Sistema Inteligente de Detección de Anomalías para IoT

Bolatti Diego, Karanik Marcelo, Todt Carolina, Scappini Reinaldo, Gramajo Sergio

Universidad Tecnológica Nacional, Facultad Regional Resistencia
Departamento de Ingeniería en Sistemas de Información
Centro de Investigación Aplicada en Tecnologías de la Información y la Comunicación (CInApTIC)
French 414 – Resistencia (3500) Chaco - Argentina
{diegobolatti, mkaranik, carolinatodt, rscappini, sergiogramajo}@gmail.com

RESUMEN

En los últimos años, con el avance de Internet de las Cosas (IoT), ha aumentado la cantidad de dispositivos conectados a la red y, consecuentemente, el incremento de los riesgos de violaciones de seguridad y ataques maliciosos. Estadísticamente la mayoría de estos ataques se producen en los dispositivos finales de IoT y existen múltiples alternativas detectarlos. En ese contexto, este proyecto tiene como objetivo el diseño de un Sistema Inteligente de Detección de Anomalías para IoT que utilice técnicas de Machine Learning (ML). Específicamente, el proyecto abarca el diseño y desarrollo de un sistema capaz de detectar ataques de seguridad en base a anomalías en los dispositivos finales de IoT, aplicando técnicas de aprendizaje automático que provean el mecanismo adecuado para dicha detección.

Palabras Clave: Internet de las cosas, Detección de anomalías, Machine Learning, Seguridad.

CONTEXTO

Este trabajo de investigación se desarrolla en el marco del proyecto "Análisis y Aplicaciones de Internet de las Cosas y Ciudades Inteligentes basadas en Telecomunicaciones y Seguridad" (Código del Proyecto: CCUTIRE0005353TC) del Centro de Investigación Aplicada en TICS (CInApTIC) de la Universidad Tecnológica Nacional, Facultad Regional Resistencia.

1. INTRODUCCIÓN

Actualmente el Internet de las cosas (IoT) vive una gran expansión, y se ha convertido en una tendencia irreversible, que se refleja en la conexión diaria a internet de miles de dispositivos y sensores los cuales obtienen y distribuyen información a través de la Web. Los ámbitos en los que se utiliza IoT son variados y van desde la agricultura [1], la salud [2], la hotelería [3], el monitoreo de tráfico [4] y la gestión de flotas [5] entre otros.

Debido a la gran diversidad de dispositivos, tecnologías y protocolos de comunicación (Lora, Zigbee, Wifi, etc.) es un gran desafío gestionar la seguridad de un ecosistema IoT. Sumado a esto, la mayoría de los dispositivos de IoT no se diseñan pensando en la seguridad, y muchos de ellos no poseen capacidades esenciales de encriptación y autenticación. Lo que ha llevado a una categoría completamente nueva de ataques dirigidos explícitamente a los dispositivos finales.

En definitiva, sin un buen nivel de protección, los usuarios no pueden adoptar muchas aplicaciones de IoT que son útiles para el desarrollo de sus actividades.

Debido a estos motivos, se propone el desarrollo de un sistema inteligente de detección de anomalías que permita detectar de forma automática actividades anormales que comprometan la integridad, la confidencialidad y la disponibilidad de un entorno de IoT.

Una anomalía es un comportamiento inusual, irregular y no habitual en el siste-

ma que puede indicar un ataque de seguridad o una falsa alarma.

Entre las anomalías que el sistema inteligente de detección de anomalías podrá detectar se encuentran:

- **Denegación de servicio (DoS):** En este tipo de ataque se envía una gran cantidad de paquetes para inundar un objetivo y hacer que sus servicios no estén disponibles para otros servicios [6].
- **Tipo de dato incorrecto:** En este tipo de anomalía, un dispositivo de IoT malicioso escribe un tipo de dato diferente del tipo de dato previsto [6].
- **Agotamiento de batería:** Ataque que intenta agotar las baterías de los dispositivos de IoT para dejarlos fuera de servicio [7].
- **Jamming:** Este tipo de ataque es una variante de los ataques DoS y consiste en desactivar o saturar los recursos del sistema consumiendo toda la memoria o enviando una gran cantidad de tráfico a la red para que nadie más pueda utilizarla [8].
- **Retraso de Paquetes:** Las transmisiones de datos válidos se retrasan maliciosamente, pero, a diferencia de los ataques de reenvío selectivo, no se eliminan. Por lo tanto, el ataque provoca un retraso en la entrega de datos y, en consecuencia, una degradación del rendimiento de la red.
- **Alteración de paquetes:** Estos ataques intentan alterar el contenido de un paquete enviado por el dispositivo para inyectar datos maliciosos en los nodos de la red.
- **Man In The Middle (Ataque de Intermediario):** Estos ataques se realizan para espiar la comunicación de red de los dispositivos y modificar el tráfico de la red para realizar ataques de inyección y reproducción [9].

Para detectar de forma automática e inteligente las anomalías, se propone la utilización de técnicas de Machine Learning (ML). ML es una rama de la Inteligencia Artificial (IA), que a través de algoritmos proporciona a los sistemas la habilidad de identificar patrones entre los datos para hacer predicciones [10].

Para utilizar el aprendizaje automático o ML se necesita una gran cantidad de muestras de datos de entrada correctamente etiquetadas para entrenar al módulo de ML.

Sin embargo, incluso cuando un algoritmo de ML ha recibido una gran cantidad de datos, aún no hay garantía de que pueda identificar correctamente las nuevas anomalías. Por lo tanto, se requiere constantemente la experiencia y el control del ser humano.

El mismo problema surge si el algoritmo solo usa sus propios datos de salida como entradas para un mayor aprendizaje. Los errores se refuerzan y multiplican, ya que los mismos resultados incorrectos vuelven a ingresar a la solución en un bucle y crean más falsos positivos ("FP": categorizar incorrectamente las muestras limpias como maliciosas) y falsos negativos (marcar las muestras maliciosas como benignas).

Por esa razón se propone diseñar un detector de anomalías híbrido que combine las técnicas de detección:

- **Basadas en reglas:** Las anomalías se detectan en base a reglas definidas por expertos en seguridad y son ideales para detectar anomalías conocidas.
- **Basadas en ML:** Las anomalías se detectan con la ayuda de técnicas de aprendizaje automático.

La propuesta es que el detector de anomalías esté basado en redes definidas por software (SDN) y se ubique en la capa de dispositivo de la arquitectura de IoT, tal como se muestra en la Figura 1.

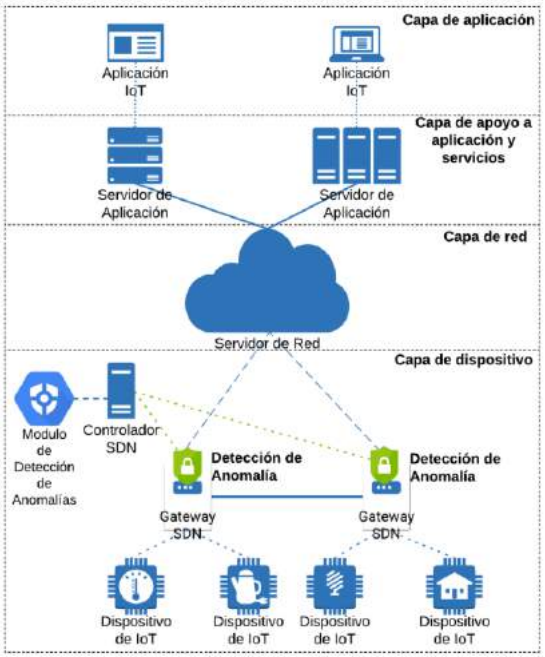

Figura 1: Arquitectura Propuesta.

En la Figura 1 se puede apreciar que el sistema está compuesto por:

- **Dispositivos finales de IoT**: de poca capacidad de procesamiento, como sensores de temperatura, luces inteligentes, entre otros.
- **Gateway SDN:** permiten que los dispositivos de IoT se conecten a la red. Para la conectividad entre los dispositivos finales y los Gateway se utilizan redes de baja potencia y área amplia (LPWAN) como LoRa, Sigfox, entre otros [11].
  Además, el gateway cuenta con un interruptor de flujo abierto para monitorear el tráfico proveniente de los dispositivos finales.
- **Controlador SDN:** este componente administra y configura los recursos de la red.
- **Módulo de detección de anomalías:** este módulo recopila los datos de las puertas de enlace para así buscar anomalías.
  El rol de este módulo es agregar inteligencia al controlador SDN para reajustar la red y mantener las políticas de seguridad definidas por los administradores al detectar anomalías.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Las líneas de investigación que se abordan en el proyecto están vinculadas con:

- **Arquitectura de redes de información para IoT:** Para el diseño del detector de anomalías se estudiarán las arquitecturas de redes de IoT .
- **Redes definidas por software:** Se investigará esta tecnología emergente con el objetivo de aplicar las ventajas de la misma, en el desarrollo del sistema.
- **Virtualización de redes:** Se utilizará herramientas de simulación y virtualización de dispositivos, para generar escenarios de pruebas y probar el sistema.
- **Inteligencia Artificial:** Se realizará un análisis de las técnicas de ML, con el objetivo de seleccionar la mejor opción para la implementación en el módulo de detección de anomalías.
- **Tecnologías LPWAN:** Se estudiarán la tecnología LPWAN, con el objetivo de identificar las características de los paquetes de datos que ayuden a detectar anomalías en los dispositivos finales de IoT.
- **Seguridad de IoT:** Se analizarán los ataques de seguridad y anomalías que se presentan en un entorno de IoT.

3. RESULTADOS OBTENIDOS/ESPERADOS

Este proyecto, se centra en el diseño de un sistema de detección de anomalías, capaz de detectar ataques de seguridad en dispositivos finales de IoT.
Específicamente se pretende:

1. Estudiar las diferentes opciones de seguridad para un entorno de IoT.

2. Evaluar los últimos desarrollos e investigaciones de detección de anomalías realizados para un entorno de IoT.
3. Diseñar un prototipo de un detector de anomalías para IoT.
4. Documentar las características, arquitectura, ventajas y desventajas del sistema diseñado.
5. Evaluar el alcance de la solución y su viabilidad.

4. FORMACIÓN DE RECURSOS HUMANOS

Con el proyecto se pretende contribuir a la formación de recursos humanos desde diversas áreas:

- **Formación de becarios:** El proyecto cuenta con la participación de alumnos becarios del último año de la carrera de Ingeniería en Sistemas de Información que están realizando su práctica supervisada.
- **Alumnos de la carrera de Ingeniería en Sistemas de Información:** Se prevé realizar actividades de actualización y talleres con alumnos de las cátedras del área de redes de información, comunicaciones y seguridad informática. Además, por las propias características de los temas que involucra el proyecto se pueden realizar actividades en cátedras como inteligencia artificial.
- **Formación de jóvenes profesionales:** Se prevé la incorporación de jóvenes profesionales de Ingeniería en Sistemas de Información con la intención de seguir con una carrera en investigación universitaria. Los cuales pueden incorporarse en carácter ad-honorem al proyecto o a través de becas de iniciación en la investigación.
- **Formación de postgrado:** A partir de las líneas de investigación desarrolladas en el proyecto se prevé que el Ing. Diego Bolatti finalice su doctorado mediante una tesis vinculada a este proyecto.
- **Equipo de trabajo:**
  - **Director:**
    - Gramajo, Sergio.
  - **Investigadores de apoyo:**
    - Bolatti, Diego
    - Scappini, Reinaldo
    - Karanik, Diego
  - **Becario alumno:**
    - Todt, Carolina
    - Federico Aguirre

5. BIBLIOGRAFÍA

[1]. Agriculturers.com Red de Especialistas en Agricultura. (2019). *Aplicaciones de IoT en agricultura*. El texto puede consultarse en la siguiente URL: http://agriculturers.com/aplicaciones-de-iot-en- agricultura/

[2]. Dostie, R. (2019). *El Internet de las Cosas (IoT) en el área de la salud en 2019*. Everything Rad. El texto puede consultarse en la siguiente URL: https://www.carestream.com/blog/2019/01/01/el internet-de-las-cosas-iot-en-el-area-de- la-salud-en-2019/.

[3]. Sanz Baños, B. (2019). *IoT en los hoteles - Think Big Empresas*. Think Big. El texto puede consultarse en la siguiente URL: https://empresas.blogthinkbig.com/iot-en-los hoteles/.

[4]. Fracttal.com. (2019). *Las 9 aplicaciones más importantes del Internet de las Cosas (IoT)*. El texto puede consultarse en la siguiente URL: https://www.fracttal.com/blog/2018/10/10/9 aplicaciones- importantes-iot.

[5]. Wireless, K. (2019). *Soluciones de IoT para la gestión de flotas*. Mx.korewireless.com. El texto puede consultarse en la siguiente URL: https://mx.korewireless.com/industries/iot-fleet- management-solutions.

[6]. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). *Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches*. Internet of Things, 7, 100059.

[7]. Smith, Ryan et al. *Battery Draining Attacks Against Edge Computing Nodes in*

IoT Networks. Cyber-Physical Systems 6.2 (2020): 96–116. Crossref. Web.
[8]. Font, V. G. (2017). *Anomaly detection in smart city wireless sensor networks* (Doctoral dissertation, Universitat Oberta de Catalunya).
[9]. Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). *A supervised intrusion detection system for smart home IoT devices*. IEEE Internet of Things Journal, 6(5), 9042-9053.
[10]. Sen, P. C., Hajra, M., & Ghosh, M. (2020). Supervised classification algorithms in machine learning: A survey and review. In Emerging technology in modelling and graphics (pp. 99-111). Springer, Singapore.
[11]. Y.4101/Y.2067 (10/17). *Common requirements and capabilities of a gateway for Internet of things applications*. El texto puede consultarse en la siguiente URL: https://www.itu.int/rec/T-REC-Y.4101-201710-I/en.