooth Low Energy* - BLE, WirelessHART, Z-Wave, LoRaWAn, 6LoWPAN, RPL, CoAP e *Message Queue Telemetry Transport* - MQTT [Zarpelão et al. 2017], se comunicam usando a Internet e desenvolvendo uma rede de objetos inteligentes [Atzori et al. 2010], tornado-se de grande importância em âmbito doméstico, saúde e transporte. Entretanto, o aumento do número de dispositivos conectados à Internet, que se deu de forma exponencial, reflete na necessidade de implementação de mecanismos que atendam aos requisitos de Segurança da Informação.

Em um relatório de ameaças à segurança na Internet da Symantec [Symantec 2019] é possível ter uma noção de como o surgimento de novas ameaças, que visam as vulnerabilidades dos dispositivos IoT, é preocupante. Destaca-se que, essas ameaças demonstraram maior interesse em IoT como vetor de infecção, principalmente em se falando de ataques por meio de botnets [Bertino and Islam 2017]. Esses ataques podem acarretar situações desastrosas, considerando que notadamente eles se utilizam da botnet para comandar incontáveis dispositivos de uma rede IoT na realização de ataques de Negação de Seviços Distribuído (*Distributed Denial of Service* - DDoS).

Nesse contexto, o uso de algoritmos Machine Learning (ML) otimizam o desempenho na detecção de intrusões através de reconhecimento de padrões. Os k-vizinhos mais próximos (*k-Nearest Neighbors* - KNN) é uma das técnicas ML mais simples para abordar os problemas de classificação e regressão. Segundo [Hamamoto et al. 1997] e [Alpaydin 1997] KNN produz resultados eficientes e com precisão comparável a classificadoes mais robustos e mais recentes.

3. Metodologia

A maioria das implementações determinam o melhor valor do parâmetro *K* empiricamente no processo de testes na implementação do problema, como observa-se em [Song et al. 2007] e [Yong et al. 2009]. Entretanto, essa análise torna-se inviável para uma série de problemas, principalmente em situações relacionadas às características presentes em dispositivos IoT como, número massivo de nós, heterogeneidade de dispositivos, alta mobilidade, troca de informações constante, entre outras.

Para determinar a classe de um elemento que não pertença ao conjunto de dados reconhecidamente como normal, o classicador KNN procura *K* elementos do conjunto de treinamento que estejam mais próximos deste elemento desconhecido.

Desta forma, o mecanismo implementará a abordagem KNN, utilizando um conjunto de treinamento formado por vetores *n*-dimensionais, e cada elemento deste con-

junto representa um ponto no espaço *n*-dimensional [Harrison 2012]. Assim, o aprendizado baseia-se no quão similar é um dado do outro, como detalha a equação $a(u) = argmax \sum_{i=1}^{m} [x_{i;u} = y] w(i,u)$, que determina que através de uma matriz de soma de todas as amostras e da probabilidade da classificação correta, *m* representa a probabilidade da amostra *i* ser classificada corretamente.

O classificador *k*-vizinho mais próximo geralmente é baseado na distância Euclidiana, dada por $d(p,q) = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2}$ entre uma amostra de teste e as amostras de treinamento especificadas. Entretanto, neste trabalho utilizaremos o Grid Search para identificar a melhor combinação de hiperparâmetros para os dados.

Neste cenário, propõem-se um mecanismo de detecção de ataques botnet em IoT com o uso do algoritmos KNN, aplicando uma abordagem para a definição do melhor valor do parâmetro *K*. À vista disso, o melhor parâmetro *K* será determinado a partir da aplicação de da abordagem proposta da Figura 1, que prediz o desenvolvimento de um pipeline e *k-means clustering*.

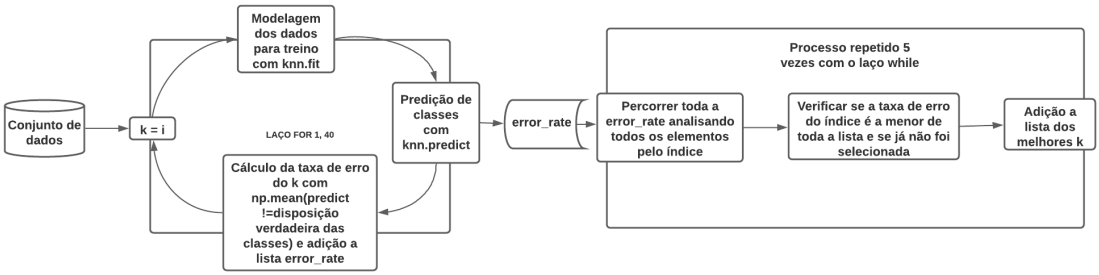

Figura 1. Visão geral da abordagem proposta.

A partir do conjunto de dados utilizado, serão extraídas características sobre o tráfego de rede, incluindo estatísticas correlativas dos dados referentes ao endereço IP, protocolo da camada de transporte, tamanho do pacote, sinalizadores (*flags*) de cabeçalho IP e outros informações coletadas. Após a extração, será realizado o pré-processamento dos dados.

Basicamente, no classificador KNN tradicional, utiliza-se um valor de K por vez. Diferentemente, na proposta, o valor vai de k = 1 a k = menor taxa erro. Então, nosso método usa a menor taxa de erro para identificar o melhor valor de k, ou seja, o que obtiver menor taxa de erro (por exemplo 1-NN, 3-NN, 5-NN, N-NN) será escolhido (Figura 2).

O mecanismo será treinado com dados normais e com ataques, onde 70% do conjunto de dados será utilizado na fase de treino e os demais 30% na fase de teste. Utilizaremos a biblioteca *Scikit-learn Machine Learning in Python* [1]. Para modelagem será utilizado o Jupyter Notebook[2].

4. Avaliação

Na perspectiva de avaliar o desempenho da metodologia proposta, bem como validar os experimentos realizados, serão utilizadas as seguintes métricas: acurácia, que é a taxa

[1]https://scikit-learn.org/stable/index.html
[2]https://jupyter.org/

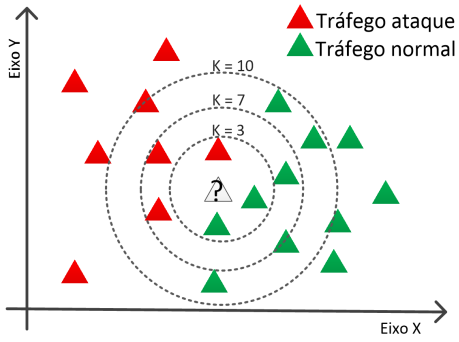

Figura 2. Funcionamento do KNN.

de classificações corretas independente da classe, dada por $\frac{TP+TN}{TP+FNz+FP+TN}$, precisão, refere-se a porcentagem de predições corretas de casos positivos dentro de determinada classe, $\frac{\mathrm{TP}}{\mathrm{TP}+FP}$ e *Recall*: eficiência do classificador em detectar as classes corretas $\frac{\mathrm{TP}}{\mathrm{TP}+FN}$. Utilizar-se-á o método de validação cruzada *K*-Fold para validação do modelo.

Agradecimentos

Os autores agradecem ao IFCE pelo apoio, através do projeto PIBIC Jr.

Referências

Alpaydin, E. (1997). Voting over multiple condensed nearest neighbors. In *Lazy learning*, pages 115–132. Springer.

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15):2787–2805.

Bertino, E. and Islam, N. (2017). Botnets and internet of things security. *Computer*, (2):76–79.

Hamamoto, Y., Uchimura, S., and Tomita, S. (1997). A bootstrap technique for nearest neighbor classifier design. *IEEE transactions on pattern analysis and Machine intelligence*, 19(1):73–79.

Harrison, O. (2012). Machine learning basics with the k-nearest neighbors algorithm.

Kurose, J. F., Ross, K. W., and Zucchi, W. L. (2007). *Redes de Computadores e a Internet: uma abordagem top-down*. Pearson Addison Wesley.

Rawlinson, K. (2014). Hp study reveals 70 percent of internet of things devices vulnerable to attack. *Hewlett Packard*.

Song, Y., Huang, J., Zhou, D., Zha, H., and Giles, C. L. (2007). Iknn: Informative k-nearest neighbor pattern classification. In *European Conference on Principles of Data Mining and Knowledge Discovery*, pages 248–264. Springer.

Symantec (2019). Istr internet security threat report. 24.

Yong, Z., Youwen, L., and Shixiong, X. (2009). An improved knn text classification algorithm based on clustering. *Journal of computers*, 4(3):230–237.

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