Numer rejestracyjny: 2023/05/Y/ST7/00192, kierownik projektu: dr hab. inż. Krzysztof Ronald Grochla

Analiza przywracania funkcjonowania poprzez testy obciążeniowe odporności infrastruktury na Ukrainie

W świetle poważnych zakłóceń systemowych, takich jak pandemia COVID, przerwy w łańcuchu dostaw i konflikty geopolityczne, potrzeba oceny odporności - zdolności systemów do przywrócenia funkcjonowania po zakłóceniach - nigdy nie była bardziej nagląca. Jednak podstawy badań odporności systemów pozostają słabo rozwinięte, szczególnie w kontekście działania czynników zewnętrznych. Projekt ten na bazie przykładów z Ukrainy, wykorzystując jej sektor usług cyfrowych, który jednocześnie stoi w obliczu zwiększonego ryzyka z powodu powtarzających się ataków zewnętrznych. Naszym celem jest zweryfikowanie hipotezy, że odzyskiwanie i odporność systemów na zagrożenia można określić ilościowo za pomocą testów warunków skrajnych połączonych sieci reprezentujących ich funkcje systemowe. Proponowane przez nas metoda Resilience-Recovery Under Attack (RRUA) ma na celu ilościowe zbadanie różnych etapów reakcji systemu na różne ataki lub katastrofalne awariie. Stosujemy wieloaspektową metodologię łączącą naukę o sieciach (ang. network science), analizę odporności, wyjaśnialną sztuczną inteligencję (xAI) i technologie cyfrowych bliźniaków. To zintegrowane podejście ma na celu przedefiniowanie systemowego modelowania odbudowy i adaptacji wzajemnie połączonej infrastruktury na Ukrainie, korzystając z wiedzy proponowanego przez nas międzynarodowego partnerstwa jednostek z USA, Ukrainy, Polski, Estonii i Litwy. Projekt ten będzie wykorzystywał trójtorowe podejście: udoskonalenie RRUA przy użyciu analiz danych z lotniska DFW, testowanie go w Polsce, Estonii i na Litwie, w tym ludzkich zachowań, oraz wspólną integrację RRUA w ukraińskich systemach infrastruktury cybernetycznej i energetycznej w obecności dynamicznych zagrożeń i zmiennych danych. Sukces może zrewolucjonizować perspektywy Ukrainy w zakresie odbudowy, pozycjonując ją jako globalny przykład strategii odporności. Ponadto nasz projekt uznaje konieczność zintegrowania ukraińskich naukowców z zachodnimi współpracownikami, w odpowiedzi na izolację społeczności naukowej tego kraju przez napięcia geopolityczne.

Zespół IITIS PAN skupi się na tworzeniu modeli matematycznych i symulacji komputerowych, aby pokazać, jak różne systemy, takie jak sieci komunikacyjne i energetyczne, radzą sobie po poważnych awariach czy katastrofach. Pozwoli nam to lepiej zrozumieć, jak przywrócić normalne funkcjonowanie systemom po różnego rodzaju zdarzeniach. W ramach projektu te modele zostaną uogólnione w celu (1) uchwycenia odbudowy systemu po załamaniu, włączając analizę stanów przejściowych pokazującą, jak system zachowuje się podczas odbudowy, oraz (2) przedstawienia scenariuszy odbudowy dla dużej różnorodności rozproszonych systemów, od sieci telekomunikacyjnych i energetycznych, po systemy transportowe czy inne niezbędne dla funkcjonowania infrastruktury. Chcemy zrozumieć, jak krytyczne systemy takie jak sieci telefoniczne, sieci energetyczne i lotniska wracają do normy po poważnych zakłóceniach. Pozwoli nam to przewidzieć czego można się spodziewać w różnych sytuacjach kryzysowych, od drobnych usterek do poważnych awarii.

Aby przetestować nasze modele, użyjemy rzeczywistych danych i różnorodnych scenariuszy, w tym związanych z danymi zebranymi podczas wojny na Ukrainie. W projekcie wykorzystamy zaawansowane metody matematyczne i symulacje zdarzeń dyskretnych. Na przykład, zbadamy scenariusz w którym zbyt wiele urządzeń jednocześnie próbuje przyłączyć się do sieci np. po zaniku prądu. Stworzymy realistyczne scenariusze "co jeśli" przy użyciu symulacji komputerowych i rzeczywistych danych, w tym informacji sprzed i podczas wojny. Zbadamy efekty jednoczesnych awarii w wielu krytycznych elementach sieci, prowadzących do globalnej zapaści infrastruktury. Następnie zestawimy syntetyczne dane z rzeczywistymi danymi dotyczącymi ataków na infrastrukturę na Ukrainie. Zintegrujemy dane z Instytutu Phukova dotyczące topologii przedwojennej sieci energetycznej i informacje na temat zmian w systemie podczas działań wojennych. Dane o miejscach, w których mogły mieć miejsce ataki, pozyskamy z publicznych źródeł informacji, takich jak np. projekt Black Marble NASA, który może być źródłem zgrubnego oszacowania lokalizacji eksplozji w trakcie konfliktu. W ostatnim etapie, techniki uczenia maszynowego zostaną użyte do identyfikacji korelacji pomiędzy różnymi czynnikami systemowymi (takimi jak np. topologia sieci i redundancja elementów) na całkowity czas odtwarzania się systemu po awarii.