Comparación de las Redes Neuronales SOM y GG en los Sistemas de Detección de Intrusos de Red

Francisco J. Mora Gimeno, Francisco Maciá Pérez y Diego Marcos Jorquera

Departamento de Tecnología Informática y Computación, Universidad de Alicante
Carretera San Vicente - Alicante s/n
03690, San Vicente (Alicante), España
{fjmora, pmacia, dmarcos}@dtic.ua.es

Abstract. El uso de redes neuronales en los sistemas de detección de intrusos se ha incrementado significativamente en los últimos años. En este artículo, presentamos los resultados de comparar la red neuronal Rejilla Creciente y los Mapas Auto-Organizativos aplicadas a los sistemas de detección de intrusos. Se comparan dos aspectos muy importantes, el rendimiento y el tiempo de entrenamiento. Los resultados muestran que la red creciente mejora el rendimiento del sistema en la detección de anomalías obteniendo mejor relación entre el ratio de detección y el número de falsos positivos. Por otra parte, se consigue una reducción del tiempo de entrenamiento muy significativa en entornos reales, donde aparecen nuevos ataques que es necesario detectar. Las redes se han entrenado y testeado con los datos de evaluación de sistemas de detección de intrusos DARPA 1999.

1 Introducción

Los sistemas de detección de intrusos (IDS) constituyen un elemento fundamental en la infraestructura de comunicaciones de las empresas. Junto a los cortafuegos, los IDS representan la principal herramienta de seguridad de la red: los primeros para las amenazas externas y los segundos tanto para las externas como para las internas a la organización. Aunque durante un tiempo los cortafuegos fueron utilizados como único mecanismo para la protección de los datos, en realidad sólo reducen la exposición del sistema, por lo que es importante tener un sistema de monitorización y detección [1].

El principal desafío de los sistemas de detección de intrusos actuales es que sean capaces de detectar ataques nuevos a partir de otros observados previamente. En este contexto, se ha incrementado el uso de las redes neuronales artificiales debido a su habilidad para generalizar y reconocer patrones nuevos a partir del entrenamiento previo. Perceptrones Multi-Capa con algoritmo de BackPropagation (MPL), Funciones de Base Radial (RBF) y Mapas de características Auto-Organizativos (SOM) han sido las redes neuronales más utilizadas en los IDS. De ellas, la red SOM tiene la ventaja de necesitar menor tiempo de entrenamiento por tratarse de una red no supervisada.

En estos modelos la topología de la red debe de ser decidida por adelantado, antes de la fase de entrenamiento. Esto es un inconveniente debido a que la elección de la topología apropiada sólo se puede realizar teniendo en cuenta propiedades estadísticas de los datos inferidas durante la fase de entrenamiento [2]. El rendimiento del sistema dependerá de la estructura de la red, la elección a priori de la estructura restringe los mapas resultantes y la exactitud de la salida. Otro inconveniente es que la capacidad de la red está predefinida por el número de nodos y parámetros de aprendizaje, provocando que sea inapropiada para el aprendizaje continuo. Este aspecto resulta fundamental si se quiere aplicar las redes neuronales en entornos reales. En la práctica, para reducir este efecto, se entrenan varias redes de este tipo con distintas topologías, posteriormente se elige la que muestre mejor rendimiento con los datos de validación.

A priori, una red neuronal creciente como Growing Grid (GG) presenta algunas ventajas sobre una red SOM [3]. La estructura de la red y el tamaño no tienen que decidirse por adelantado en la red GG, por lo que la red modificará y adaptará su estructura según los datos de entrada en la fase de entrenamiento. La red GG sólo utiliza parámetros constantes, por lo que es capaz de continuar el aprendizaje de forma indefinida, o bien detenerlo en un punto y continuar desde el mismo en cualquier momento; en la red SOM los parámetros decrecen con el tiempo, por lo que cuando alcanzan el mínimo ya no existe más capacidad de aprendizaje.

Con el objetivo de aprovechar las ventajas citadas en el párrafo anterior, en este artículo presentamos un IDS basado en la red neuronal GG y su comparación con otro basado en la red SOM. Los sistemas se han validado con los datos de evaluación de detección de intrusos DARPA. Mostramos como la red GG mejora los resultados obtenidos por la red SOM, tanto en rendimiento conseguido como en tiempo de entrenamiento empleado.

2 Trabajos Relacionados

Algunos de los primeros trabajos que han utilizado IDS basados en redes neuronales lo han hecho tanto para detectar abusos como para detectar anomalías, además han sido sistemas orientados a procesos, donde la red neuronal MPL generalmente modela el comportamiento normal del proceso en función de sus llamadas al sistema. La misma red neuronal se ha combinado con métodos estadísticos para trabajar de forma conjunta en la detección abusos y anomalías con el objetivo de combatir los defectos de cada método en un único sistema. La red MPL también se ha empleado en sistemas de detección de abusos del tráfico de red, mediante el análisis de distintos campos de las cabeceras de los paquetes e intentando, al mismo tiempo, clasificar los ataques. Con el objetivo de reducir el alto ratio de falsas alarmas se diseñó un sistema para detectar abusos basado en la red MPL, pero en este caso en lugar de analizar los paquetes de forma aislada se estudiaban sesiones completas [4].

En los estudios realizados para comparar el rendimiento de la red MPL y RBF, los resultados muestran que la red RBF mejora el rendimiento de los IDS en la detección de anomalías, obteniendo mayor ratio de detección y menor índice de falsos positivos y necesitando, además, menos tiempo de entrenamiento [5]. El trabajo que se presenta

en este artículo sigue el mismo enfoque, pero comparando la utilización de dos redes neuronales con entrenamiento no supervisado. La red neuronal RBF se ha usado como base de dos IDS jerárquicos, uno serie y otro paralelo, clasificando cada ataque en el serie y los distintos tipos en el paralelo, permitiendo a la red seguir entrenado en tiempo de ejecución.

La red neuronal SOM también se ha utilizado en el campo de la detección de intrusos: en [6] se presenta un sistema de detección de abusos que combina SOM con MPL. Han sido empleadas múltiples SOM integradas en un mismo sistema para modelar y monitorizar el perfil de los datos de red de las distintas capas de la pila de protocolos TCP/IP. Esta misma red ha formado parte de sistemas de detección para la clusterización y visualización de los datos, en este caso también se ha combinado con Resilient Propagation Algorithm (RPROP) para la detección. El algoritmo SOM se ha implementado para clusterizar el contenido de los paquetes de red en un sistema de detección de dos etapas que usa en la segunda etapa un algoritmo de detección de anomalías tradicional. En este caso la detección se lleva a cabo tanto a nivel de paquete como a nivel de sesión [7]. Otra aplicación de esta red neuronal en los IDS ha sido la integración de múltiples SOM para construir perfiles de comportamiento de las sesiones de los usuarios dentro de un sistema de detección basado en host.

En [8] se presenta un sistema de detección de anomalías a nivel de conexiones de red, donde cada conexión se define con las siguientes seis características: duración de la conexión, tipo de protocolo, tipo de servicio, estado de la conexión, bytes origen y bytes destino. Este sistema se ha validado con el conjunto de datos de detección de intrusos DARPA 1998. En [9] se muestra la utilidad de la red neuronal SOM aplicada en los IDS para detectar anomalías en las conexiones de red caracterizando cada conexión con seis parámetros estadísticos, pero en este caso distintos de los anteriores. Otra diferencia entre estos dos trabajos es que el primero se aplica a todo el tráfico de red, mientras que el segundo construye una red neuronal por cada servicio de red. El trabajo que se presenta en este artículo sigue un planteamiento muy similar a estos dos sistemas, pero modelando cada conexión de red con diferentes parámetros y utilizando la red neuronal GG como motor de detección del sistema.

3 Propuesta Basada en la Red Neuronal GG

En la presente propuesta se ha diseñado un IDS que utiliza como motor de detección la red neuronal GG, el sistema recibe como entrada los paquetes de red obtenidos de la interfaz del sistema. Nuestro IDS detecta ataques a nivel de conexión, por lo que es necesario definir los parámetros que van a caracterizar cada conexión y que constituyen la entrada a la red neuronal. En nuestro caso se han usado las cinco características siguientes:

- DOC, duración de la conexión.
- SRC, es el número de bytes enviados desde el cliente al servidor.
- DST, número de bytes enviados desde el servidor al cliente.

- SPA, promedio de paquetes enviados por segundo desde el cliente.
- DPA, promedio de paquetes enviados por segundo desde el servidor.

Para obtener estos datos es necesario preprocesar los paquetes de entrada. Primero, y dado que en nuestro sistema se va a construir una red neuronal por cada servicio, se filtrarán los datos para obtener solamente aquellos paquetes que estén dirigidos al servicio correspondiente, en nuestro caso se han utilizados filtros *tcpdump*. Segundo, se obtienen los parámetros que caracterizan cada conexión, para lo cual se ha implementado un módulo con el fin de ir leyendo todos los paquetes que forman las distintas conexiones, construir la conexión entera y, después, calcular las variables estadísticas de entrada. Finalmente, con el fin de que uno de los cinco parámetros no predomine sobre los restantes por tener valores de distintas dimensiones, es necesario normalizar los parámetros de entrada. Se ha elegido una normalización de varianza, de forma que cada dimensión de los vectores de entrada tenga una varianza de uno. Este proceso de normalización se lleva a cabo en el módulo de normalización, teniendo en cuenta la media y la desviación típica de cada dimensión calculadas en módulo anterior. En la figura 1 se puede observar la arquitectura del sistema.

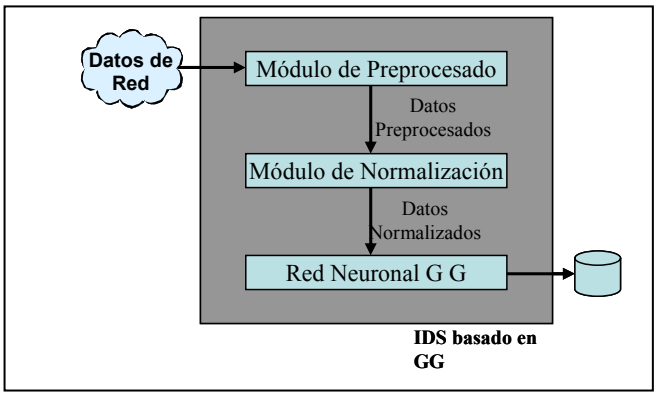

Fig. 1. Arquitectura del sistema

Los vectores de cinco componentes obtenidos en el módulo de normalización serán la entrada a la red neuronal GG. La red neuronal clasificará cada conexión en normal o anómala, almacenando el resultado en una base de datos para su análisis posterior y lanzando una alarma en el caso de que la conexión sea anómala.

La red GG es una red neuronal rectangular creciente que inicia el entrenamiento con un número de neuronas mínimo y que cada N iteraciones del algoritmo añade una fila o columna a la estructura hasta alcanzar una cantidad de neuronas determinada o cualquier criterio de finalización definido por el programador. Las filas o columnas se añaden en función de los datos de entrenamiento, por lo que la estructura final de la red depende de estos datos y no de una elección previa.

4 Experimentos

Con el fin de evaluar nuestra propuesta, en esta sección mostramos la comparación de los resultados experimentales de la aplicación de la red GG y la red SOM en el entrenamiento y detección de ataques de trafico Web, es decir, se ha desarrollado un IDS orientado a servicio en el que las redes se han entrenado con tráfico HTTP y son capaces de reconocer ataques a este servicio. La comparación de los resultados se ha llevado a cabo en función de dos aspectos: el tiempo de entrenamiento y el rendimiento.

Los datos utilizados para el entrenamiento y prueba de las redes neuronales implementadas han sido el conjunto de datos de evaluación de IDS DARPA 1999. Estos datos están formados por todas las conexiones que tuvieron lugar en una red simulada durante cinco semanas, tres semanas con datos para el entrenamiento de sistemas de detección y dos semanas con datos para la evaluación de los sistemas. De las semanas correspondientes a los datos de entrenamiento se han seleccionado aleatoriamente 10.000 conexiones que constituirán los patrones de entrenamiento de las redes.

La elección de la topología de la red neuronal SOM se ha llevado a cabo calculando los dos eigenvectores de la matriz de autocorrelación de los datos de entrenamiento que tienen los eigenvalores más grandes, la relación entre las dimensiones de la red se obtiene teniendo en cuenta la relación entre estos dos eigenvalores y considerando el número de patrones en los datos de entrenamiento [10]. Siguiendo estos criterios se ha seleccionado una SOM de dimensiones 18 x 28, con inicialización lineal dentro del rango de los patrones de entrenamiento y con función de vecindad Gaussiana.

Después de obtener las dimensiones de la red SOM debemos seleccionar el tamaño de la red GG. Con el objetivo de que ambas tengan el mismo nivel de detalle a la hora de preservar la topología, se ha decidido que la red tenga el mismo número de neuronas que la SOM. En general, una red sólo puede preservar completamente la topología si la dimensión del mapa coincide con la dimensión del espacio de entrada [3]. Las dimensiones de la red no se pueden conocer a priori, ya que es el propio algoritmo el que partiendo de cuatro nodos y en base a los datos de entrenamiento, va creciendo hasta establecer las dimensiones del mapa. Al igual que en la red SOM, la función de vecindad será Gaussiana.

Finalmente, para la validación de las redes después de la fase de entrenamiento se han utilizado los mismos datos de nuevo, y se ha calculado la distancia de cada patrón a la neurona vencedora. Las redes son validadas si al menos el 95% de los vectores de los patrones de entrada tienen una distancia con respecto a los vectores de las neuronas vencedoras menor que dos desviaciones típicas [9], esta heurística asume que los datos de entrada siguen una distribución Gaussiana.

Para que los resultados sean directamente comparables se han empleado los valores de los parámetros de las redes recomendados por sus autores [2, 10]. En la red GG los parámetros fundamentales utilizados han sido: paso de adaptación medio en la fase de crecimiento 30, ratio de aprendizaje constante de 0.1, parámetro de vecindad constante de 0.9 y pasos de adaptación en fase final 100. Los parámetros básicos de la red SOM han sido: ratio aprendizaje inicial 0.9 decreciente, vecindad inicial elevada

y decreciente para una mejor ordenación y el número de iteraciones de aprendizaje han sido un mínimo de 500 veces el número de neuronas.

4.1 Tiempo de Entrenamiento

Si se pretende utilizar las redes neuronales en escenarios realistas es necesario que estos sistemas se adapten a una realidad cambiante, es decir, continuamente aparecen nuevos ataques que los sistemas de detección necesitan reconocer. En este sentido, en un IDS basado en redes neuronales, es necesario adaptar las redes entrenándolas de nuevo. Igual que, en un IDS basado en reglas, cuando aparecen nuevos ataques, se añaden en la base de datos del sistema de detección las reglas necesarias para reconocer los ataques nuevos.

Una importante propiedad de la red GG para adaptarse a los nuevos ataques es que puede continuar el entrenamiento desde el mismo punto en el que lo hizo el anterior, gracias a que los parámetros son constantes, por lo que la red sólo tendrá que entrenarse con los nuevos patrones. Por el contrario, la red SOM utiliza parámetros variables que decrecen con cada iteración hasta llegar a un mínimo, indicando que el aprendizaje de la red está finalizado. Para que la red SOM aprenda los nuevos patrones de ataques, es necesario repetir el proceso de aprendizaje desde el inicio, añadiendo a los patrones ya existentes los nuevos.

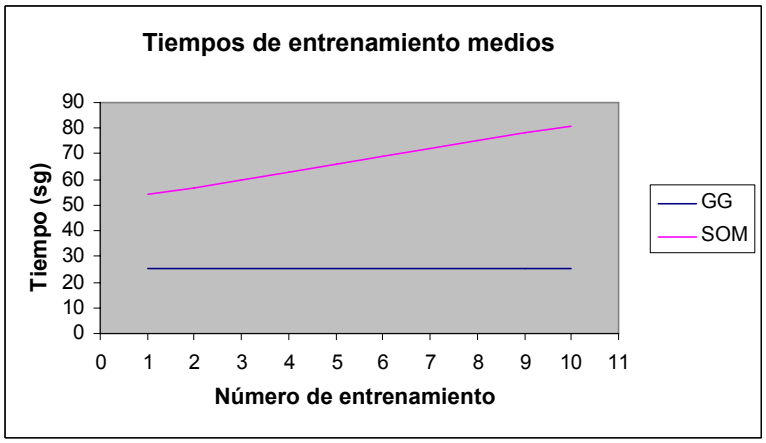

Fig. 2. Comparación de los tiempos de entrenamiento de nuevos patrones

Teniendo en cuenta lo expresado en el párrafo anterior, las pruebas se han orientado a evaluar el tiempo de entrenamiento que necesitan las dos redes para adaptarse a los nuevos patrones de ataques que aparecen continuamente. Como se puede observar en la Fig. 2, el tiempo necesario en la red GG es constante, mientras que el tiempo en los mapas auto-organizativos crece linealmente con el número de patrones nuevos que necesita aprender. El hecho de que la red GG presente un tiempo de entrenamiento

adicional constante añade a los sistemas basados en esta red la característica de escalabilidad.

4.2 Rendimiento

El rendimiento en los sistemas de detección de intrusos se suele medir tanto desde el punto de vista de la habilidad de detección como del ratio de falsos positivos. Utilizando curvas Receiver Operating Characteristic (ROC) podemos comparar estas dos magnitudes con el fin de extraer conclusiones válidas acerca de, por ejemplo, el número de falsos positivos producidos a partir de una capacidad dada o para observar el volumen de falsas alarmas alcanzado con una detección del 100%.

En la Fig. 3 se aprecia claramente que para una detección del 80%, la red GG sólo produce un falso positivo al día, mientras que el mapa SOM provoca tres falsas alarmas, lo cual implica una reducción de 66%. También es significativo el hecho de que para el 100% de detección, la red SOM se equivoca en once falsos positivos al día, mientras que la red GG lo hace en seis ocasiones, mejorando el resultado en un 45%.

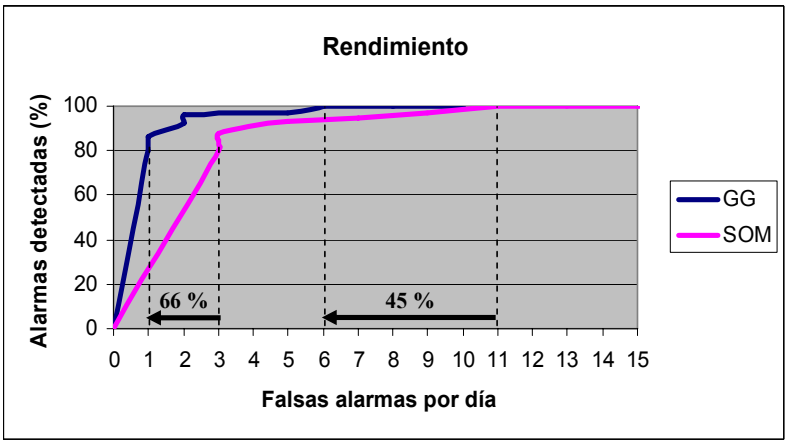

Fig. 3. Comparación del rendimiento

Podemos observar que la red GG obtiene una clasificación mejor que la SOM, para el mismo índice de detección siempre comete menos falsos positivos, posiblemente debido a que para establecer su estructura tiene en cuenta los datos de entrenamiento del problema concreto y no una decisión a priori. Además, mejora el tiempo de entrenamiento en entornos reales pasando de un incremento de tiempo lineal a uno constante.

5 Conclusiones

En este trabajo se ha presentado la aplicación de la red neuronal creciente GG en el campo de los IDS y los resultados muestran la viabilidad del enfoque. Esta red se ha comparado con la red SOM, muy utilizada en este tipo de aplicaciones. La comparativa demuestra que el tiempo de entrenamiento en entornos reales de la red GG es menor que el tiempo de la SOM, siendo constante en la primera y lineal creciente en la segunda. No sólo es menor, sino que es constante, lo que facilita la escalabilidad del sistema. Además, el rendimiento de la primera red es siempre mejor que la segunda obteniendo menor número de falsos positivos para el mismo ratio de detección. La reducción de falsas alarmas va desde el 66% para una detección del 80% hasta el 45% para una detección del 100%.

Como trabajo futuro, estamos estudiando la utilización de redes neuronales crecientes como Grow When Required (GWR) [3], donde la topología no está restringida a redes bidimensionales rectangulares, capaces de adaptarse a datos de entrenamiento dinámicos presentes en el campo de los sistemas de detección de intrusos.

Referencias

1. C. Zhang, J. Jiang and M. Kamel, “Intrusion detection using hierarchical neural net-works”, Pattern Recognition Letters, vol. 26, pp. 779-791, May 2005
2. B. Fritzke, “Growing Grid – a self-organizing network with constant neighbourhood range and adaptation strength”, Neural Processing Letters, vol. 2, pp. 9-13, 1995
3. S. Marsland, J. Shapiro and U. Nehmzow, “A self-organizing network that grows when required”, Neural Networks, vol. 15, pp. 1041-1058, 2002
4. R. Lippmann and R. Cunningham, “Improving intrusion detection performance using keyworkd selection and neural networks”, Computer Networks, vol 34, pp. 597-603, 2000
5. C. Zhang, J. Jiang and M. Kamel, “Comparison of BPL and RBF Network in Intrusion Detection System”, LNAI 2639, pp. 466-470, 2003
6. J. Cannady and J. Mahaffey, “The application of artificial intelligence to misuse detection”, Proceedings of the 1st RAID conference, 1998
7. S. Zanero and S. Savaresi, “Unsupervised learning techniques for an intrusion detection system”, Proceedings of the ACM SAC 2004, Nicosia, Ciprus, March 2004
8. P. Lichodzijewski, A. Zincir-Heywood and M. Heywood, “Dynamic intrusion detection using self-organizing maps”, Proceedings of the 14th CITSS 2002, May 2002
9. M. Ramadas, S. Ostermann and B. Tjaden, “Detecting anomalous network traffic with self-organizing maps”, Proceedings of the RAID 2003, LNCS 2820, pp. 36-54, September 2003
10. T. Kohonen, “Self-organizing maps”, Springer, third edition, 2001