Aplicación de Redes Neuronales Profundas para la Detección Automática de Nombres de Dominio Generados de Manera Algorítmica.

Carlos A. Catania, Jorge Guerra, Martin Marchetta, Gabriel Caffaratti,
Lucia Cortez, Alfredo Rezinovsky, Franco Palau y Juan Manuel Romero
[1] Universidad Nacional de Cuyo, Facultad de Ingeniería, LABSIN
{harpo, martin.marchetta, gabriel.caffaratti, jorge.guerra,franco.palau, alfredo.rezinovsky, lucia.cortez
juan.romero}@ingenieria.uncuyo.edu.ar

CONTEXTO

El presente proyecto se desarrolla en el marco de Facultad de Ingeniería dentro Laboratorio de sistemas inteligentes (LABSIN) de la Universidad Nacional de Cuyo. Este trabajo es parte del proyecto de investigación que dio inicio en setiembre de 2019 en el marco de los proyectos bienales de secretaria de Investigación, Internacionales y Posgrados (SIIP) de la Universidad Nacional de Cuyo.

El proyecto propone analizar la aplicación de redes neuronales profundas para el aprendizaje de los patrones comunes a los un nombre de dominio generado de manera algorítmica (DGA), de tal manera que permita desarrollar herramientas de detección, no solo con una baja tasa de falsos positivos, sino también con la capacidad de operar en tiempo real. Esto último resulta fundamental para lidiar con las amenazas de seguridad de hoy. En particular se consideró la aplicación de dos tipos de redes profundas que han probado ser adecuadas para su aplicación en cadenas de caracteres: las Long Term Support Network (LSTM) y las redes convolucionales en 1D (1D - CNN).

Durante los últimos 6 meses del proyecto se ha puesto el foco en la experimentación y evaluación de estos dos modelos para detección de DGA (Etapa 3 del proyecto). En particular se han explorado distintas alternativas en la metodología de evaluación con el fin de obtener una estimación de su capacidad de generalización

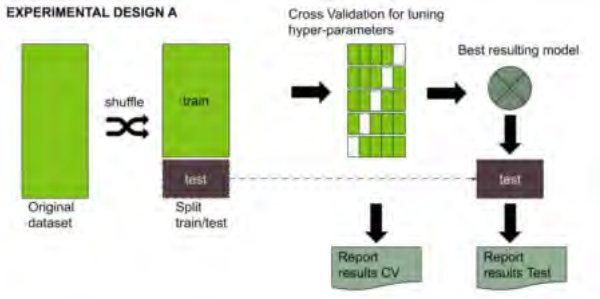

Figura 1: Metodología para la evaluación de un modelo

La estrategia común para evaluar la capacidad de generalización de un modelo consiste en separar el conjunto de datos disponible en un conjunto de entrenamiento y otro de prueba (Ver Figura 1). Si bien esta separación aleatoria del conjunto de datos es una práctica habitual, podría no ser siempre el mejor enfoque para estimar la generalización del rendimiento en algunos escenarios. El hecho es que esta metodología habitual dentro del área de aprendizaje automático puede a veces sobreestimar el error de generalización cuando un conjunto de datos no es representativo o cuando los ejemplos raros y esquivos son un aspecto fundamental del problema de detección.

.

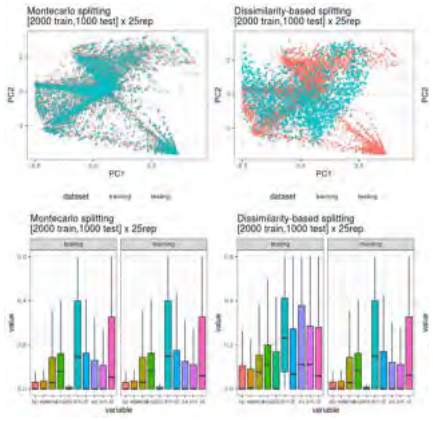

Figura 2: Dos de las técnicas de muestreo evaluadas. Montecarlo y Dissimilarity-based Splitting

LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

El proyecto se enmarca en el área de investigación sobre la aplicación de técnicas de aprendizaje automático a la seguridad informática que se lleva a cabo en el LABSIN desde 2017.

RESULTADOS OBTENIDOS

Durante esta etapa del proyecto se completaron las siguientes actividades:

a) Recopilación de información bibliográfica sobre las diferentes estrategias para muestreo de datos sobre la cual evaluar los diferentes modelos de detección.
b) Construcción de diferentes conjuntos de datos de entrada aplicando las diferentes estrategias de muestreo (Ver Figura 2)
c) Evaluación de los resultados de los diferentes modelos implementados sobre los distintos conjuntos de datos

FORMACIÓN DE RECURSOS HUMANOS

El proyecto ha permitido la capacitación en el ámbito de la investigación a profesores y alumnos interesados en participar en un entorno académico y tecnológico innovador y a todos aquellos actores interesados en los resultados del proyecto.

PUBLICACIONES:

Catania, Guerra, Romero, Caffaratti y Marchetta *"Beyond Random Split for Assessing Statistical Model Performance"* **Anales de CICCSI 2020. Congreso Internacional de Ciencias de la Computación y Sistemas de Información.** Noviembre 19 y 20 de noviembre 2020. Mendoza Argentina.