MaDIoT 3.0: Análisis de Ataques a la Demanda y Generación Distribuida en un Sistema Eléctrico

Néstor Rodríguez-Pérez
Instituto de Investigación Tecnológica, Universidad Pontificia Comillas
nestor.rodriguez@iit.comillas.edu

Javier Matanza
Instituto de Investigación Tecnológica, Universidad Pontificia Comillas
Madrid, España

Lukas Sigrist
Instituto de Investigación Tecnológica, Universidad Pontificia Comillas
Madrid, España

Jose Luis Rueda Torres
Delft University of Technology, Países Bajos

Gregorio López López
Instituto de Investigación Tecnológica, Universidad Pontificia Comillas

***Resumen*—Este artículo analiza el impacto y la eficacia de los ataques MaDIoT 3.0 en el modelo PST-16, un sistema europeo simplificado. Estos ataques, de carácter novedoso, permiten comprometer de forma simultánea dispositivos IoT de alta potencia en la demanda y recursos de generación distribuida, como inversores fotovoltaicos. Los resultados muestran que la incorporación de generación solar fotovoltaica distribuida reduce tanto la tasa de éxito como el impacto de los ataques MaDIoT centrados en la alteración de la demanda, en comparación con un sistema sin dicha generación. En los ataques MaDIoT 3.0, la manipulación de la demanda resulta más determinante para el éxito global del ataque que la generación distribuida. Asimismo, se evidencia que la escalabilidad y la replicabilidad local de dispositivos IoT vulnerables de alta potencia son factores más críticos que su despliegue en áreas geográficas extensas.**

***Index Terms*—MaDIoT, sistemas eléctricos, estabilidad, ciberataque**

Tipo de contribución: *Investigación ya publicada (límite 2 páginas)*: "MaDIoT 3.0: Assessment of Attacks to Distributed Energy Resources and Demand in a Power System"[1]

I. Introducción

El creciente uso de dispositivos de Internet de las Cosas (IoT) y de Recursos Energéticos Distribuidos (DER) está ampliando la superficie de ciberataque de los sistemas eléctricos. Además de los ataques a sistemas de control, la manipulación coordinada de dispositivos IoT de alta potencia puede reducir los márgenes de seguridad de la red eléctrica y provocar la actuación de protecciones.

Los ataques MaDIoT (Manipulation of Demand via IoT) han sido analizados previamente en distintos sistemas eléctricos [2, 3, 4], mostrando que su impacto depende en gran medida de las características del sistema afectado. El artículo publicado que aquí se resume presenta y estudia los ataques MaDIoT 3.0, que combinan la manipulación de demanda y la desconexión de generación fotovoltaica distribuida, con el objetivo de responder a dos preguntas:

- P1: ¿Cómo afecta la presencia de generación solar fotovoltaica distribuida al éxito de los ataques de MaDIoT 1.0?
- P2: ¿Cuál es el éxito y el impacto de los ataques de MaDIoT 3.0 en comparación con los ataques de MaDIoT 1.0 en el mismo sistema eléctrico?

II. Metodología

El estudio se realiza sobre el modelo PST-16, una representación simplificada del sistema eléctrico europeo con tres áreas, utilizando DIgSILENT PowerFactory. En el modelo se incluyen protecciones de subfrecuencia, sobrefrecuencia, subtensión y sobretensión, cuya configuración se detalla en [1], así como las características del modelo de red PST-16 empleado. Se consideran escenarios con y sin generación fotovoltaica distribuida en el área C del PST-16, con un nivel de penetración de DER representativo de escenarios realistas para 2030 [1].

Los ataques analizados corresponden a MaDIoT 1.0, donde únicamente se incrementa la demanda a través de dispositivos IoT comprometidos, y MaDIoT 3.0, que combinan el aumento de demanda con la desconexión coordinada de DER. En todos los casos se asume que el atacante no dispone de información detallada del sistema, seleccionándose de forma aleatoria los nodos atacados y evaluándose el éxito del ataque en función de si ha habido alguna protección que ha actuado. Para facilitar la comprensión de los resultados, la Figura 1 detalla el sistema seguido para nombrar los escenarios analizados.

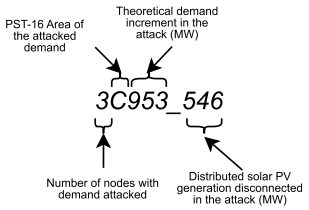

Figura 1. Nomenclatura de los escenarios analizados en [1]

III. Resultados

Para responder a las preguntas de investigación planteadas, se realizaron simulaciones de distintos escenarios en PowerFactory (Tabla IV en el artículo original [1]).Esta sección resume los principales hallazgos en [1]; debido al límite de extensión del resumen, no es posible incluir todas las figuras y tablas.

III-A. Influencia de los DER en los ataques MaDIoT 1.0 (Pregunta 1)

Los resultados de la Figura 2 muestran que la inclusión de generación solar distribuida en el área C del PST-16

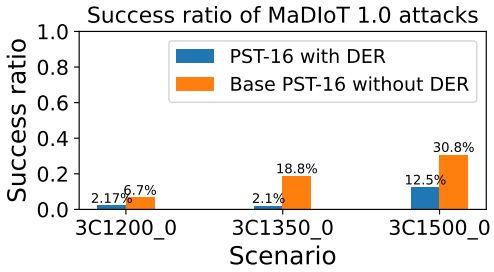

Figura 2. Éxito de los ataques MaDIoT 1.0 en el PST-16 con y sin DER

reduce significativamente la tasa de éxito y el impacto de los ataques MaDIoT 1.0 en comparación con el sistema original sin DER. En los escenarios analizados, las tasas de éxito son estadísticamente más bajas cuando hay DER (nivel de significación del 5 %). Solo se observan tasas de éxito significativas en los ataques de mayor magnitud (aumento de la demanda de 1500 MW).

Esto se explica porque, aunque la conexión de DER reduce la inercia síncrona, la frecuencia no es el principal factor que provoca inestabilidad de la red en estos escenarios. En cambio, el éxito del ataque está relacionado principalmente con la tensión en la red y el ángulo de rotor de los generadores. La conexión de DER aumenta las tensiones de los buses en el área C en un 1 % de media, lo que coloca al sistema en mejores condiciones para enfrentarse al ataque.

Los ataques de mayor impacto que se analizan de manera detallada en [1] muestran que, en el sistema con DER, los ataques principalmente provocan caídas progresivas de tensión en los buses atacados, lo que conduce a una desconexión limitada de cargas por subtensión y a la eventual estabilización del sistema. La desconexión máxima de demanda observada en presencia de DER es de aproximadamente el 1,2 % de la demanda inicial, lo que es sustancialmente inferior al 13-20 % registrado en ataques equivalentes en el sistema sin DER. Simulaciones adicionales confirman que los escenarios de ataque que tienen éxito en el sistema PST-16 básico se vuelven ineficaces cuando hay DER. En general, la sustitución del 10 % de la generación centralizada por generación de DER mejora notablemente la robustez del sistema PST-16 frente a los ataques MaDIoT 1.0.

III-B. Comparativa entre los ataques MaDIoT 1.0 y MaDIoT 3.0 (Pregunta 2)

Los ataques MaDIoT 3.0 presentan tasas de éxito más bajas que los ataques MaDIoT 1.0 con potencia total equivalente. Los resultados indican que la cantidad y la concentración de la demanda comprometida tienen una mayor influencia en el éxito del ataque que la desconexión de los DER por sí sola. Además, los ataques centrados en unos pocos nodos de demanda producen mayores caídas de tensión locales y, por lo tanto, son más disruptivos que los ataques distribuidos entre muchos nodos.

Los análisis de los casos de MaDIoT 3.0 de gran magnitud muestran caídas moderadas de tensión con algunas desconexiones de demanda por este motivo, con una dinámica estable del ángulo del rotor y sin inestabilidad de frecuencia. Cuando se comparan con los ataques MaDIoT 1.0 de magnitud teórica similar, los ataques MaDIoT 3.0 causan perturbaciones menores en el sistema, lo que indica un papel más relevante de la manipulación de la demanda en las consecuencias del ataque.

Los escenarios en los que la demanda comprometida y los DER atacados se encuentran en zonas diferentes no aumentan significativamente ni la tasa de éxito ni el impacto de los ataques. Aunque atacar la demanda en la zona A produce una tasa de éxito ligeramente superior a la de la zona C, el impacto global en el sistema sigue siendo comparable y reducido. Los ataques dirigidos a la demanda en la zona B no tienen éxito en las condiciones analizadas.

Por último, distribuir la demanda comprometida entre un mayor número de nodos reduce drásticamente la tasa de éxito, lo que confirma que la tensión localizada es un factor clave para la eficacia del ataque en el PST-16. Sin embargo, cuando los ataques a los DER se combinan con ataques a la demanda moderadamente distribuidos, la tasa de éxito y el impacto aumentan considerablemente. En el escenario combinado más grave, se observan colapsos de tensión, desconexiones de generadores y desconexiones de demanda a gran escala, lo que indica la posibilidad de apagones en áreas extensas.

IV. Conclusiones

Los resultados muestran que añadir un 10 % de generación solar distribuida (reemplazando generación centralizada) en el área C del sistema PST-16, resultó en un aumento promedio de tensión de un 1 %, reduciendo la efectividad de los ataques MaDIoT 1.0 en comparación con escenarios sin DER (Pregunta 1).

En el caso de los ataques MaDIoT 3.0 (Pregunta 2), los resultados indican que la demanda desempeña un papel más decisivo en el éxito del ataque que el DER. Dispersar la demanda atacada en múltiples nodos o enfocar el ataque a la demanda de áreas distintas a las que contienen el DER comprometido redujo significativamente la tasa de éxito de MaDIoT 3.0. En consecuencia, la concentración de dispositivos IoT vulnerables en un número limitado de nodos puede representar un riesgo mayor que una vulnerabilidad generalizada en dispositivos distribuidos en el sistema.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el proyecto eFORT (European Union's Horizon Europe Research and Innovation programme, Grant Agreement No 101075665); y el proyecto RESPONSE (European Union's Horizon 2020 research and innovation programme, Grant Agreement No. 957751).

Referencias

[1] N. Rodríguez-Pérez, J. Matanza, L. Sigrist, J. Rueda Torres, and G. López, "Madiot 3.0: Assessment of attacks to distributed energy resources and demand in a power system," *IEEE Open Access Journal of Power and Energy*, vol. 12, pp. 552–563, 2025.

[2] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium*, 2018, pp. 15–32.

[3] T. Shekari, A. A. Cardenas, and R. Beyah, "Madiot 2.0: Modern high-wattage iot botnet attacks and defenses," in *31st USENIX Security Symposium*, 2022, pp. 3539–3556.

[4] N. Rodríguez-Pérez, J. Matanza Domingo, L. Sigrist, J. L. Rueda Torres, and G. López López, "Confronting the threat: Analysis of the impact of madiot attacks in two power system models," *Energies*, vol. 16, no. 23, 2023.