espol Facultad de Ciencias Naturales y Matemáticas

Tomás Guijo
tguijo@espol.edu.ec

Gabriel Villanueva
gabstvil@espol.edu.ec

Desarrollo de un sistema inteligente IDS/IPS/IRS usando ML en una infraestructura IoT para agricultura de precisión.

PROBLEMA

Los pequeños y medianos agricultores ecuatorianos necesitan utilizar soluciones de Internet de las cosas para conocer a detalles los factores ambientales que influyen en sus cultivos para poder aumentar la utilidad de sus cultivos disminuyendo costos operacionales.

OBJETIVO GENERAL

Implementar una red inteligente que detecte, prevenga y restringa el acceso a los usuarios dentro de un sistema de agricultura de precisión mediante el uso de Software y Hardware que permita conocer factores importantes como temperatura, humedad y presión.

PROPUESTA

Crear un módulo que bloque el tráfico malicioso, detectado de forma inteligente, para mitigar un ataque de red.

Automatizar la actualización de los datos que serán utilizados por el modelo de aprendizaje automático, para detectar anomalías en las mediciones realizadas por los sensores.

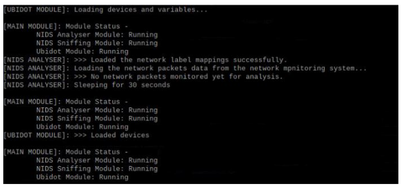
Implementar una conexión inalámbrica por medio del protocolo Zigbee para la comunicación de los dispositivos de la red.

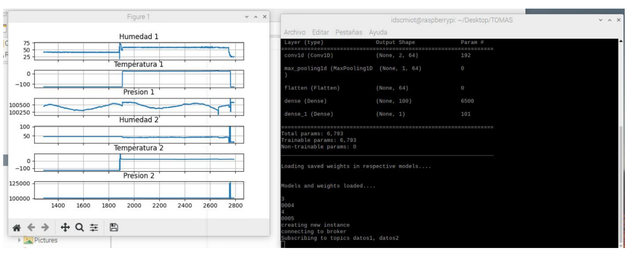
RESULTADOS

La implementación de un sistema IDS/IPS permite la detección inteligente y la toma de decisiones contra ataques en la red; sin embargo, no es capaz de parar el ataque, si no mitigar el mismo y reducir el alcance que pueda provocar.

El proceso de automatización para la actualización de datos permite que el modelo para la detección de anomalías trabaje con información actual, sin embargo los datos obtenidos en el proceso automático no son validados por lo que podría introducirse datos aberrantes que afecten al modelo.

La implementación de Zigbee es capaz de cubrir más terreno que el protocolo Wi-Fi. Sin embargo, en trabajos futuros se puede implementar LoRaWan para aumentar la distancia entre los dispositivos.





CONCLUSIONES

- El aprendizaje automático permite ayudarnos a predecir los ataques a la red y tomar las acciones pertinentes ante los mismos.
- Debido al tráfico de datos recopilados es posible crear reglas para filtrar el tráfico peligroso.
- Se concluyó que al utilizar los sistemas propuestos es posible mitigar ataques a dispositivos IoT.
- Se determinó que con el uso de los módulos es posible cubrir una gran área para la conexión inalámbrica