PROPOSTA DE UM SISTEMA WEB BASEADO NO APRENDIZADO DE MÁQUINA PARA A DETECÇÃO E MITIGAÇÃO DE ATAQUES EM REDE DEFINIDA POR SOFTWARE

Fernando Luiz Moro[1]; Alexandre Amaral[2]; Ana Paula Amaral[3]; Rodrigo R. Nogueira[4];

RESUMO

Nos últimos anos o uso de dispositivos IoT para o desenvolvimento de cidades inteligentes tem sido essencial. Todavia, a falta de segurança de tais dispositivos têm resultado no aumento do número de ataques afetando diversos setores da indústria. Para endereçar este problema, os sistemas de detecção de intrusão têm sido integrados com a rede definida por software, sendo uma alternativa para implementar soluções inteligentes que buscam preservar a segurança e disponibilidade da rede. O objetivo deste trabalho consiste em propor um sistema web baseado no aprendizado de máquina para detectar e mitigar ataques de rede gerados por dispositivos IoT no contexto da rede definida por software. Os quatro procedimentos principais do sistema serão explicados para que seja possível compreender o funcionamento da proposta.

Palavras-chave: Aprendizado de máquina. Detecção de intrusão. Rede definida por software.

INTRODUÇÃO

Em 2018, uma onda "[…] de ataques cibernéticos e violações de dados atingiram quase todos os setores da indústria [...]", sendo muitos executados por dispositivos IoT (SARANG, 2018). Um dos fatores preocupantes é que muitos deles são comprometidos para formarem grandes *botnets* com o objetivo de executar ataques DDoS (*Distributed Denial of Service*). Este tipo de ataque teve um "[...] crescimento de 29% desde o segundo trimestre de 2017, com o tamanho médio dos ataques aumentando cerca de 543% [...]" (ABRAMS, 2018). Os problemas de segurança provenientes das tecnologias IoT tem sido um desafio para garantir a confidencialidade, integridade e disponibilidade dos serviços prestados por uma

1 Cursando Bacharelado em Sistemas de Informação. Instituto Federal Catarinense – Campus Camboriú. fernandoluizmoro@gmail.com.
2 Doutor em Engenharia Elétrica. Instituto Federal Catarinense – Campus Camboriú. alexandre.amaral@ifc.edu.br.
3 Doutora em Ciência da Computação. Instituto Federal Catarinense – Campus Camboriú. ana.amaral@ifc.edu.br.
4 Mestre em Ciência da Computação. Instituto Federal Catarinense – Campus Camboriú. rodrigo.nogueira@ifc.edu.br.

cidade inteligente (CHOURABI *et al.*, 2012).

Neste contexto, a integração de uma rede definida por software (*Software Defined-Networking*) e um sistema de detecção de intrusão (*Intrusion Detection System* - IDS) automatizado baseado no aprendizado de máquina podem preservar a segurança da rede contra os ataques executados por dispositivos IoT comprometidos. Através de uma SDN, "[....] uma rede pode ser gerenciada dinamicamente, adaptativamente e remotamente" permitindo que os fluxos maliciosos sejam detectados e mitigados com agilidade (BHUNIA; GURUSAMY, 2017). Tais fatores são possíveis devido o desacoplamento do plano de controle e dados em uma SDN "[...] possibilitando que o controle da rede seja diretamente programável e a infraestrutura abstraída para aplicativos e serviços de rede" (OPEN NETWORKING FOUNDATION, 2019).

"O aprendizado de máquina é um subcampo da inteligência artificial que dá ao computador a capacidade de aprender sem ser explicitamente programado" (DAS; NENE, 2017). Devido às limitações do entendimento humano, este paradigma tem sido utilizado para obter uma melhor compreensão os dados que serão analisados. "Os métodos de aprendizado de máquina para a detecção de ataques podem ser usados para extrair automaticamente os padrões dos dados da rede, ao contrário das técnicas tradicionais baseadas em assinaturas" (NAJAFABADI *et al.*, 2015). Assim, o desenvolvimento de uma ferramenta automatizada baseada em aprendizado de máquina pode "[...] ajudar os defensores a superar determinadas lacunas, tornando-os mais eficazes na identificação e resposta a ameaças conhecidas e emergentes" (CISCO, 2018).

Este trabalho tem o objetivo de propor um sistema web baseado no aprendizado de máquina para a detecção e mitigação de ataques em rede definida por software. O administrador de rede terá a disposição um conjunto de algoritmos de aprendizado de máquina supervisionado que poderão ser treinados e executados em tempo real para o monitoramento do tráfego de rede em busca de ataques. Ao detectar um ataque o dispositivo atacante terá a comunicação automaticamente interrompida através da inserção de regras de bloqueio diretamente nos *switches* OpenFlow preservando a disponibilidade da rede e dos serviços prestados por ela. Os ataques detectados poderão ser gerenciadas através de uma *blacklist* que informará as principais características dos ataques ocorridos.

PROCEDIMENTOS METODOLÓGICOS

O desenvolvimento deste trabalho está sendo realizado no Instituto Federal Catarinense – Campus Camboriú vinculado ao projeto de pesquisa denominado redução da intervenção humana no processo de diagnóstico e solução de anomalias em redes. Inicialmente foi realizada uma pesquisa exploratória realizando o levantamento bibliográfica sobre o tema e os trabalhos relacionados nas principais bases científicas especializadas como IEEE (*Institute of Electrical and Electronics Engineers*), ACM (*Association for Computing Machinery*) e Elsevier.

Procurou-se identificar as potenciais tecnologias para a implementação do sistema e dos algoritmos de aprendizado de máquina supervisionado. Na pesquisa e testes realizados, algumas linguagens de programação como Python e Java se destacaram, por possuírem ferramentas e bibliotecas específicas para a área de inteligência artificial. Foi testada cada uma delas para avaliar qual seria a mais adequada para alcançar o objetivo deste trabalho. Posteriormente foi definido uma arquitetura de software para estruturar o projeto e facilitar a manutenção do código fonte.

RESULTADOS ESPERADOS OU PARCIAIS

O sistema web em desenvolvimento é baseado na arquitetura de software MVC (*Model-View-Controller*) e utiliza como principais tecnologias Python, Flask (*microframework)*, Scikit-learn (biblioteca), HTML, CSS e JavaScript, jQuery (biblioteca). A Figura 1 apresenta os quatro procedimentos principais do sistema responsáveis por detectar e mitigar os ataques de rede gerados por dispositivos IoT.

Figura 1 – Procedimentos do sistema.

Fonte: Autor, 2019.

Ao entrar no sistema o administrador de rede deverá realizar algumas configurações necessárias com o intuito de possibilitar o ajuste dos melhores parâmetros de acordo com o ambiente de rede monitorado. Deverão ser definidos a

base de dados para o treinamento e teste, o método de pré-processamento dos dados, os algoritmos de aprendizado de máquina que serão treinados, as características (colunas) dos fluxos IP que servirão para o aprendizado, entre outras. Com base nas pesquisas realizadas por Buczak e Guven (2016) e Das e Nene (2017) sobre as técnicas de aprendizado de máquina para a segurança cibernética, foram definidos para integrar o sistema os classificadores *Decision Tree, Random Forest, Gaussian Naive Bayes, K-Nearest Neighbors, Support Vector Machine* e *Multilayer Perceptron.*

O segundo procedimento utiliza todas as configurações definidas anteriormente para realizar o treinamento dos algoritmos de aprendizado de máquina em uma parte da base de dados e o teste em outra. Ao término, o tempo de processamento consumido durante o treinamento e teste são contabilizados e o resultado para cada um deles é apresentado de acordo com as principais métricas encontradas na literatura que são a acurácia, precisão, revocação e *f1-score* originadas da matriz de confusão. O administrador de rede com base nos dados observados selecionará o melhor modelo para ser treinado novamente, só que agora, na base de dados inteira para posteriormente realizar a detecção de ataques em tempo real.

O processo de detecção de ataques inicia-se com a execução de uma *thread* responsável por alimentar o modelo com os fluxos IP coletados e exportados pelos *switches* OpenFlow a cada 1 minuto. O modelo com base no aprendizado realizado analisará os dados em busca de um ataque de rede e caso detectado, será aberto um *socket* com a interface web do administrador para comunicar a quantidade de fluxos anômalos detectados. Em paralelo a esta ação, o sistema identifica os dispositivos envolvidos e notifica o próximo procedimento do ocorrido.

O procedimento de mitigação automaticamente envia uma regra de bloqueio nas tabelas de fluxos do *switch* OpenFlow onde o dispositivo atacante está conectado. A regra inserida interrompe a comunicação unidirecionalmente entre o atacante e a vítima preservando a disponibilidade de toda a infraestrutura de rede e serviços. Todos os ataques detectados poderão ser observados através de uma *blacklist* que conterá informações pertinentes e possibilitará em virtude de um falso alarme, excluir a regra de bloqueio para restabelecer a comunicação entre os dispositivos.

CONSIDERAÇÕES FINAIS

O sistema web proposto neste trabalho visa colaborar através da integração do aprendizado de máquina e a rede definida por software no processo de identificação e resposta às ameaças de rede geradas por dispositivos IoT. Busca-se reduzir a intervenção humana neste procedimento para que os ataques de rede sejam detectados antecipadamente e as ações de contramedida sejam executadas de forma automatizada para impedir que o controle centralizado e os serviços oferecidos pela rede fiquem indisponíveis. Foram realizados experimentos iniciais com um ataque DoS em uma rede definida por software simulada virtualmente. Os resultados obtidos foram promissores, mas o sistema ainda necessita ser aprimorado.

REFERÊNCIAS

ABRAMS, L. **Dramatic Increase of DDoS Attack Sizes Attributed to IoT Devices**. Disponível em: <https://www.bleepingcomputer.com/news/security/dramatic-increase-of-ddos-attack-sizes-attributed-to-iot-devices/>. Acesso em: 1 abr. 2019.

BHUNIA, S. S.; GURUSAMY, M. **Dynamic attack detection and mitigation in IoT using SDN**. 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). **Anais**... In: 2017 27TH ITNAC. Melbourne, VIC: IEEE, 2017.

BUCZAK, A. L.; GUVEN, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. **IEEE Communications Surveys & Tutorials**, v. 18, n. 2, p. 1153-1176, 2016.

CHOURABI, H. *et al.* **Understanding Smart Cities: An Integrative Framework**. 2012 45th Hawaii International Conference on System Sciences. **Anais**... In: 2012 45TH HICSS. Maui, HI, USA: IEEE, 2012.

CISCO. **Cisco 2018 - Annual Cybersecurity Report**. San Jose, CA: Cisco, 2018. Disponível em: <https://www.cisco.com/c/en/us/products/security/security-reports.html#~stickynav=4>.

DAS, S.; NENE, M. J. **A survey on types of machine learning techniques in intrusion prevention systems**. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). **Anais**... In: 2017 WISPNET. Chennai: IEEE, 2017.

NAJAFABADI, M. M. *et al.* **Detection of SSH Brute Force Attacks Using Aggregated Netflow Data**. 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA). **Anais**... In: 2015 IEEE 14TH ICMLA. Miami, FL, USA: IEEE, 2015.

OPEN NETWORKING FOUNDATION. **Software-Defined Networking (SDN) Definition**. Disponível em: <https://www.opennetworking.org/sdn-definition/>. Acesso em: 1 abr. 2019.

SARANG, R. **Trending: IoT Malware Attacks of 2018**. Disponível em: <https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/top-trending-iot-malware-attacks-of-2018/>. Acesso em: 1 abr. 2019.