Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Alicia Mayor Bal
presenta el resumen del trabajo

Detección de ataques en entornos IoT mediante técnicas de canal lateral y de Inteligencia Artificial

Felipe Lemus Prieto, Javier Sánchez Rivero, Carlos Castañares Cañas, Andrés Caro Lindo, José-Luis González-Sánchez

Actas VIII JNIC, atlanTTic, 299-305, (2023).

19 de marzo de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Ciberataques, IoT, Securización, Técnicas side-channel.

Introducción

El crecimiento experimentado por el Internet de las Cosas desde su nacimiento en 2009 en sectores tan variados como salud, hostelería o logística, ha supuesto que en el año 2022 se estimara el uso de unos 16.000 millones de dispositivos IoT. Sin embargo, su securización no ha avanzado en consonancia, por lo que es necesario desarrollar técnicas de ciberseguridad que disminuyan el riesgo de ataques.

Este estudio aborda esta problemática basándose en técnicas side-channel, detectando ataques o anomalías supervisando el consumo energético de los dispositivos IoT y analizándolo mediante técnicas de aprendizaje automático.

1. Metodología

Se diseña un **dataset propio**.

El **sistema hardware** usado es simple, flexible y escalable: tres Raspberry Pi 3 Model B como dispositivos IoT con comportamientos distintos entre ellos, un medidor de energía INA 3221 y una Raspberry Pi 4 Model B como dispositivo maestro que realiza lecturas con frecuencia de 10Hz, guardando en un fichero csv la intensidad en mA de cada dispositivo, la fecha y la hora. La comunicación se realiza mediante el protocolo de comunicaciones i2c.

Se utilizan tres **tipos de ataques**: intrusión, minado y keylogger. Su ejecución genera un fichero csv que almacena el tipo, dispositivo afectado, fecha y hora.

Los **datos** en bruto obtenidos se **preprocesan** para extraer características. Al trabajar con un aprendizaje supervisado, el primer paso es el etiquetado, que distingue acciones de dispositivos y ataques. A continuación se crea una ventana temporal, que permite que las trazas de datos pasen de tener una única característica (intensidad) a un número definido de caracterísitcas, lo cual implica algoritmos de machine learning más precisos.

Para realizar la **detección de ataques** se llevan a cabo dos fases: detección y clasificación.

La elección de **algoritmos de clasificación** tiene como objetivos la sencillez, rapidez y ligereza. Para el dataset generado, los modelos basados en árbol ofrecen menor intensidad computacional que técnicas de deep learning, por lo que los algoritmos elegidos son el Random Forest y el Extreme Gradient Boosting Trees.

2. Resultados

Para la evaluación de precisión, las métricas se establecen en función de True Positive, True Negative, False Negative y False Positive, usando como métrica de rendimiento la F1 score.

Para la **mejor combinación** de parámetros de ventana se obtienen valores de precisión de un **99,21 %** en Random Forest y un **99,05 %** en Extreme Gradient Boosting. Cabe destacar también que el modelo con peor rendimiento tiene una puntuación F1 score de 98,01 %.

Tras generar matrices de confusión, se contempla que los modelos apenas cometen errores al identificar ataques keylogger, mientras que los que generan más problemas son los de intrusión.

3. Discusión/Conclusiones

La proliferación de dispositivos IoT hace necesario garantizar su seguridad. El sistema de detección de intrusiones propuesto en este paper arroja luz a esta necesidad. Tiene en cuenta las limitaciones de estos

dispositivos y a pesar de su sencillez alcanza valores de precisión del 99,21 %. Además, este sistema cuenta con la ventaja de poder desplegarse en los dispositivos IoT finales, lo cual permite una mayor capilaridad y escalabilidad del sistema.

4. Valoración del documento original

El paper explica de forma clara la contribución del estudio a una necesidad real, siendo esta el crecimiento del IoT pero no de su securización. La metodología está desgranada de una forma que aporta sencillez a la hora de entender el proceso entero que se ha seguido para obtener los resultados finales, sin expandirse en cosas que carecen de relevancia. Además, las conclusiones reflejan claramente que el estudio iguala o supera otras propuestas más complejas.