نماذج تعلم مُحسَّنة للدفاع ضد الهجمات السيبرانية في الأنظمة السيبرانية - الفيزيائية

وليد يمّاني
المشرفون
د. نور مصطفى
أ.د. بنيامين تيرنبول
د. مروة كشّك

أطروحة مقدمة لتحقيق متطلبات الحصول على درجة دكتوراه الفلسفة

مدرسة الهندسة وتكنولوجيا المعلومات
جامعة نيو ساوث ويلز
أستراليا، ديسمبر

٢٠٢٣

● الملخص

تركز هذه الأطروحة البحثية على تعزيز أمان الأنظمة السيبرانية-الفيزيائية (CPS) في البنية التحتية الحيوية، وذلك في ظل التحديات الأمنية المتزايدة التي تطرأ مع تزايد اعتماد هذه الأنظمة. لذا، أصبح من الضروري تحليل نقاط ضعف مكونات هذه الأنظمة في سياق الهجمات الخبيثة لضمان حماية فعالة. الهدف الرئيسي من هذه الأطروحة هو تقديم فهم شامل لنقاط ضعف أنظمة CPS وتطوير إطار دفاعي باستخدام طرق التعلم العميق وخوارزميات التحسين لمواجهة الهجمات السيبرانية ضد أنظمة CPS، وبشكل محدد في الشبكات الذكية مثل نظم الطاقة ونظم النقل. لتحقيق هذا الهدف تم تقسيم هذا التحدي الكبير إلى ثلاثة تحديات فرعية: تحديد الهجمات المنسقة وسلوكياتها في أنظمة CPS، دراسة تأثير تحسين نموذج الدفاع القائم على التعلم العميق في البيئات العدائية، وكشف الأنشطة الخبيثة في أنظمة CPS اللامركزية و تحسين نماذج الدفاع المعتمدة على التعلم الفيدرالي.

لمعالجة هذه التحديات، تقترح هذه الدراسة إطارًا دفاعيًا مبتكراً باستخدام طرق التعلم العميق وأساليب التحسين لفحص وتحديد نقاط ضعف أنظمة CPS عند التعرض للهجوم السيبراني. يتضمن هذا الإطار ثلاث مساهمات رئيسية. المساهمة الأولى هي تطوير نموذج برمجي ثلاثي المستويات فعال يحدد سيناريوهات الهجوم، بالإضافة إلى أفضل الإجراءات الدفاعية في نظم الطاقة الذكية. المساهمة الثانية هي تصميم تقنية لامركزية جديدة لحماية المعلومات السرية لأنظمة CPS والدفاع ضد الملاحظات الخبيثة. يتم تحقيق ذلك باستخدام تقنية تحسين سرب الجسيمات ذات السلوك الكمي لضبط تلقائي البارامترات الفائقة للتعلم الفيدرالي في المركبات الذاتية القيادة. المساهمة الثالثة هي تطوير نموذج تعلم فيدرالي يعتمد على نسخه مطوره من خوازمية تحسين السرب لتحقيق معايير الأمان لأنظمة CPS اللامركزية المتنوعة.

لإثبات فعالية الإطار المقترح، تم إجراء تجارب محاكاة واسعة على هجمات تسميم البيانات في سيناريوهات متعددة. تكشف نتائج هذه التجارب عن فعالية الإطار المقترح مقارنة بالطرق المماثلة.