Análisis y Aplicaciones de Internet de las Cosas y Ciudades Inteligentes. Escenario de Testeo de Seguridad

Gramajo Sergio, Scappini Reinaldo, Bolatti Diego, Todt Carolina

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
{sergiogramajo, rscappini, diegobolatti, carolinatodt}@gmail.com

RESUMEN

El rápido desarrollo de las nuevas tecnologías de Internet de las Cosas (IoT) como sus usos en diferentes campos de la industria, las ciudades, la salud, los hogares, entre otros, ha planteado nuevas formas de enfrentar amenazas de seguridad. IoT es una colección de dispositivos interconectados fortalecido con pequeños procesadores, placas o interfaces de red que se comunican con servicios web u otro tipo de interfaces a través de diferentes medios de telecomunicación.

Naturalmente si una nueva tecnología es ampliamente adoptada por el público y hay una notoria falta de estándares para el campo, las amenazas de ciberseguridad crecen.

En esta etapa del proyecto nos centramos en generar un escenario para realizar un relevamiento de los diferentes tipos de tráfico y crear un posterior datasets de análisis para poder identificar diferentes amenazas en sistemas IoT industriales o corporativos.

Palabras Clave: Internet de las cosas, Ciudades Inteligentes, Framework.

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" del Centro de Investigación Aplicada en TICS (CInApTIC) de la Universidad Tecnológica Nacional, Facultad Regional Resistencia.

1. INTRODUCCIÓN

Como hemos mencionado, actualmente el Internet de las cosas (IoT) vive una gran expansión [1] y fue el resultado de la evolución sistemática de las telecomunicaciones y la electrónica de sensores [2] [3] acompañada con la demanda de la sociedad y dispositivos con mínima intervención humana [4]. En este contexto de intercomunicación, los sistemas pueden enviar información y tomar decisiones [5]. Para ello deben hacerlo en un ecosistema seguro y confiable y hoy existe un creciente número de amenazas de ciberseguridad para ellos [6].

Es así que, en este punto del proyecto de investigación se está desplegando un escenario de testeo (monitor) que pueda ser modelo para detectar tráfico anómalo y clasificar oportunamente amenazas o tráfico normal.

El diseño del monitor de tráfico se creó a partir de un bridge y un contenedor Docker con un software de captura tcpdump. Esta captura se realiza en modo "raw" obteniendo la totalidad de los paquetes de una determinada interfaz del puente al cual se conecta el contenedor monitor, sin privilegios elevados, solo un contenedor

convencional. El puente al reflejar todo el tráfico de la interfaz elegida permite además que múltiples herramientas obtengan los mismos datos, siendo esto de gran utilidad si por ejemplo se desea establecer funciones de selección y discriminación de tráfico, siendo éste un requisito fundamental para el desarrollo del proyecto.

Cabe destacar que el uso de docker facilita un entorno aislado y fácilmente replicable que asegura la portabilidad e implementación del monitor allí donde haga falta.

Las etapas que se están llevando a cabo para la creación del escenario son las siguientes:

1. Configuración de conexión VPN a la red de la UTN FRRe en terminales Wndows10 y Ubuntu 20.04.
2. Inspección y verificación de la MV que da soporte al Gateway LORA y donde residen los servicios implementados en el ámbito del proyecto.
3. Instalación vía SSH del software requerido para el desarrollo de las actividades de investigación (soporte NetworManagerCLI, Docker, OpenVswitch, y otros).
4. Copiar los contenedores necesarios.
5. Montaje de escenario de pruebas
6. Ajuste del diseño desarrollado y probado
7. Rediseño conforme el contexto y soporte de la plataforma de la MV UTI CINAPTIC.

La propuesta final es que el detector de anomalías esté basado en redes definidas por software (SDN) [7] y se ubique en la capa de dispositivo de la arquitectura de IoT, tal como se muestra en la Figura 1.

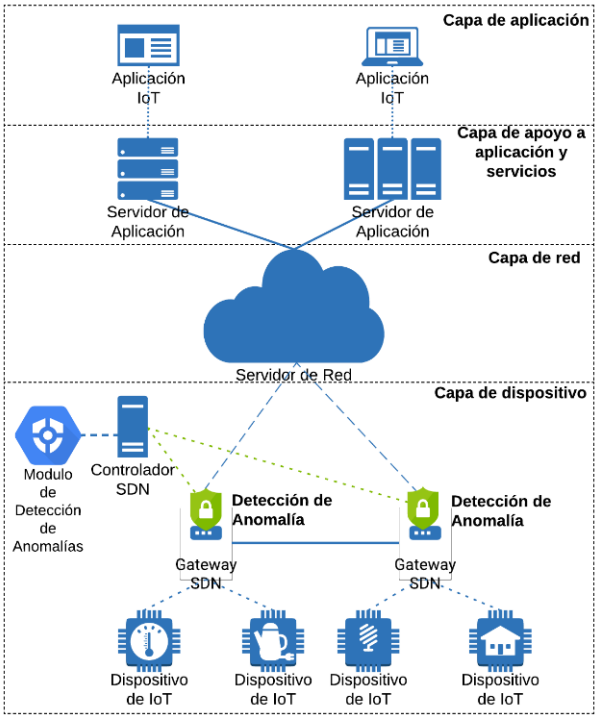

Figura 1: Arquitectura Propuesta.

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.
  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:

- **Frameworks genérico de captación y presentación de datos:** Consiste en el desarrollo del framework que pueda ser adaptado a diferentes situaciones del medio local.
- **Arquitectura de redes de información para IoT:** Para el diseño de un detector de anomalías sobre IoT.
- **Inteligencia Artificial:** Se realizará un análisis de las técnicas de Machine Learning, con el objetivo de seleccionar la mejor opción para la implementación en el módulo de detección de anomalías.
- **Seguridad de IoT:** Se analizarán los ataques de seguridad y anomalías que se presentan en un entorno de IoT.

3. RESULTADOS OBTENIDOS/ESPERADOS

Los resultados obtenidos en el proyecto podrán ser utilizados en las siguientes áreas del conocimiento:

A) Arquitecturas de redes de Información para IoT. El relevamiento y análisis de las nuevas tendencias de redes de información de corto y amplio rango, conllevará a publicaciones científicas y transferencias al medio local o regional. Esto propiciará el contacto con investigadores de nivel internacional y nacional de otras instituciones para posibles intercambios de experiencias como el que se está llevando a cabo con el proyecto REMIND de la Unión Europea[1].

B) Programación y pruebas de diversos dispositivos usados para IoT y ciudades inteligentes como sensores y equipos de telecomunicación entre ellos sin intervención humana y que ayude a la toma de decisiones y mejore la gestión que lo utilice.

Una vez finalizado el proyecto generará nuevo conocimiento y aplicaciones que pueden ser transferidos tanto a entornos de investigación como diferentes entornos organizacionales o empresas del medio. En este sentido se pretende impulsar el intercambio de conocimiento con investigadores de otras instituciones, asistencia a eventos científicos, elaboración de publicaciones científicas, estancias de investigación en el exterior, convenios de transferencia, etc.

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

[1] (REMIND) de Horizonte2020 https://remind-research.com/

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
  - **Becario alumno:**
    - Todt, Carolina
    - Federico Aguirre

5. BIBLIOGRAFÍA

[1] The number of smart homes in Europe and North America reached 45 million in 2017, 2018, IoT Business News, https://iotbusinessnews.com/2018/09/24/20413-the-number-of-smart-homes-in-europe-and-north-america-reached-45-million-in-2017/. Online. (Accessed 24 Feb 2022).

[2] Silva, B. N., Khan, M., & Han, K. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. IETE Technical Review, 1–16. 2017.

[3] Silva, B. N., Khan, M., & Han, K. Big data analytics embedded Smart City architecture for performance enhancement through real-time data processing and decision-making. Wireless Communications and Mobile Computing. 2017.

[4] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29, 1645–1660. 2013.

[5] Bhagya Nathali Silva, Murad Khan, Kijun Han. Towards sustainable Smart Cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society. 38. 2018

[6] N. Moustafa, B. Turnbull, K.-K.R. Choo, Towards automation of vulnerability and exploitation identification in iot networks, in: 2018 IEEE International Conference on Industrial Internet, ICII, IEEE, 2018, pp. 139–145.

[7] T. D. Nadeau y K. Gray, SDN: Software Defined Networks, 1ra ed. .O'Reilly Media, Inc.", 2013.