Detección de Botnets en Redes IoT Utilizando Técnicas de Aprendizaje Automático
Botnet Detection in IoT Networks Using Machine Learning Techniques

Trabajo de Fin de Máster
Curso 2024–2025

Autor
Joel Gómez Santos

Director
Pablo Cerro Cañizares

Colaborador
Colaborador no definido. Usa `\colaboradorPortada`

Máster en Internet de las Cosas
Facultad de Informática
Universidad Complutense de Madrid

Detección de Botnets en Redes IoT Utilizando Técnicas de Aprendizaje Automático
Botnet Detection in IoT Networks Using Machine Learning Techniques

Trabajo de Fin de Máster en Internet de las Cosas
Departamento de Sistemas Informáticos y Computación

Autor
Joel Gómez Santos

Director
Pablo Cerro Cañizares

Colaborador
Colaborador no definido. Usa `\colaboradorPortada`

Convocatoria: *Febrero/Junio/Septiembre 2025*
Calificación: *Nota*

Máster en Internet de las Cosas
Facultad de Informática
Universidad Complutense de Madrid

February 16, 2025

Dedicatoria

A Pedro Pablo y Marco Antonio, por crear TeXiS
e iluminar nuestro camino

Agradecimientos

A Guillermo, por el tiempo empleado en hacer estas plantillas. A Adrián, Enrique y Nacho, por sus comentarios para mejorar lo que hicimos. Y a Narciso, a quien no le ha hecho falta el Anillo Único para coordinarnos a todos.

Resumen

Detección de Botnets en Redes IoT Utilizando Técnicas de Aprendizaje Automático

Un resumen en castellano de media página, incluyendo el título en castellano. A continuación, se escribirá una lista de no más de 10 palabras clave.

Palabras clave

Máximo 10 palabras clave separadas por comas

Abstract

Botnet Detection in IoT Networks Using Machine Learning Techniques

An abstract in English, half a page long, including the title in English. Below, a list with no more than 10 keywords.

Keywords

10 keywords max., separated by commas.

Contents

List of figures

List of tables

Chapter 1

Introducción

"Frase célebre dicha por alguien inteligente"
— Autor

En los últimos años, los avances en el ámbito del Internet de las Cosas y la rápida proliferación de dispositivos IoT han traído consigo importantes mejoras en la conectividad, permitiendo la automatización y el monitoreo en contextos que van desde el hogar hasta la industria.

Sin embargo, la propia idiosincrasia del Internet de las Cosas, en su heterogeneidad, lo hace un objetivo ideal para los ataques con redes de bots (*Botnets*). Es en este contexto donde aparece el aprendizaje automático como herramienta para la detección de estas amenazas.

En este trabajo se estudiarán e implementarán diferentes modelos de aprendizaje automático para comprobar cuáles de ellos son los más apropiados para detectar los distintos tipos de posibles *botnets*.

1.1 Motivación

Mirai, *Perisai* o *Matrix* son solo algunas de las *botnets* que han protagonizado recientemente noticias por su infiltración y ataque en redes IoT.

Los avances tecnológicos de la última década no solo mejoran las vidas de los ciudadanos, también permiten que estos ataques sean cada vez más complejos. Los métodos tradicionales para hacerles frente quedan obsoletos y se presenta la necesidad de desarrollar sistemas más inteligentes para poder hacer frente a esta amenaza, el aprendizaje automático.

1.2 Objetivos

El presente trabajo tiene como objetivo principal diseñar y evaluar diferentes sistemas de detección de *botnets* en redes IoT haciendo uso de técnicas de aprendizaje automático.

Además, se busca discutir las ventajas y limitaciones de los enfoques propuestos para poder determinar los casos de uso más apropiados de cada uno de ellos. Como último objetivo, se quiere presentar un resumen de algunas de las técnicas de implementación de contramedidas frente a las *botnets* detectadas.

1.3 Plan de trabajo

Para conseguir los objetivos anteriormente mencionados se empleará el siguiente proceso de trabajo.

Chapter 2

Estado de la Cuestión

En esta sección se presentará el estado actual de la detección de *botnets* en redes IoT. Para ello, se comienza introduciendo dos conceptos fundamentales, por un lado el de Redes de Bots y, por otro el de Aprendizaje Automático.

Una vez habiendo sentado estas bases se procederá a analizar la situación actual del campo de la detección de este tipo de redes maliciosas empleando técnicas de Aprendizaje Automático.

2.1 Conceptos Fundamentales

Para una correcta comprensión del presente trabajo es crucial que el lector esté familiarizado tanto con las *botnets* como con el aprendizaje automático.

2.1.1 Botnets: Una Amenaza en Auge

Considérese una red de dispositivos IoT. Se denomina *botnet* a una subred de dichos dispositivos que se encuentran controlados remotamente por un usuario externo denominado *"Botmaster"*.

Estos aparatos, al pertenecer a la red IoT original, son empleados por su nuevo dueño para realizar ataques o acciones maliciosas en perjuicio de la red y/o en beneficio del *"Botmaster"*. Entre los ataques más habituales pueden encontrarse:

- **Ataque de Denegación de Servicio (DDOS):** En un ataque de este tipo los dispositivos "infectados" buscan imposibilitar a la víctima su uso del servicio (por ejemplo, su conexión a Internet). Para ello se dedican a enviar una gran cantidad de paquetes inutiles a través de la red buscando congestionarla hasta que no pueda abarcar la gestión de tantos mensajes y deje de poder funcionar correctamente.
  Ejemplo IoT: Una red de dispositivos IoT de monitorización de cabezas de ganado por ejemplo podría ser víctima de un ataque de este tipo. En este caso, el *"Botmaster"* podría inundar el servidor que controla las reses con mensajes de posición hasta que colapsara. De esta forma este no sería capaz de detectar, por ejemplo, la desaparición o rapto de un animal.

- **Robo de Información/Espionaje:** En este caso los dispositivos controlados formarían parte de alguna red de recolección de información (por ejemplo sensores o cámaras en un hogar inteligente) y el ataque consistiría en desviar la información recogida para poder, por ejemplo, chantajear al dueño original.

- **Minado de Criptomonedas (Cryptojacking):** Este tipo de ataque, de gran interés desde el auge de Bitcoin en la última década, consiste en emplear los dispositivos de la víctima para minar cryptomonedas sin su conocimiento.

Las redes IoT, compuestas normalmente por muy diversos y muy alejados dispositivos, son un objetivo especialmente vulnerable ante este tipo de ataques.

2.1.2 Mirai: Crisis de Denegación de Servicio

Es a finales de 2016 cuando comienzan a sucederse ataques de Denegación de Servicio que inutilizaron algunas grandes compañías tecnológicas como la francesa OVH o la estadounidense DynDNS.

Creada en sus inicios por un grupo de 3 jóvenes estadounidenses la Red de Bots Mirai fue utilizada por diversos hackers después de que su código fuente fuera publicado en varios foros de Internet.

Mirai buscaba realizar un Ataque de Denegación de Servicio y, para ello, se valía de Ataques de Fuerza Bruta para adivinar claves de dispositivos IoT que, muchas veces, eran aquellas que el fabricante creó por defecto con poco grado de complejidad. Una vez se había logrado apoderar del dispositivo usaba su nueva red de bots para saturar los servidores mediante la generación masiva de tráfico.

Entre los tipos de ataques DDOS que se realizaban destacan:

- **SYN flood:** Este ataque consiste en iniciar rápidamente conexiones al servidor sin llegar a finalizarlas, obligando a este a destinar recursos en esperar a estas conexiones parciales. Impidiendo así el tráfico legítimo.

- **ACK flood:** En este caso se activa el *flag* ACK en una gran cantidad de *requests* de forma que el envío de las mismas y su recepción colapsa el servidor.

- **UDP flood:** En este ataque el servidor recibirá una gran cantidad de paquetes UDP a puertos aleatorios, lo cual obligará al servidor a gestionarlos y, generalmente, responder con paquetes ICMP informando de que no hay ninguna aplicación escuchando en dicho puerto. Esta gran cantidad de paquetes desborda la capacidad del servidor.

- **HTTP flood:** En un ataque HTTP flood los *bots* envían solicitudes HTTP (generalmente GET o POST) para lograr que el servidor tenga que dedicar sus recursos a gestionar dicho ataque.

El ataque de Mirai puso de manifiesto la vulnerabilidad de las redes IoT y los peligros que este nuevo paradigma traía consigo si se descuidaba la seguridad.

2.1.3 Aprendizaje Automático: Detectando lo Indetectable

Chapter 3

Descripción del Trabajo

Aquí comienza la descripción del trabajo realizado. Se deben incluir tantos capítulos como sea necesario para describir de la manera más completa posible el trabajo que se ha llevado a cabo. Como muestra la figura 3.1, está todo por hacer.

Figure 3.1: Ejemplo de imagen

Si te sirve de utilidad, puedes incluir tablas para mostrar resultados, tal como se ve en la tabla 3.1.

Col 1	**Col 2**	**Col 3**
3	3.01	3.50
6	2.12	4.40
1	3.79	5.00
2	4.88	5.30
4	3.50	2.90
5	7.40	4.70

Table 3.1: Tabla de ejemplo

Chapter 4

Conclusiones y Trabajo Futuro

Conclusiones del trabajo y líneas de trabajo futuro.

Antes de la entrega de actas de cada convocatoria, en el plazo que se indica en el calendario de los trabajos de fin de máster, el estudiante entregará en el Campus Virtual la versión final de la memoria en PDF. En la portada de la misma deberán figurar, como se ha señalado anteriormente, la convocatoria y la calificación obtenida. Asimismo, el estudiante también entregará todo el material que tenga concedido en préstamo a lo largo del curso.

Chapter 5

Introduction

Introduction to the subject area. This chapter contains the translation of Chapter 1.

Chapter 6

Conclusions and Future Work

Conclusions and future lines of work. This chapter contains the translation of Chapter 4.

Appendix A

Título del Apéndice A

Contenido del apéndice

Appendix B

Título del Apéndice B

Este texto se puede encontrar en el fichero Cascaras/fin.tex. Si deseas eliminarlo, basta con comentar la línea correspondiente al final del fichero TFMTeXiS.tex.

–¿Qué te parece desto, Sancho? – Dijo Don Quijote –
Bien podrán los encantadores quitarme la ventura,
pero el esfuerzo y el ánimo, será imposible.

Segunda parte del Ingenioso Caballero
Don Quijote de la Mancha
Miguel de Cervantes

–Buena está – dijo Sancho –; fírmela vuestra merced.
–No es menester firmarla – dijo Don Quijote–,
sino solamente poner mi rúbrica.

Primera parte del Ingenioso Caballero
Don Quijote de la Mancha
Miguel de Cervantes