idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik IEE

Uwe Krengel

16.07.2024
http://idw-online.de/de/news837070

Forschungsprojekte
Elektrotechnik, Energie, Informationstechnik, Umwelt / Ökologie
überregional

Schutzschild für virtuelle Kraftwerke

Das Projekt SecDER hat ein neuartiges Schutzsystem entwickelt, das virtuelle Kraftwerke mit dezentralen Energieanlagen automatisiert vor Ausfällen schützt. Das System nutzt künstliche Intelligenz, um Cyberangriffe und Störungen zu erkennen. Anders als marktübliche Systeme arbeitet das neue System nur mit Daten der Kommunikation zwischen den Anlagen in virtuellen Kraftwerken. Eine genaue Kenntnis der Energieanlagen und ihrer Messgrößen ist nicht notwendig. Damit ist die Lösung unabhängig von proprietärer Technologie der Anlagen und lässt sich herstellerunabhängig einsetzen. Die im Projekt prototypisch realisierte Lösung soll nun gemeinsam mit der Energiewirtschaft weiterentwickelt werden.

Für die Nutzung erneuerbarer Energien spielen virtuelle Kraftwerke eine wichtige Rolle. Sie bündeln, steuern und überwachen die Energieflüsse aus einer Vielzahl von unterschiedlichen dezentralen Energiequellen wie Windenergie-Anlagen, Photovoltaik-Anlagen, Wasserkraftwerke etc. und agieren damit wie ein Großkraftwerk, um die erforderliche Poolgröße für die erfolgreiche Teilnahme an den Strommärkten (Spot- und Regelreserve) zu erreichen. Der Betrieb eines solchen Anlagenparks ist technisch anspruchsvoll und lässt sich nur mittels moderner IT-Systeme bewältigen. Das vergrößert die Angriffsfläche virtueller Kraftwerke für Cyberangriffe enorm, im Gegensatz zu klassischen Großkraftwerken. „Cyber-Angriffe auf Energiesysteme lassen sich nicht vollständig vermeiden. Und wir müssen davon ausgehen, dass die Angriffe in diesem Bereich in Zukunft noch weiter zunehmen. Deshalb haben wir im Projekt SecDER den Systemen beigebracht, auf Cyber-Angriffe und Störungen so zu reagieren, dass Totalausfälle vermieden werden“, sagt Projektleiter Tobias Schellien vom Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik IEE.

KI erkennt Angriffe

Die Forschenden im Projekt SecDER haben deshalb zunächst die Sicherheit virtueller Kraftwerke untersucht und Cyberangriffe auf ein Modell eines virtuellen Kraftwerks simuliert. Dabei stellten sie fest, dass selbst erfolgreiche Attacken auf einzelne Anlagen bislang nicht immer von Kraftwerks- oder Anlagenbetreibern bemerkt werden. Denn herkömmliche Überwachungssysteme reagieren nicht unbedingt auf Ausfälle einzelner Anlagen, beispielsweise einer einzelnen Windenergie-Anlage. Doch verschiedene kleinere Ausfälle können in Summe auch die Sicherheit des Gesamtsystems gefährden und dazu führen, dass virtuelle Kraftwerke keinen Strom mehr liefern.

Daraufhin hat das Projektkonsortium ein System entwickelt, das dieses Problem aufgreift: Das Intrusion-Detection-System erkennt mittels Machine Learning sowohl Cyberangriffe als auch technische Störungen automatisch und wehrt diese ab, indem das gesamte System in eine passende Cybersafe-Position versetzt wird. In diesem Zustand kann keine unsichere Steuerungsmaßnahme (unsafe control action UCA) mehr ausgeführt werden. Dabei gibt es nicht nur eine Cybersafe-Position, sondern so viele, wie es Gefahrenszenarien gibt. So reagiert das System dynamisch und passgenau auf unterschiedliche Szenarien, wie Brände, DoS-Attacken u. v. m. Trotz laufender Angriffe und Störungen können virtuelle Kraftwerke so zuverlässig weiter Strom erzeugen.

Herstellerunabhängiges System

Das SecDER-Intrusion-Detection-System nutzt allgemeine Daten und Kommunikationskanäle, die jede Anlage mit ihrem virtuellen Kraftwerk teilt, statt Daten aus einem spezifischen Netz und Systemen einer spezifischen Anlage. Dadurch ist die SecDER-Lösung unabhängig von jeder speziellen proprietären Technologie, spezifischer Netzwerkarchitektur oder -protokollen und abstrahiert von herstellerspezifischer Technik. Dennoch schafft es die Lösung nachweislich immer noch, Störungen zu finden.

Die Forschenden haben das System im Projekt prototypisch realisiert. Jetzt sollen die Lösungen gemeinsam mit der Energiewirtschaft weiterentwickelt werden. „Angesichts der komplexen und fortgeschrittenen Bedrohungen, die den Energiesektor und die virtuellen Kraftwerke betreffen, sind fortschrittliche Lösungen erforderlich. Die im SecDER-Projekt entstandenen Lösungen sind genau für diese Herausforderungen entwickelt worden und sorgen dafür, dass die Systeme auch während eines Angriffs funktionsfähig bleiben", sagt George Gkoktsis, Wissenschaftler in SecDER am Fraunhofer-Institut für Sichere Informationstechnologien SIT.

Das Projekt SecDER - KI-basierte Erkennung und resiliente Vermeidung von Cyber-Angriffen und technischen Störungen bei virtuellen Kraftwerken und dezentralen Energieanlagen wurde vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) mit insgesamt 2,7 Millionen Euro gefördert und vom Projektträger Jülich unterstützt. Das Projekt begann im April 2021 und dauerte 36 Monate. Beteiligt waren die Fraunhofer-Institute IEE und SIT sowie die Hochschule Hannover, die DECOIT GmbH, die ENERTRAG AG und die ANE GmbH & Co. KG.

wissenschaftliche Ansprechpartner:
Tobias Schellien, Fraunhofer IEE

URL zur Pressemitteilung:
https://www.iee.fraunhofer.de/de/presse-infothek/Presse-Medien/2024/schutzschild-virtuelle-kraftwerke.html

KI-basiertes Schutzsystem für Energiesysteme der Zukunft: Florian Rehwald und Christoph Decker (vorn) greifen über das Dashboard auf das im Project SecDER entwickelte Intrusion-Detection-System zu.
Fraunhofer IEE
Fraunhofer IEE