Chapter 3

Estado de la Cuestión

Resulta fundamental analizar el estado actual de las soluciones existentes frente a la creciente amenaza que suponen las botnets en los entornos del Internet de las Cosas. Esta revisión permite identificar las técnicas actualmente empleadas, así como los logros alcanzados y las posibles limitaciones aun existentes, especialmente en lo referente al despliegue y al uso de modelos más avanzados de aprendizaje automático.

El objetivo de esta sección es aportar contexto al trabajo desarrollado dentro del panoráma de investigaciones recientes en el ámbito, identificando las aproximaciones relevantes y las posibilidades aún no abordadas. Esta base comparativa servirá como punto de partida para argumentar la necesidad de la solución planteada posteriormente. En particular, el artículo *Foggier skies, clearer clouds*, constituye el referente principal sobre el que se articula esta propuesta, siendo complementado y ampliado con nuevos modelos, arquitectura modular y una comparativa en detalle de los resultados de diferentes modelos.

3.1 Revisión de soluciones para detección de botnets en IoT

Se abordará el estado del arte siguiendo el proceso natural de una solución de detección de botnets en redes IoT desde la selección de datasets hasta la comparativa de resultados de evaluación de modelos, haciendo hincapié tanto en las decisiones tomadas por otros autores como en las áreas abiertas que se dejan sin investigar.

3.1.1 Datasets

Existe cierto consenso en el campo de la detección de botnets mediante aprendizaje automático respecto a la importancia de emplear datasets directamente tomados de entornos IoT reales o lo más parecido posible a ellos pues de esta forma se consiguen datos abundantes y de gran calidad, impactando directamente en los resultados del modelo, como se menciona en Nazir et al. (2023). La diversidad, considerada en el ya citado artículo, también tiene una importancia crítica en la consecución de objetivos. Existen diversos tipos de ataque que una botnet puede realizar, habiendo presentado ya algunos de ellos en el capítulo previo. Por tanto, si quiere realizarse un modelo lo más completo posible (entendiendo completitud como la capacidad para detectar una botnet presente en la red independientemente del tipo de ataque que esta realice) es importante entrenar el modelo con datasets que incluyan ataques diferentes. No obstante, puede seleccionarse un solo tipo de ataque y especializar el servicio en su detección, como es el caso de Snehi et al.

(2024) y los ataques de denegación de servicio.

En la mayoría de los casos se realiza una selección de 4 o 5 datasets relevantes y ampliamente aceptados en el ámbito de la detección de botnets en redes IoT. Entre estos conjuntos de datos destacan los siguientes:

- **Aposemat IoT-23**, un extenso dataset obtenido de dispositivos IoT reales en la Universidad Técnica Checa que incluye diversos tipos de ataque en ficheros log obtenidos mediante Bro (actualmente Zeek).
- El dataset **Bot-Iot** de la Universidad de Nueva Gales del Sur (UNSW). Similar al anterior en la diversidad de registros de ataques que proporciona pero su formato es CSV y no logs.
- **N-BaIoT**, creado por investigadores de la Ben-Gurion University, incluye tráfico de red de dispositivos IoT infectados por malware como Mirai y BASHLITE. Está disponible como ficheros CSV.
- **TON_IoT** es un dataset creado también por la Universidad de Nueva Gales del Sur con tráfico de diversos dispositivos IoT como puertas y sistemas de iluminación automatizados.

Pese a la existencia y el uso de muchos otros datasets se ha decidido resaltar estos 4 al ser aquellos sobre los que se trabajará en el presente trabajo. Para realizar evaluaciones completas y robustas de los modelos es conveniente realizar, por ejemplo, mezcla de datasets para entrenar y predecir sobre ellos o realizar predicciones en un dataset con un modelo entrenado con otro conjunto de datos. Esto busca abordar una de las principales dificultades en el IoT que es su heterogeneidad, cuantas más situaciones se hayan probado en el modelo más alta será su fidelidad.

3.1.2 Preprocesamiento, EDA y Selección de Características

El siguiente paso natural sería el preprocesamiento de los datos y la realización de un análisis exploratorio. Sin embargo, este aspecto es muchas veces obviado por completo o infravalorado excepto la extracción de la importancia de las características (como ocurre en Snehi et al. (2024)). En este trabajo se ha decidido dar una mayor relevancia y profundidad a este apartado, realizando, además de un análisis de correlaciones y relevancias, otro tipo de estudios como detección y visualización de outliers o análisis de series temporales.

En *Foggier skies, clearer clouds* se realiza ingeniería de características en base a la correlación de Pearson entre las mismas, eliminando así aquellas que no aportan información nueva relevante, y se seleccionan las de mayor significancia empleando ANOVA. Se ha decidido hacer uso de esta técnica también, añadiendo la información obtenida en un Feature Importances de un Random Forest para proporcionar mayor respaldo a la decisión final.