Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Detecção de *phishing* via redes neurais ART auto-expansíveis

Gustavo Henrique Santiago da Silva[1]
DCC/ICEx/UNIFAL-MG, Alfenas, MG
Reginaldo José da Silva[2]
FEIS/Unesp, Ilha Solteira, SP
Angela Leite Moreno[3]
DEMAT/ICEx/UNIFAL-MG, Alfenas, MG

Nas últimas décadas as aplicações *web* cresceram exponencialmente devido a crescente dependência do eletrônico. Em consequência, o fluxo de informações na internet é alta, fornecendo oportunidades a criminosos de roubar informações confidenciais e/ou pessoais. Esse ato é chamado de ataque de *Phishing* e está se tornando um dos maiores problemas de segurança da internet [1]. Em um ataque *Phishing* o infrator comunica sua vítima através de um meio de comunicação eletrônica como sites, SMS, *e-mail*, entre outros, a fim de persuadi-la a realizar ações que beneficiem a si mesmo. Esse trabalho foca em ataques *Phishing* que utilizam sites.

Visto que não há medidas que permitam evitar totalmente sites *Phishing* é importante desenvolver técnicas para sua detecção. Em geral, há duas maneiras de detectá-los: através da utilização de uma lista negra ou utilizando métodos heurísticos. A lista negra possui uma série de URL's de sites que são *Phishing* e, ao acessar um *link*, é verificado se esse não está na lista negra. Isso demanda tempo, tanto de atualização da lista negra como de investigação se um site é realmente *Phishing*, somado a isso, com as tecnologias atuais a criação de uma nova URL para um site pode ser feita rapidamente, alterando o domínio de nível superior por exemplo. Já os métodos heurísticos, baseiam-se no estudo de casos históricos de *Phishing* para a construção de um sistema que detecte novos casos. Os métodos heurísticos podem detectar sites *Phishing* em tempo real [2]. Com o avanço dos estudos de ML (*Machine Learning*), já existem muitos modelos inteligentes para resolver o problema de detecção de sites *Phishing* como no trabalho desenvolvido por Tahir *et al.*, que propuseram um modelo híbrido, combinando vários métodos de classificação, como *Naive Bayes*, *Bayes Net*, Floresta Aleatória, Árvore de Decisão e Máquina de Vetores de Suporte [6]. Já Joshua Saxe e Konstantin Berlin usaram uma rede neural convolucional (CNN) como parte de sua abordagem para automatizar a extração de recursos [5].

É nesse cenário que esse trabalho se insere, apresentando os resultados obtidos com os modelos de Redes Neurais ART Euclidiana Auto-Expansível e ART *Fuzzy* Auto-Expansível para o problema de *Phishing*, utilizando o conjunto de dados "*Phishing websites dataset*" disponível na *UCI Machine Learning Repository* [3], desenvolvido por Rami Mohammad [4].

A rede *Fuzzy* utiliza operadores lógicos *Fuzzy* e contém os parâmetros α, β e ρ. Já a rede Euclidiana baseia-se na distância Euclidiana e contém os parâmetros β e ρ. Esses, de acordo com sua variação produzem diferentes resultados de classificação. Em decorrência disso, para a construção dos modelos, usou-se a técnica de busca exaustiva para determinar quais parâmetros obtêm os melhores resultados. Os resultados dos modelos foram representados pelas métricas de

[1]gustavo.tw@hotmail.com.
[2]resisilva_mb@hotmail.com.
[3]angela.moreno@unifa-mg.edu.br

© 2021 SBMAC

validação Acurácia (ACC), Sensibilidade (Se), Especificidade (Sp), Coeficiente de Correlação de Matthews (MCC) e F-Score.

Salienta-se que, devido ao tipo de problema abordado optou-se em focar nas métricas de validação Sensibilidade e MCC, resultando em uma representatividade maior, visto que se o modelo classificar um site *Phishing* como legítimo causará danos, devendo evitar esse tipo de comportamento. A busca exaustiva para a Rede ART Euclidiana Auto-Expansível foi realizada utilizando os seguintes valores: $\beta \in \{0,1; 0,13; 0,2; 0,25; 0,30; 0,35\}$ e para o ρ foi utilizado o intervalo de 0,05 a 0,95 com saltos de 0,005. No caso da Rede ART *Fuzzy* Auto-Expansível a busca exaustiva foi realizada usando para todos os parâmetros α, β e ρ o período de 0,05 a 0,95 com saltos de 0,05. Para cada par ou grupo de parâmetros foi realizado o treinamento de um modelo, utilizando-se da técnica de validação cruzada *10-fold*. Os resultados são apresentados na Tabela 1.

Tabela 1: Resultados das Redes Neurais ART Auto-Expansíveis.

Modelo	α	β	ρ	ACC	Se	Sp	MCC	F-score
Fuzzy	0,95	0,80	0,85	**92,24%**	94,77%	89,07%	**0,8431**	0,9316
Fuzzy	0,05	0,2	0,95	86,57%	**98,06%**	72,02%	0,7405	0,7647
Euclidiana	–	0,1	0,09	**96,46%**	**97,61%**	95,02%	**0,9284**	0,9685

Ambos os modelos apresentaram resultados satisfatórios para o problema. Por outro lado a Rede ART Euclidiana Auto-Expansível apresentou uma sensibilidade alta sem perda de acurácia, o que reflete diretamente no MCC extremamente alto (0,9284), indicando que essa rede é apropriada para o problema de detecção de *Phishing*.

Referências

[1] Abdelhamid, N. *et al.* Phishing detection based associative classification data mining, *Expert Systems with Applications*, 41:5948–5959, 2014. DOI:10.1016/j.eswa.2014.03.019.

[2] Ali, W. Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection, *International Journal of Advanced Computer Science and Applications*, 8:72–78, 2017. DOI:10.14569/IJACSA.2017.080910.

[3] Dua, D. and Karra, T. E. *UCI Machine Learning Repository*: University of California, School of Information and Computer Science, 2017. Disponível em: <http://archive.ics.uci.edu/ml>.

[4] Mohammad, R. M., Thabtah, F. and McCluskey, L. Predicting phishing websites based on self-structuring neural network, *Neural Computing and Applications*, 25:443–458, 2014. DOI:10.1007/s00521-013-1490-z.

[5] Saxe, J. and Berlin, K. eXpose: A Character-Level Convolutional Neural Network with Embeddings For Detecting Malicious URLs, File Paths and Registry Keys. *CoRR*, 2017. To appear.

[6] Tahir, M. Amaad *et al.* Hybrid Model to DetectPhishing-Sites Using Supervised Learning Algorithms, *International Conference on Computational Science and Computational Intelligence (CSCI)*, 1126–1133, 2016. DOI:10.1109/CSCI.2016.0214.

© 2021 SBMAC