Modelado Probabilístico Basado en Aprendizaje Profundo para la Detección de Anomalías en el Tráfico de Red

Santiago Eguren[1], Carlos A. Catania[12], Jorge Guerra[2]

[1]Instituto de Investigaciones, Facultad de Informática y Diseño, U. Champagnat, Belgrano 721, 5501 Godoy Cruz, Mendoza, Argentina.

[2]Facultad de Ingeniería, Universidad Nacional de Cuyo Campus Universitario, Mendoza, Argentina.

santiago.e@live.com.ar, harpo@ingenieria.uncuyo.edu.ar, jguerra@uncu.edu.ar

RESUMEN

En la detección de intrusos en el tráfico de red pueden distinguirse dos estrategias: la detección por mal uso y la detección por anomalías. En la primera, se parte de patrones conocidos que representan el comportamiento malicioso y posteriormente se identifica a los mismos en el tráfico de red. Mientras que en la segunda, se modela el tráfico normal y luego se asume que toda instancia de tráfico que no se adapte al modelo se trata de un comportamiento malicioso. Uno de los mayores inconvenientes de la detección por mal uso es no es capaz de reconocer tipos de ataques que no se encuentran en el conjunto de patrones de ataque previamente conocidos. Por su parte la ventaja de la detección de anomalías es que son capaces de detectar nuevos ataques, sin embargo puede en muchos casos clasificar como maliciosas a instancias de tráfico normal. El presente proyecto se centra en la generación de modelos probabilísticos para la detección de anomalías en el tráfico de red. En particular, se propone analizar la utilización de un enfoque de aprendizaje de máquinas basado en redes neuronales profundas, las cuales han demostrado una gran eficacia en la detección de patrones en diversas áreas.

Palabras Claves: Seguridad de Redes, Detección de Anomalías, Aprendizaje Automático

CONTEXTO

El presente proyecto se desarrolla en el Instituto de Investigaciones de la Facultad de Informática y Diseño de la Universidad Champagnat (Godoy Cruz, Mendoza), en el marco de la Licenciatura en Sistemas de Información. Este trabajo es parte del proyecto de investigación que dio inicio en diciembre de 2017 en el marco de los proyectos bienales de investigación de la Facultad de Informática y Diseño de la Universidad Champagnat. Es importante destacar que el proyecto cuenta con la colaboración de investigadores de la facultad de ingeniería de la Universidad Nacional de Cuyo.

1 INTRODUCCIÓN

En los últimos años garantizar la seguridad de los datos en las redes de computadoras se ha transformado en un serio problema. En la actualidad un especialista en seguridad de redes debe estar alerta para detectar posibles ataques, informándose de las nuevas vulnerabilidades descubiertas o tipos de ataques perpetrados. Para dar soporte a esta

tarea se cuenta con herramientas para el análisis y detección de intrusos (IDS).

En la detección de intrusos en el tráfico de red se distinguen dos estrategias: la detección por mal uso y la detección por anomalías [1]. En la primera, se parte patrones conocidos que representan el comportamiento malicioso y posteriormente se trata de identificar a los mismos en el tráfico de red. Mientras que en la segunda, se modela el tráfico normal de red y luego se asume que toda instancia de tráfico que no se adapte al modelo puede deberse a un comportamiento malicioso.

La mayoría de los sistemas de detección de intrusos actuales se basan en detección por mal uso. Uno de los mayores inconvenientes es que no son capaces para reconocer tipos de ataques que no se encuentran en el conjunto de patrones de ataque previamente conocidos. Por su parte la ventaja de la detección de anomalías es que puede ser de gran ayuda en la detección de nuevos ataques, sin embargo presenta el inconveniente de que en muchos casos clasifica como maliciosas a instancias de tráfico normal. Lo que se conoce como falsos positivos.

De detallan a continuación los enfoques más relevantes aplicados en los últimos años al problema de la detección de intrusos en el tráfico de red [2].

Modelos basados en reglas: En este enfoque cada posible incidente de seguridad es descrito mediante una regla o firma utilizando un lenguaje específico. Posteriormente, cuando se observa en el tráfico de red alguna regla previamente especificada, se dispara una alarma. Este tipo de sistemas son los más frecuentemente utilizados en la actualidad. SNORT [3], quizás el sistema de detección más utilizado en la actualidad, sigue una estrategia de detección por mal uso aplicando un enfoque basado en reconocimiento de de reglas.

Modelos Probabilísticos: La idea detrás de estos métodos consiste en el análisis del tráfico de red y la construcción de un modelo que describa su comportamiento. La construcción del modelo normalmente se basa en ciertas métricas obtenidas a través del tiempo [6,7,8,9]. Un enfoque común para la generación de estos modelos consiste en la aplicación de técnicas de Aprendizaje de Máquinas. Dichas técnicas permiten la construcción automática de los modelos de la red a partir de lo datos previamente recopilados. Entre las muchas técnicas de aprendizaje de máquina aplicadas al problema de detección de intrusos se destaca [8,9,10,11,12,13].

El presente proyecto se centra en la generación de modelos probabilísticos para la detección de anomalías en el tráfico de red. En particular, se propone analizar la utilización de un enfoque de aprendizaje de máquinas basado en redes neuronales profundas. En particular se propone evaluar la aplicación de las redes recurrentes de tipo Long Short Term Support (LSTM) [14], las cuales han resultado adecuadas para en análisis de secuencias. Se considerarán además, las redes convolucionales multi-capa (ConvNets), las cuales han demostrado una gran eficacia en la detección de patrones en diversas áreas.

2 LÍNEAS DE INVESTIGACIÓN Y DESARROLLO.

El proyecto se enmarca en dos de las áreas de investigación del instituto de investigaciones de la universidad, en particular la Captura y procesamiento de datos a gran escala y el aprendizaje estadístico.

Para el desarrollo del presente proyecto pueden diferenciarse 3 etapas principales:

A) Análisis preliminar del problema. Las tareas asociadas a esta etapa tienen por objetivo conocimiento de los problemas asociados a la detección de anomalías como así también los modelos probabilísticos actualmente implementados. Una tarea fundamental consistirá en realización de una breve revisión de la literatura sobre la

aplicación de las técnicas de aprendizaje profundo a problemas de detección de comportamiento malicioso. Dicha tarea tiene por objetivo el de tratar de determinar cuáles han sido los beneficios e inconvenientes al aplicar este tipo de algoritmos. Finalmente como última tarea de esta primer etapa se realizará un análisis estadístico descriptivo de diversos conjuntos de datos provistos por el proyecto Stratosphere IPS a fin de analizar diversos aspectos del tráfico de red.

B) Desarrollo de un algoritmo para el reconocimiento de anomalías basado en técnicas de aprendizaje profundo. Esta etapa tiene por objetivo el desarrollo, evaluación y puesta a punto de un primer prototipo funcional para la detección de anomalías en el tráfico de red. Este primer prototipo será desarrollado utilizando alguna de las bibliotecas disponibles que permitan la implementación de modelos basados en aprendizaje profundo de manera simple y eficiente. En esta etapa se definirán los diferentes aspectos de la red como ser: el tipo de red a utilizar, la topología de la red y la secuencia de entrada entre otras. Luego se evaluarán los resultados utilizando un conjunto de datos conteniendo tráfico etiquetado (malicioso y normal).

C) Experimentación. Finalmente en la última etapa se centrará en la evaluación del algoritmo propuesto sobre distintos conjuntos de datos: En particular, se evaluará el algoritmo propuesto con diferentes conjuntos de datos previamente etiquetados. Durante este proceso se consideran las métricas habituales en el área utilizando mecanismos para validar la generalidad del modelo obtenido como validación cruzada. Durante esta etapa se realizaran también estudios comparativos con otros modelos de reconocimiento de anomalías de la literatura.

3 RESULTADOS ESPERADOS

Al término de los dos años de duración del plan de trabajo se pretende que se haya logrado:

1. Fortalecer la línea de investigación en la aplicación de modelos probabilísticos relacionados con el tráfico de red.
2. Obtener una implementación funcional del modelo probabilístico para la detección de anomalías basado en redes neuronales con aprendizaje profundo.
3. Incrementar la experiencia para la posterior aplicación de modelos probabilísticos basados en aprendizaje profundo a nuevas líneas de investigación relacionadas con problemas de ciencia y tecnología.

4 FORMACIÓN DE RECURSOS HUMANOS

Se espera capacitar 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.

Sobre la temática de este proyecto se está trabajando en:

• La tesis doctoral de Jorge Guerra, en el doctorado en Ciencias Informáticas de la Universidad Nacional del centro de la provincia de Buenos Aires.

5 BIBLIOGRAFÍA

[1] Mukherjee, B., Heberlein, L., & Levitt, K. (1994). Network intrusion detection. Network, IEEE,8, 26 –41.
[2] Sperotto, A.; Schaffrath, G.; Sadre, R.; Morariu, C.; Pras, A. & Stiller, B. An Overview of IP Flow-Based Intrusion Detection Communications Surveys Tutorials, IEEE, 2010, 12, 343 -356
[3] Wu, S. X. & Banzhaf, W. The use of

computational intelligence in intrusion detection systems: A review Applied Soft Computing, 2010, 10, 1 - 35
[4] Holland, J. Adaptation In Natural and Artificial Systems The University of Michigan Press, 1975
[5] Goldberg, D. Genetic Algorithms in search Optimization and Machine Learning. Addison Wesley,1989
[6] Lakhina, A.; Crovella, M. & Diot, C. Diagnosing network-wide traffic anomalies SIGCOMM Comput. Commun. Rev., ACM, 2004, 34, 219-230
[7] Stoecklin, M. P.; Le Boudec, J.-Y. & Kind, A. A two-layered anomaly detection technique based on multi-modal flow behavior models Proceedings of the 9th international conference on Passive and active network measurement, Springer-Verlag, 2008, 212-221
[8] Mahoney, M. & Chan, P. Learning rules for anomaly detection of hostile network traffic Data Mining, 2003.ICDM 2003. Third IEEE International Conference on, 2003, 601 - 604
[9] Livadas, C.; Walsh, R.; Lapsley, D. & Strayer, W. Using Machine Learning Techniques to Identify Botnet Traffic Local Computer Networks, Proceedings 2006 31st IEEE Conference on, 2006, 967 -974
[10] C. Catania and C. G. Garino, "Una propuesta de reconocimiento de patrones en el tráfico de red basada en algoritmos genéticos," in ninth Argentinian Symposium on Artificial Intelligence, ASAI, D. Godoy and A. Maguitman, Eds., 2007, pp. 174–185.
[11] Catania, C.; Bromberg, F. & Garcia Garino, C. Bromberg, F. & Verdun, L. (Eds.) An autonomous labeling approach to SVM algorithms for network traffic anomaly detection Proceedings of ASAI 2009 Argentine Symposium on Artificial Intelligence, 2009, 144-15. ISSN 1850-2784.
[12] Catania C., Bromberg F. y García Garino C. "Detección de intrusos en el tráfico de red Mediante Máquinas de Vectores Soporte". En los anales de V EnIDI. Encuentro de Investigadores y Docentes de Ingeniería. San Rafael, 2009. pp. 168-182. ISBN 978-950-42-0087-1.
[13] Catania C., Bromberg F. y García Garino C. "An Autonomous Labeling approach to Support Vector Machines Algorithms for Network Traffic Anomaly Detection". Expert Systems with Applications. Elsevier.DOI:10.1016/j.eswa.2011.08.068
[14] Pablo Torres, Carlos Catania, Sebastian Garcia, and Carlos Garcia Garino "An Analysis of Recurrent Neural Networks for Botnet Behavior Detection". Congreso Bienal de IEEE Argentina (ArgenCon), 2016. Buenos Aires. Argentina.