Académicos UOH desarrollan pionera investigación en Chile sobre detector de ciberataques

Claudio Burgos y Diego Muñoz, junto al investigador Anant Kumar, publicaron -en una prestigiosa revista internacional- sus estudios sobre el detector de ciberataques para sistemas eléctricos e infraestructuras críticas.

La plataforma de compras Mercado Público sufrió durante septiembre de 2023 importantes problemas de ciberseguridad con su proveedor de infraestructura tecnológica, situación que la mantuvo varios días con sus operaciones paralizadas, afectando a cientos de entidades estatales que operan a través de la plataforma.

A nivel mundial, nos estamos acostumbrando a la frecuencia de estos intentos no deseados de querer robar, exponer, deshabilitar o destruir información mediante el acceso no autorizado a sistemas informáticos. Generalmente, estos ciberataques se producen a nivel de captura de datos e información sensible de ellas, no obstante, pueden afectar infraestructura crítica para los países.

Dada su envergadura, la prestigiosa revista científica de carácter internacional ***IEEE Transactions on Industrial Electronics***, acaba de publicar la investigación de los académicos del Instituto de Ciencias de la Ingeniería de la Universidad de O’Higgins (UOH), Claudio Burgos y Diego Muñoz, junto al investigador postdoctoral Anant Kumar: “Reinforcement Learning-Based False Data Injection Attacks Detector for Modular Multilevel Converter”, la cual propone un detector de ciber ataques para convertidor multinivel.

El artículo científico, elaborado en colaboración con investigadores de la Universidad de Chile: Cristóbal Gallardo, Yeiner Arias y Roberto Cárdenas; de la Universidad Andrés Bello: Alex Navas; y de la Universidad Técnica de Dinamarca: Tomislav Drgiceviv; desarrolla estudios pioneros en la academia en nuestro país, basado en la técnica de inteligencia artificial llamada ***reinforcement learning*** (aprendizaje por refuerzo), que permite entrenar una red neuronal capaz de darse cuenta si las mediciones utilizadas por el sistema de control del convertidor están siendo afectadas por el ciberataque denominado inyección de datos falsos.

Pensando en sistemas eléctricos modernos, cada vez más complejos y que mantienen un flujo de información considerable a través de la denominada capa ciber física, un ciberataque a este tipo de sistema podría provocar una falla crítica del mismo, afectando el suministro eléctrico de todo un país.

“Un ciberataque de estas características podría llegar a ser catastrófico en otros ámbitos como centrales nucleares, plantas de tratamiento de aguas, etcétera. Debido a esto, es necesario comenzar a estudiar la ciberseguridad en infraestructura crítica y proponer métodos de detección de ciberataques y contra-medidas. Esto lo estamos realizando en el SCoPE Lab de la UOH y dicha investigación nos ha permitido publicarlo en revistas Q1 del mundo. Este tema debería ser estudiado más en detalle en Chile y la UOH es la única Universidad del país que está estudiando y generando conocimientos el tema de ciberseguridad en sistemas eléctricos e infraestructura critica”, señala Dr. Claudio Burgos, director del Laboratorio de Sistemas de Conversión de Potencia y autor de la publicación.

Por su parte, el Dr. Diego Muñoz, también académico UOH agrega que “este tipo de ciberataque modifica la información utilizada por el sistema de control del convertidor y puede afectar la operabilidad del mismo e incluso ocasionar su desconexión del sistema eléctrico. Este trabajo mezcla

bastantes áreas de la ingeniería eléctrica, como son, electrónica de potencia, inteligencia artificial y fundamentos de control, por lo cual, es un artículo bastante completo e innovador lo que lo llevo a ser aceptado en esta prestigiosa revista científica”.