XXIX WARSZTATY NAUKOWE PTSK

SYMULACJA W BADANIACH I ROZWOJU

STRESZCZENIA REFERATÓW

POLSKIE TOWARZYSTWO SYMULACJI KOMPUTEROWEJ

POLITECHNIKA GDAŃSKA
ODDZIAŁ GDAŃSKI POLSKIEGO TOWARZYSTWA FIZYCZNEGO

Patronat honorowy

J.M. Rektor Politechniki Gdańskiej
prof. dr hab. inż. Krzysztof Wilde

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Nauki w ramach Programu „Doskonała Nauka II”.

SWORNEGACIE
22-24 maja 2025

SPIS TREŚCI

A1

Andrzej Ameljańczyk

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: andrzej.ameljanczyk@wat.edu.pl

Projektowanie rankingów odpornych na manipulacje

Zagadnienie tworzenia rankingów zbioru obiektów ocenianych wieloma kryteriami jest bardzo powszechne w wielu dziedzinach życia. Różni się od klasycznego zagadnienia optymalizacji tym, że określa „jakość" wszystkich obiektów od „najlepszego do najgorszego" a nie wyłącznie element „najlepszy" co jest domeną optymalizacji. Rankingi są prostym i wygodnym narzędziem wspomagania decyzji w bardzo wielu dziedzinach życia.Mogą też być wykorzystywane do tzw. „miękkiego" sugerowania podejmowania konkretnych wyborów (decyzji). Typowe rankingi, konstruowane na potrzeby komercyjne czy też społeczne tworzone są na ogół w oparciu o tzw. funkcje rankingowe, lub też heurystycznie, a nawet intuicyjnie w oparciu o bardzo proste metody i narzędzia. Nie mają one zatem wystarczającego waloru obiektywizmu i często służą jedynie celom marketingowym a nawet swego rodzaju manipulacjom.W wielu obszarach życia jest to jednak niedopuszczalne i bardzo szkodliwe. Takimi przykładami są np. procedury ustalania rankingu ofert w zamówieniach publicznych (przetargach) i wszelkich innych przedsięwzięciach, takich jak konkursy projektów, grantów itp., w których wynik rankingu może mieć duże konsekwencje finansowe, prestiżowe lub handlowe. Powszechnie stosowane metody polegające na tworzeniu tzw. „ocen ważonych" czy też „ważonych decyzji ekspertów" są obarczone subiektywizmem i możliwością kamuflowanej manipulacji. Łatwo można pokazać, że dobierając odpowiednie wartości współczynników wagowych lub wartości progów można istotnie zmieniać ranking wynikowy. Celem niniejszej pracy jest pokazanie metod tworzenia rankingów odpornych na możliwość kamuflowanej manipulacji.

A2

Ryszard Antkiewicz, Andrzej Najgebauer, Dawid Maślanik

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: ryszard.antkiewicz@wat.edu.pl

Badanie wpływu nowych i przełomowych technologii na działania wielodomenowe w obronie kolektywnej. Metody, narzędzia i wnioski z gry wojennej.

W dniach 23.10. 24 - 25.10.2024 r. we Włoszech w La Spezii w ośrodku NATO - CMRE odbyła się gra wojenna z udziałem wysokich rangą oficerów polskich i NATO-wskich, dotycząca obrony kolektywnej, pozwalająca na badanie wpływu nowych przełomowych technologii (EDT) na wielodomenowe działania wojenne (MDO). Autorzy tej prezentacji odegrali kluczową rolę w organizacji i przygotowaniu gry, w tym narzędzi optymalizacyjnych i symulacyjnych wspierających przebieg gry. Celem gry było kompleksowe przetestowanie wpływu EDT na prowadzenie operacji wielodomenowych w konflikcie na dużą skalę, wymagającym uruchomienia art. V Traktatu Waszyngtońskiego. Gra miała charakter eksperymentalny, z trzema zespołami graczy, jednym czerwonym i dwoma niebieskimi (innowacyjnym i konwencjonalnym), zorganizowanymi poza zespołem EXCON, podejmującymi strategiczne decyzje w celu przygotowania niebieskich sił reagowania na ten sam plan działania przeciwnika. Gracze to doświadczeni planiści, rekrutujący się ze Sztabu Generalnego WP, Dowództwa Operacyjnego SZ RP oraz Centrum Doktryn i Szkolenia SZ RP, a także dowództw NATO ACT i ACO. Plan użycia sił innowacyjnych, wyposażonych w środki walki o najnowszych technologiach wojskowych i działających we wszystkich domenach walki kontra plan sił konwencjonalnych w podstawowych domenach i z przewagą działań kinetycznych w celu zidentyfikowania różnic w efektach realizowanych planów. Przygotowano również drugą fazę gry, zakładającą wykorzystanie sił perspektywicznych (5-7 lat) zarówno dla Czerwonych, jak i Niebieskich w dwóch wariantach EDT i konwencjonalnym. Scenariusz ataku dla czerwonych podobny jak w pierwszej fazie, ale ich siły zmodernizowane, a odpowiedź ze strony niebieskich

perspektywiczna. Efekty posunięć graczy - plany działań - zostały zasymulowane i obliczone za pomocą aplikacji WAT, w postaci parametrów konfliktu - strat stron, z podziałem na różne rodzaje wojsk, tempa posuwania się sił, głębokości wejścia w obronę, czasu trwania operacji oraz różnych efektów zakończenia operacji - osiągnięcia celu, zatrzymania sił, przekroczenia dopuszczalnych strat. Uzyskane wyniki potwierdziły skuteczność metody badania wpływu EDT na przebieg operacji realizowanych w środowisku wielodomenowym i pozwoliły profesjonalnym operatorom wojskowym (planistom strategicznym i operacyjnym) wziąć udział w nowatorskim eksperymencie ACT i zapoznać się z nowoczesnym podejściem do planowania operacji i badania efektów tych operacji. Badacze byli w stanie uzupełnić bazy danych, urealnić swoje analizy, uzyskać szczegółowe uwagi na temat aplikacji wykorzystywanych do wsparcia gry wojennej, w tym sformułować dodatkowe wymagania funkcjonalne. Ponadto uzyskano oszacowanie potencjalnych kosztów modernizacji sił dla EDT w operacjach MDO.

A3

Franco Bagnoli, Michele Baia

Dept. Physics and Astronomy
University of Florence, Italy
e–mail: lukasz. franco.bagnoli@unifi.it

Synchronization and control of Lorenz systems

We are interested in developing techniques for meteorological data assimilation and forecasting. We shall use Lorenz systems as toy model, exploiting the replica synchronization scheme for estimating the parameters of a (supposedly unknown) master system, in the case of possible access to the dynamical variables and when these are not directly available, and the synchronization can by enacted only through a projection or from the analysis of a data series.

A4

Maciej Bobrowski, Sapajan Ibragimow, Leonard Komando, Justice Inkoom, Hope Dzamesi

Faculty of Technical Physics and Applied Mathematics,
Gdańsk University of Technology
Narutowicza 11/12, 80-233 Gdańsk, Poland
e–mail: macbobro@pg.edu.pl

Iron(III) oxide isomers: structure, spin and redox properties. Application in ferrofluids based on ionic liquids

Iron (III) oxides exhibit various configurations and even the smallest stoichiometricallymolecules can create diverse structures. Their spin is generally very high, similarly to the case of the iron atom, iron (III) cations and iron (III) complexes. It turns out that the redox properties of iron (III) oxidemolecules are also quite good, similarly to salts and complexes. Iron (III) oxide nanosystems are stoichiometrically and structurally large molecules. It is important to learn the redox properties of iron oxide nanosystems because these systems, already commonly produced in both wet and dry methods, can act as redox couples when added to electrochemical cells or when included in the structure of electrodes. It has recently been shown that a suspension of ferromagnetic nanoparticles in ionic liquids can, under certain conditions, become a stable ferrofluid. In addition, in such systems, some redox pairs can be dissolved and electrochemical properties can be improved.What'smore, such amaterial can be additionally used as a thermoelectric in a Peltier-type device, i.e. instead of traditional semiconductors based on solid-state materials. Constructively, ferrofluid cells can be built into amatrix made of flexible polymers or, for example, ceramics, and the whole can constitute a thermo-electric plate. This solution is possible in the case of additional use of technology based on the use of polymers deposited on liquids in an ultra-precise manner while maintaining the shape of the drop, which at the same time enables miniaturization of individual galvanic cells and the entire device of the Peltier converter type. In addition, it has recently been confirmed that a suspension of ferromagnetic nanoparticles in organic solvents induces the Sorret efect and generates the Seebeck efect,with the

Seebeck coeficient being asmuch as about 10−5 V/K,which is about an order ofmagnitude more than in the case of ionic liquids or traditional semiconductors based on bismuth telluride. Therefore, the use of ferromagnetic nanoparticles in ionic liquid systemsmay prove to be a very efectivemethod of increasing heat recovery and its conversion into electrical energy. In thework, informationwas obtained about the structures of iron (III) oxides themselves of even larger sizes as well Acknowledgements: Research supported by grant number 731976 for the projectwith acronymMagenta implemented within theHorizon 2020 programof the European Union.

A5

Łukasz Czerniszewski

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: lukasz.czerniszewski@wat.edu.pl

Symulacja działań wojennych przy wykorzystaniu refleksyjnej teorii gier oraz teorii Schwartza

W artykule opisano, jak można modelować zachowania ludzkie z wykorzystaniem teorii Schwartza oraz refleksyjnej teorii gier. Omówiono ideę zamodelowania osób przy pomocy jedenastu uniwersalnych cech wartości, które są opisane w teorii Schwartza. Udało się stworzyć matematyczny model ludzki, który ustala, jak dane jednostki lub grupy osób w zależności od stany swojej wiedzy będą się zachowywać. Dzięki niemu możliwe jest zdecydowanie, jaką wiedzę należy udostępnić, aby w uzyskać najbardziej korzystny wynik.

A6

Jakub Grątkiewicz

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: jakub.grontkiewicz@wat.edu.pl

Inteligentni czatbot-asystenci w dobie dużych modeli językowych (LLM)

Prezentacja podejmie kluczowe zagadnienia związane z dynamicznym rozwojem generatywnego AI i jego zastosowaniami w konwersacyjnych systemach wsparcia. Na wstępie zostanie syntetycznie objaśnione, czym będą duże modele językowe (LLM): głębokie sieci liczące dziesiątki miliardów parametrów i trenowane samonadzorowanie na bilionach tokenów. Zostaną przedstawione wykorzystywane korpusy tekstu, przebieg tokenizacji oraz powody, dla których skala danych okaże się krytyczna dla jakości generacji. Zostanie również zilustrowane, w jaki sposób modele te nabędą zdolność „rozumienia" intencji użytkownika – od poziomu składni, przez semantykę, aż po kontekst dialogu.

Następnie zostanie omówiony problem „zamrożonej wiedzy": po zakończeniu pre treningu LLM y nie będą aktualizowały swoich wag, przez co szybko „zestarzeją się" poznawczo. Skutkiem okażą się halucynacje faktograficzne oraz odwoływanie do nieaktualnych standardów i protokołów. W odpowiedzi zostanie wprowadzona koncepcja Retrieval Augmented Generation (RAG) – hybrydowego podejścia, w którym model językowy włączy do promptu wyniki wyszukiwania z wektorowego indeksu, zyskując dostęp do bieżących danych poza własną „pamięcią".

W dalszej części zostanie pokazane, jak agenci AI rozszerzą możliwości RAG. Agent planujący będzie mógł kolejno: przeformułować zapytanie, wywołać właściwe narzędzie – reprezentację wektorową lub zewnętrzne API, zweryfikować fakty, zbudować ostateczną odpowiedź z cytatami źródeł.

Takie podejście ograniczy halucynacje, zautomatyzuje odświeżanie wiedzy i zapewni większą kontrolę nad tokiem rozumowania systemu.

Kulminacją wystąpienia będzie demonstracja prototypu „CyberSecurity Expert", przygotowanego przez zespół Coddiers

(Wydział Cybernetyki WAT) na NATO TIDE Hackathon 2025 w Dunkierce.

A7

Romuald Hoffmann

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: romuald.hopffmann@wat.edu.pl

Stochastyczny model (Q_1,Q_2,r) - strategii odnowy redundantnych konfiguracji zasobów obrony cybernetycznej ze zmiennym momentem złożenia żądania uzupełnienia

Istotną trudnością w zwalczaniu ukierunkowanych ataków cybernetycznych jest asymetria informacji. Atakom tym zwykle towarzyszy etap rekonesansu, realizowanego w ramach cyklu życia ukierunkowanego ataku cybernetycznego, prowadzonego przez atakujących w celu lepszej identyfikacji podatności systemu. W przeciwieństwie do atakujących, obrońcy są zazwyczaj w niekorzystnej sytuacji podczas odpierania celowo maskowanych ataków na ich systemy informatyczne. Aby przeciwdziałać tej asymetrii, dobrym podejściem jest Moving Target Defense (MTD). Obrona MTD, która wykorzystuje proaktywne mechanizmy obrony systemów, w znacznym stopniu może zakłócać lub blokować potencjalne ataki. W pracy omawia się propozycję jednej z takich taktyk MTD, w której obrońcy mogą cyklicznie rekonfigurować system, aby zwiększyć niepewność atakujących i ich szanse na sukces. W artykule proponuje się probabilistyczną (Q_1,Q_2,r) – strategię polegającą na odnawianiu i sukcesywnej aktywacji puli wstępnie zmontowanych konfiguracji zasobów obronnych. Akumulacja i odnawianie zasobów operacyjnych opierają się na trzech poziomach aprowizacji: Q_1, Q_2 i r, przy założeniu, że poziomy Q_1 i Q_2 są całkowitoliczbowymi wielkościami większymi od r. Poziom r jest poziomem liczby pozostałych niewykorzystanych konfiguracji w aktualnie eksploatowanej puli po osiągnięciu, którego, składane jest zapotrzebowanie odtworzenia puli zapasowych konfiguracji. Ponadto zakłada się, że wybór jednej z dwóch wielkości Q_1,Q_2 jest losowy i uzależniony od czasu życia (eksploatacji) jednej z konfiguracji aktualnie eksploatowanej puli. Czas potrzebny na przygotowanie nowej puli zasobów jest również losowy. Prezentowany model zakłada

powtarzalność cyberataków i wobec tego, zakłada się wyłączenie systemu w przypadku braku wolnych zasobów. Zakłada się ciągłe rozkłady prawdopodobieństwa czasów życia zasobów oraz czasu niezbędnego na przygotowanie kolejnej puli zasobów oraz czasów aktywności atakujących i obrońców. W pracy podstawowe charakterystyki probabilistyczne modelu uzyskuje się w oparciu o stochastyczne procesy odnowy i procesy regenerujące się. Prezentowany model jest pewną kontynuacją i rozwinięciem prac wcześniej opublikowanych przez Autora.

A8

Piotr Kisielewski

Politechnika Krakowska
ul. Warszawska 24, 31-155 Kraków
e–mail: piotr.kisielewski@pk.edu.pl

Optimization of transport tasks of a heterogeneous fleet of vehicles considering electromobility and real world constraints

Planning vehicle tasks and crew duties is the first stage of operational planning in public transport and consists of combining scheduled trips, which are input data, into work portions constituting daily tasks of vehicles and drivers. In the case of a large, mixed fleet of vehicles of different types, especially battery-powered buses, requiring charging during task execution, operating from multiple depots, with numerous requirements and restrictions of rolling stock, the problem is a major engineering challenge, even for an experienced team of planners. IT solutions based on realistic, mathematical decision models and fast optimization algorithms can come to the rescue. For such a formulated problem, multi-criteria, mathematical decision models for vehicle and driver tasks were built, taking into account economic, technical and ecological criteria and discrete decision variables. The models take into account real requirements for vehicles and drivers' work, a mixed fleet of vehicles of different types, including electric buses, multiple depots, technical trips, battery charging with consideration of queuing at fast chargers, legal and organizational restrictions of drivers' work. The problem under consideration is an NP-hard combinatorial optimization problem. The use of classic, accurate algorithms to solve this problem is not possible in the case of timetables with many thousands of daily trips and fleets of hundreds or thousands of vehicles. The research proposed an original, fast heuristic algorithm for optimizing vehicle tasks, allowing to obtain an acceptable, although still suboptimal solution in a very short time, and an evolutionary algorithm for optimizing driver tasks. The algorithms were tested on real databases of public transport systems of selected four large Polish cities. The results of computer simulations using the developed metaheuristics were compared with the results obtained manually by a team of experienced planners. Using the developed algorithms, comparable and better results were obtained in a short time than those prepared manually by expert planners.

A9

Leonard Komando, Maciej Bobrowski

Politechnika Gadańska
Narutowicza 11/12, 80-233 Gdańsk
e–mail: leonard.komando@pg.edu.pl

Probing Solvent-Dependent Interactions of Citrate(3–) with small Iron Oxide (Fe2O3)n=1,2 clusters: A theoretical perspective

In this study, we analyzed the nature of interactions within the Fe2O3–(citrate)3− complex and the influence of different solvent environments on its stability and electronic structure. Our system involves three distinct interactions: (a) coordinate covalent bonds (Fe–O) directly anchoring citrate to the iron oxide center, (b) ionic interactions between charged groups providing overall structural integrity and enhancing solubility, and (c) hydrogen bonds stabilizing and fine-tuning the internal conformation of the ligand. Computational results indicated a complex interplay between solvent polarity and system stability. Total energy calculations showed increased overall stability in high-polarity solvents like water due to superior solvation effects. Conversely, well depth data revealed the Fe–citrate binding itself was strongest in low-dielectric solvents (EMIM-BF4), highlighting complementary rather than contradictory effects: low-dielectric solvents enhance internal ligand-cluster binding, while high-dielectric solvents optimize overall system energetics. In essence, an Fe–O bond that is quite strong in the gas-phase and low-ε solvents – due to direct Fe3+···O2− electrostatic attraction – becomes somewhat weaker in solution, as the O2− is partially stabilized by the surrounding high-ε medium and thus binds less tightly to Fe3+. Furthermore, analysis of iron weight densities demonstrated reduced ligandto-metal charge transfer (LMCT) as solvent polarity increased. B3LYP-D3(BJ) predicts higher absolute electron donation values compared to MP4(SDQ). The gas phase exhibited the strongest LMCT, while water moderately lowered iron contributions, stabilizing ligand electron density and weakening LMCT. Ionic liquids displayed intermediate behavior, emphasizing solvent-driven modulation of charge distribution within this system.

A10

Marzenna Miłek

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: marzenna.milek@wat.edu.pl

Wytyczne NIS2 jako podstawa do budowy systemu cyberodpornosci w organizacjach objętych Dyrektywą NIS2

Bardzo dynamiczny rozwój technologii cyfrowych, a co się z tym wiąże rosnąca liczba zagrożeń cybernetycznych wpływa na fakt, że wyzwaniem dla przedsiębiorstw staje się zbudowanie systemu cyberodporności. Taki stan rzeczy sprawia, że kluczowym elementem strategii każdego podmiotu gospodarczego jest zapewnienie bezpieczeństwa informacji, jakie są przetwarzane w organizacji oraz bezpieczeństwa posiadanych systemów informatycznych. Bezpieczeństwo informacji oraz właściwe zabezpieczenie danych, szczególnie wrażliwych staje się kluczowym elementem strategii każdego przedsiębiorstwa. Aby zapobiegać wielu zagrożeniom czy incydentom na poziomie rządów wielu państw pojawiła się konieczność wyznaczenia ogólnych norm i standardów cyberbezpieczeństwa w celu zbudowania cyberodporności w organizacjach. W Unii Europejskiej prace nad takimi normami rozpoczęto w 2016 roku, wprowadzając dyrektywę NIS (Network and Information Systems) , która miała na celu poprawę ogólnego poziomu cyberbezpieczeństwa, skupiając swoją uwagę na zwiększeniu bezpieczeństwa w sektorach krytycznych. Dyrektywa NIS uwydatniła kluczowe elementy cyberbezpieczeństwa takie jak zarządzanie ryzykiem, zgłaszanie incydentów, czy współpraca międzynarodowa w celu prewencji zagrożeniom transgranicznym. Kolejnym krokiem w celu osiągniecia wysokiego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej było opublikowanie w grudniu 2022 roku w Dzienniku Urzędowym Unii Europejskiej dyrektywy NIS2(Network and Information Systems 2). Termin implementacji Dyrektywy NIS-2, której celem jest dostosowanie w całej Unii Europejskiej standardów bezpieczeństwa informatycznego do nowych zagrożeń cyfrowych wyznaczono na 17 października 2024 roku. Cyberodporność nie jest jednorazowym

projektem, lecz procesem ciągłego doskonalenia. Kluczowym wyzwaniem staje się podniesie świadomości cyberodporności pracowników. Nie jest to łatwe zadanie, ponieważ polega na częstych ćwiczeniach i testowaniu reakcji na potencjalne zagrożenia
i często stoi to w kolizji do codziennych wyzwań zawodowych. Podmioty, które proaktywnie testują scenariusze kryzysowe, zabezpieczają swoje systemy i inwestują w nowe rozwiązania, mają szanse nie tylko skutecznie minimalizować skutki cyberataków, ale także skuteczniej przywracać normalne funkcjonowanie po potencjalnym incydencie. Tylko takie podejście pozwala na osiągniecie należytego poziomu cyberodporności oraz utrzymanie stabilności biznesowej w obliczu ciągle nowych zagrożeń cyfrowych. Skuteczna ochrona organizacji to połączenie cyberodporności z cyberbezpieczeństwem, można to uzyskać poprzez holistyczne podejście w którego skład wchodzi identyfikacja ryzyka, regularne testy i symulacje, analizy zagrożeń oraz stan gotowości do reagowania na zagrożenia.

https://eur-lex.europa.eu/eli/dir/2016/1148/oj [dostęp: 14.01.2025]

A11

Paweł Moszczyński, Maciej Wiśniewski, Andrzej Walczak

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: pawel.moszczynski@wat.edu.pl

Zastosowanie AI w procesie wspomagania certyfikacji urządzeń kwantowej wymiany klucza

Rozwój komputerów kwantowych stanowi wyzwanie dla współczesnej kryptografii asymetrycznej, w szczególności może stanowić zagrożenie dla kryptografii klasycznej ze względu na znane algorytmy kwantowe zagrażające współcześnie stosowanym algorytmom uzgadnia klucza. Jednym z najważniejszych kierunków odpowiedzi jest kwantowa dystrybucja klucza (QKD), która wykorzystuje prawa mechaniki kwantowej do bezpiecznej wymiany kluczy kryptograficznych. Odejście od fundamentu klasycznej kryptografii asymetrycznej, w której bezpieczeństwo opiera się na założeniu ograniczonych zasobów obliczeniowych adwersarzy, wymaga opracowania nowego podejścia do certyfikacji.

Kluczowym wyzwaniem staje się stworzenie spójnych, standaryzowanych procedur, które umożliwią rzetelną ocenę bezpieczeństwa takich systemów przed ich wdrożeniem w infrastrukturze krytycznej. Proces certyfikacji powinien obejmować nie tylko analizę teoretycznego bezpieczeństwa protokołów QKD, ale także ocenę ich praktycznej implementacji, w tym odporności na znane ataki wykorzystujące niedoskonałości sprzętowe.

Aby zwiększyć skalowalność i powtarzalność tych procesów, niezbędne jest rozwijanie zautomatyzowanych narzędzi wytwarzania ustandaryzowanej dokumentacji, jak narzędzi do wsparcia oceny bezpieczeństwa na podstawie dokumentacji technicznej. Powinny one umożliwiać generowanie procedur testowych, monitorowanie parametrów pracy i identyfikację podatności w realistycznych scenariuszach zagrożeń. W artykule wskazujemy obszary, w których AI może wspomóc przygotowania do certyfikacji, jak i proces jej przeprowadzenia. Dzięki zastosowaniu AI szereg procedur może zostać przeprowadzonych szybciej i sprawniej. Dodatkowo wdrożona jako źródło wiedzy staje się

interaktywnym wsparciem dla badaczy, przyspieszając proces oceny bezpieczeństwa na różnych etapach gotowości technologicznej urządzeń QKD.

A12

Tadeusz Nowicki, Michał Sobolewski, Paweł Pieczonka, Robert Waszkowski

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: tadeusz.nowicki@wat.edu.pl

Charakterystyki przebiegu i wyników obliczeń algorytmów genetycznych

U podstaw konstrukcji algorytmów genetycznych wyróżnić można takie pojęcia, jak populacja, osobnik populacji, operatory mutacji, operatory krzyżowania, funkcji przystosowania, operatory selekcji oraz inne. Definiuje się te elementy w taki sposób, aby oddawały one elementy sformułowanego problemu decyzyjnego. Można założyć, że dla istotnie różnych problemów decyzyjnych elementy te różnić się będą też znacząco. Realizacja algorytmów genetycznych osadzona jest najczęściej w środowisku symulacji komputerowej. Im rozwiązywany problem decyzyjny jest bardziej skomplikowany, tym środowisko symulacji jest bardziej złożone. Można postawić również tezę, że każdy problem decyzyjny można rozwiązywać różnymi algorytmami genetycznymi.
Powstaje jednak pytanie: czy pewne charakterystyki przebiegu procesu, w którym realizuje się algorytm genetyczny, mają pewne wspólne cechy, miary charakterystyki itd. niezależne od natury problemu decyzyjnego? Praca ma dać odpowiedz na to pytanie. Zdaniem Autorów można pokazać cała grupę charakterystyk, które można zdefiniować i które są charakterystyczne dla wszystkich algorytmów genetycznych.
Na podstawie procesów obliczeniowych związanych z realizacją algorytmów genetycznych zostaną przedstawione i zdefiniowane zmienne i funkcje, które odzwierciedlają te procesy, np. wielkość populacji, liczba iteracji/populacji, maksymalna liczba iteracji, parametry i wyniki operatora mutacji, parametry i wyniki operatora krzyżowania, jakość rozwiązania, różnorodność rozwiązania, czasy obliczeń składowych itd. Podana zostanie ich interpretacja oraz to, jak ich wartości mogą przedstawić własności algorytmu genetycznego odpowiadającego problemowi decyzyjnemu. Stanowić one mogą bazę do procesów

zobrazowania przebiegów obliczeniowych algorytmów genetycznych zorganizowanych w postaci ciągu eksperymentów symulacyjnych.

A13

Tadeusz Nowicki, Krzysztof Panufnik

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
E–mail: Andrzej.ameljanczyk@wat.edu.pl

Konstrukcja i badanie własności modelu symulacyjnego komunikacji symulatorów w środowisku HLA

Jednym z najważniejszych standardów prowadzenia złożonych eksperymentów symulacyjnych jest Architektura Wysokiego Poziomu (ang. High Level Architecture, HLA). HLA pozwala na integrację symulatorów różnych typów, które mogą być zbudowane przy użyciu różnych technologii. Do licznych usług zapewnianych przez HLA można wymienić zarządzanie wymianą informacji między symulatorami. Ma to szczególne znaczenie w przypadku rozbudowanych eksperymentów symulacyjnych, w których nierzadko istnieje jednocześnie kilkadziesiąt tysięcy obiektów symulacyjnych. Zarządzanie wymianą informacji o zmianach obiektów staje się więc kluczowe w celu zapewnienia wysokiej wydajności prowadzonych eksperymentów.

W literaturze spotkać można różne modele opisujące zjawisko wymiany informacji między symulatorami. Wśród nich można wyróżnić matematyczny stochastyczny model stworzony przez autorów. Losowy charakter wielu elementów modelu uniemożliwia znalezienie rozwiązania metodami analitycznymi, z wyjątkiem wąskiego podzbioru problemów. Wymusiło to budowę własnego symulatora, aby przeprowadzone eksperymenty były miarodajne.

Skonstruowano modułowy symulator z wykorzystaniem platformy .NET. W celu poprawy wydajności wykorzystano własną bibliotekę do obsługi symulacji zdarzeniowej. Badanie adekwatności symulatora wykonano w dwóch eksperymentach. W ramach pierwszego eksperymentu porównano zmierzone i teoretyczne wartości wybranych parametrów modelu matematycznego. Podczas drugiego eksperymentu tak dobrano parametry wymiany informacji między symulatorami, aby możliwe było przeprowadzenie analizy obciążenia systemu z wykorzystaniem teorii masowej obsługi.

A14

Marcin Pery, Tadeusz Nowicki, Robert Waszkowski

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: robert.waszkowski@wat.edu.pl

Badanie odporności metody steganografii wideo RAI

Celem pracy jest zaprezentowanie kompleksowego scenariusza symulacyjnego, który pozwala automatycznie testować odporność (robustness) steganograficznej metody RAI (Robust Adaptive Incremental) w warunkach zniekształceń typowych dla realnych scenariuszy transmisji wideo z dużym poziomem zakłóceń. Badania wykonano na autorskiej platformie symulacyjnej, łączącej generowanie steganogramów, aplikowanie losowych transformacji oraz w pełni automatyczne dekodowanie i analizę wyników. Z pewnej bazy utworzono algorytmem kodującym c-RAI ponad 3000 steganogramów dla kilku poziomów kodowania oznaczających coraz większą ingerencję i tym samym modyfikację pliku wideo.
Każdy steganogram poddano różnym klasom zniekształceń: kompresji, transkodowaniu, zaszumieniu Gaussa oraz przekształceniom geometrycznym (rotacji i skali). Łącznie wygenerowano ponad 20000 wariantów zniekształconych steganogramów wideo, dla których wyznaczono charakterystyczne metryki. Algorytm dekodujący d-RAI wykonywał symulacje odkodowania. Symulacje zatrzymywały się po 10s czasu odtwarzania pliku wideo. Brak odczytu zakodowanej informacji w tym limicie czasowym klasyfikowano jako niepowodzenie eksperymentu. Okazało się, że w większości przypadków wystarcza niski poziom kodowania, co zmniejsza podatność steganogramów na wykrycie (większa wartość metryki niewykrywalności). Podczas symulacji w połowie steganogramów udawało się odkodować ukrytą informację. Przedstawiona platforma symulacyjna skutecznie odwzorowuje potencjalne scenariusze występujące w praktyce (kompresja serwisów VOD, transkodowanie, zakłócenia analogowe).
Z kolei wyniki symulacyjne potwierdzają, że metoda steganografii wideo RAI zapewnia wysoką odporność. Zaproponowana metodyka symulacji może zostać bezpośrednio zaadaptowana do testowania innych

algorytmów steganografii wideo, stanowiąc uniwersalne narzędzie oceny odporności w środowisku laboratoryjnym.

A15

Stefan Rozmus

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: stefan.rozmus@wat.edu.pl

Koncepcja aplikacji wspierającej przeprowadzenie testów akceptacyjnych w ujęciu procesowym

Skuteczna organizacja testów akceptacyjnych (ang. User Acceptance Test - UAT) ma kluczowe znaczenie dla zapewnienia zgodności oprogramowania ze specyfikacją wymagań oraz zaspokojenia potrzeb i oczekiwań użytkowników końcowych. Ze swej natury jest to przedsięwzięcie złożone, wymagające odpowiedniego przygotowania. Przeprowadzenie testów akceptacyjnych wymaga bowiem nie tylko zainstalowania końcowej wersji tworzonego systemu w środowisku użytkownika, ale również dostarczenia szeregu produktów dokumentacyjnych, przeprowadzenia szkoleń dla użytkowników wytypowanych do przeprowadzenia testów oraz przygotowania zespołu helpdesku, do obsługi błędów wykrytych podczas testów. Z formalnego punktu widzenia aby możliwe było rozpoczęcie testów akceptacyjnych, wykonawca zobowiązany jest zgłosić gotowość do testów wraz z dostawą wymaganych produktów i usług wyszczególnionych w protokole dostawy. Działania wykonywane w ramach testów akceptacyjnych oraz wyniki tych działań muszą zostać udokumentowane w raporcie z przebiegu testów. Taki dokument, wstępnie wypełniony danymi, które są znane przed rozpoczęciem testów (m.in. harmonogram testów, dzienniki testów dla zespołów testowych, szablony rejestrów zgłoszeń błędów i raportu końcowego) musi być przekazany użytkownikowi w ramach dostawy. Sam przebieg testów można podzielić na cztery fazy:

- potwierdzenie w raporcie z przebiegu testów spełnienia formalnych, wymaganych warunków rozpoczęcia testów,
- wykonywanie procedur testowych przez zespoły testowe zgodnie z dziennikami testów i rejestrowanie wyników wykonania a w przypadku wykrycia błędów, wprowadzenie stosownych zapisów do rejestrów zgłoszeń błędów,

- uzgadnianie rejestrów zgłoszeń błędów i, po ich uzgodnieniu, przesłanie opisów błędów do zewnętrznego systemu obsługi incydentów,
- wygenerowanie, ewentualne uzupełnienie i uzgodnienie raportu końcowego a następnie, zamknięcie testów.

Celem niniejszej pracy jest przedstawienie koncepcji aplikacji, która z jednej strony umożliwiałaby zautomatyzowane tworzenie wstępnie wypełnionych raportów z testów, a z drugiej, zapewniłaby możliwość interaktywnego wypełniania dzienników testów i rejestrów zgłoszeń błędów. Koncepcja zakłada, że stan wykonywania testów będzie utrzymywany we wspólnej bazie danych, co pozwoli kierownikowi testów na bieżącą ocenę przebiegu testów. Ponadto, po wprowadzeniu przez testującego informacji o wystąpieniu błędu podczas wykonywania procedury testowej aplikacja zablokuje możliwość wprowadzenia danych do dzienników testów wszystkich następników tej procedury testowej. Istotnymi funkcjami aplikacji będą: automatyczne generowanie harmonogramu testów, generowanie dzienników testów, protokołu końcowego oraz przekazywanie rejestrów zgłoszeń błędów do systemu JIRA.

A16

Patryk Serafin

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: Patryk.serafin@wat.edu.pl

Model planowania zadań wielordzeniowych uwzględniający zależności

W nowoczesnych wielordzeniowych systemach obliczeniowych, systemy operacyjne są odpowiedzialne za dynamiczne przydzielanie czasu procesora dla wielu współbieżnych zadań. Choć systemowe programy planujące efektywnie zarządzają wysyłaniem wątków w oparciu o priorytety i sprawiedliwość, zazwyczaj nie są one świadome logicznych zależności pomiędzy zadaniami na poziomie aplikacji. W konsekwencji, wątki mogą być uruchamiane przedwcześnie, nawet jeśli muszą czekać na zakończenie innych zadań, co skutkuje bezczynnymi cyklami procesora, rywalizacją zasobów i opóźnionym wykonaniem.
Niniejszy artykuł przedstawia model (Dependency-Aware Model – DAM), który wprowadza zewnętrzną warstwę wykonywania świadomą zależności, która uzupełnia domyślne zachowanie harmonogramu systemu. Proponowany model ocenia, czy wszystkie zadeklarowane zależności danego zadania są spełnione przed wysłaniem go do wykonania. Uruchamiane są tylko te zadania, których zależności są spełnione, co pozwala skutecznie uniknąć scenariuszy, w których wątki są niepotrzebnie aktywne i blokują zasoby procesora w oczekiwaniu na spełnienie warunków wstępnych. Model ten został zaprojektowany do działania niezależnie od wewnętrznych mechanizmów szeregowania systemu operacyjnego i może być stosowany zarówno do statycznie zdefiniowanych, jak i dynamicznie wprowadzanych zestawów zadań. Jego rozwój został oparty na dokładnej analizie zachowania wykonywania wątków, przełączania kontekstu i logiki planowania w środowiskach Windows i Linux, w odniesieniu do ich oficjalnej dokumentacji systemowej. Teoretyczne uzasadnienie tego podejścia opiera się na zasadzie, że zapobieganie uruchamianiu zadań z niespełnionymi zależnościami zmniejsza niepotrzebne zajęcie procesora, szczególnie w środowiskach o wysokiej współbieżności zadań i relacjach między zadaniami. Oczekuje się, że poprzez minimalizację aktywnego oczekiwania i zmniejszenie rywalizacji o zasoby, model ten poprawi ogólną wydajność wykonywania.

A17

Patryk Serafin

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: Patryk.serafin@wat.edu.pl

Środowisko symulacyjne do oceny planowania zadań z uwzględnieniem zależności w systemach wielordzeniowych

Opracowano konfigurowalne środowisko symulacyjne do oceny strategii planowania zadań opartych o model DAM (Dependency-Aware Model) w systemach wielordzeniowych ze złożonymi zależnościami między zadaniami.
Framework składa się z Configuration Loader, Main Controller, Test Runner, Task Generator, DepThread Class i DepRunner Manager i obsługuje zarówno opartą na YAML, jak i losową parametryzację rozkładów czasu wykonania, dynamiki przybycia zadań, prawdopodobieństwa powinowactwa CPU i gęstości zależności z wymuszonymi grafami acyklicznymi. Każde zadanie wykonuje obciążenie związane z obliczeniami, aby narzucić rzeczywiste obciążenie procesora.
Porównywane są dwa modele wykonania: standardowy harmonogram, który uruchamia zadania natychmiast i pozwala na bierne oczekiwanie, oraz model świadomy zależności (DAM), który odracza aktywację do momentu spełnienia wszystkich warunków wstępnych.
Metryki są rejestrowane w formacie CSV i wizualizowane za pomocą wykresu słupkowego wygenerowanego przez matplotlib, pokazującego procentową poprawę wraz z liczbą zależności.
Reprezentatywny, jednostkowy eksperyment pokazuje, że DAM zmniejsza bezczynność procesora i zapewnia znaczny wzrost czasu wykonywania w scenariuszach bogatych w zależności
.

A18

Patryk Serafin

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: Patryk.serafin@wat.edu.pl

Ocena harmonogramowania zadań z uwzględnieniem zależności na dużą skalę za pomocą szeroko zakrojonych prób symulacyjnych

W niniejszym opracowaniu przedstawiono zakrojoną na szeroką skalę ocenę modelu DAM (Dependency-Aware Model) do szeregowania zadań w systemach wielordzeniowych, z wykorzystaniem metodologii opartej na symulacji.
Ocena koncentruje się na weryfikacji zdolności modelu do poprawy wydajności wykonywania poprzez zapobieganie przedwczesnej aktywacji zadań z nierozwiązanymi zależnościami.
Niestandardowe środowisko symulacyjne zostało wykorzystane do przeprowadzenia dziesiątek tysięcy prób, z których każda została skonfigurowana z losowymi parametrami, takimi jak liczba wątków, czas wykonania, prawdopodobieństwo powinowactwa CPU i gęstość zależności.
Symulacja działa przy rzeczywistym obciążeniu procesora i modeluje zarówno statyczne, jak i dynamicznie przybywające zadania, zachowując acykliczny charakter grafów zadań. Dla każdej próby zmierzono wydajność, porównując całkowity czas wykonania harmonogramu kontrolowanego przez DAM ze standardowym harmonogramem.
Wyniki zostały zebrane w ustrukturyzowanym formacie CSV i zwizualizowane za pomocą wykresów słupkowych, podkreślających względne ulepszenia i złożoność zależności. Wyniki wskazują, że proponowany model osiąga znaczny wzrost wydajności w szerokim spektrum konfiguracji, demonstrując jego solidność i skalowalność w obsłudze obciążeń zależnych od zależności.

A19

Michał Sobolewski, Tadeusz Nowicki, Paweł Pieczonka, Robert Waszkowski

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: michal.sobolewski@wat.edu.pl

Sposoby zobrazowania przebiegu i wyników obliczeń algorytmów genetycznych

Zobrazowanie wybranych charakterystyk przebiegu procesu, w którym realizuje się algorytm genetyczny, związane jest z organizacją struktur danych oraz z projektem i implementacją interfejsu graficznego. Wizualizacja danych odgrywa kluczową rolę w procesie analizy, ponieważ umożliwia intuicyjne uchwycenie wzorców i zależności, które mogą być trudne do zauważenia w postaci surowych danych liczbowych. Odpowiednio zaprojektowane wizualizacje pozwalają ocenić przebieg działania algorytmu, zidentyfikować potencjalne problemy oraz wspierają podejmowanie decyzji dotyczących modyfikacji parametrów lub struktury algorytmu.

Dane przedstawione graficznie mogą również wpływać na sposób ich postrzegania. Ułatwiają wtedy zrozumienie złożonych procesów, zwiększają czytelność wyników oraz pomagają komunikować efekty eksperymentów nawet osobom niezwiązanym bezpośrednio z implementacją algorytmu. Dzięki temu wizualizacja staje się nie tylko narzędziem analitycznym, ale także elementem wspierającym proces projektowania, kalibracji i prezentacji działania algorytmów genetycznych w szerszym kontekście badawczym i inżynierskim.

W pracy zostanie przedstawiona koncepcja zobrazowania działania algorytmów genetycznych, ze szczególnym uwzględnieniem graficznej interpretacji ich kluczowych charakterystyk. Autorzy koncentrują się na identyfikacji między innymi takich zmiennych, jak: wielkość populacji, liczba iteracji, skuteczność i parametry operatorów mutacji i krzyżowania, jakość oraz różnorodność rozwiązań czy czas trwania obliczeń. Zaprezentowane zostaną sposoby ich graficznego przedstawienia oraz propozycje interpretacji tych wizualizacji w kontekście analizy działania algorytmu. Celem pracy nie jest zaprezentowanie gotowego rozwiązania,

lecz zarysowanie podejścia oraz projektu i wybranych elementów implementacji, które mogą stanowić podstawę do budowy środowisk programowanych wspomagających projektowanie i kalibrację algorytmów genetycznych. Graficzne ujęcie przebiegu obliczeń ma ułatwić identyfikację zależności między parametrami, a skutecznością działania algorytmu oraz umożliwić porównywanie jego wariantów w ramach eksperymentów symulacyjnych.

A20

Jerzy Stanik

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: jerzy.stanik@wat.edu.pl

Rola certyfikowanego SZBI w zapewnianiu zgodności w cyberbezpieczeństwie

W dzisiejszym dynamicznie rozwijającym się środowisku cyfrowym, cyberbezpieczeństwo stało się kluczowym elementem strategii zarządzania ryzykiem w organizacjach. Certyfikowany System Zarządzania Bezpieczeństwem Informacji (SZBI), zgodny z normą ISO 27001, odgrywa istotną rolę w zapewnianiu zgodności z regulacjami prawnymi oraz standardami branżowymi, takimi jak RODO, NIS 2, DGA, DORA oraz akty cyberbezpieczeństwa. Pomimo rosnącego znaczenia SZBI, istnieje ograniczona liczba badań dotyczących praktycznych aspektów jego wdrożenia i utrzymania w kontekście zgodności z wymogami cyberbezpieczeństwa. Problem badawczy dotyczy identyfikacji korzyści i wyzwań związanych z certyfikacją SZBI oraz jej wpływu na zgodność z regulacjami prawnymi. Celem artykułu jest analiza znaczenia certyfikowanego SZBI w kontekście budowy zgodności w cyberbezpieczeństwie, przedstawienie korzyści wynikających z jego wdrożenia oraz wyzwań związanych z utrzymaniem certyfikacji. Artykuł opiera się na przeglądzie literatury oraz studium przypadku, które ilustruje praktyczne zastosowanie certyfikowanego SZBI w organizacji. Przeprowadzono analizę dokumentów, wywiady z ekspertami oraz audyty wewnętrzne, aby uzyskać kompleksowy obraz funkcjonowania SZBI. Wyniki badań wskazują, że certyfikowany SZBI znacząco poprawia zarządzanie ryzykiem, zwiększa efektywność operacyjną oraz redukuje koszty związane z incydentami bezpieczeństwa. Certyfikowany SZBI umożliwia również lepsze przygotowanie organizacji na audyty zewnętrzne oraz zgodność z regulacjami prawnymi, takimi jak RODO, NIS 2, DGA oraz DORA. Wyzwania związane z utrzymaniem certyfikacji obejmują konieczność ciągłego doskonalenia procesów bezpieczeństwa informacji, zaangażowanie kadry zarządzającej, opór wśród pracowników oraz wysokie koszty wdrożenia i utrzymania systemu. Aby skutecznie

budować i zapewniać zgodność w cyberbezpieczeństwie, organizacje powinny skupić się na kilku kluczowych aspektach. Po pierwsze, pełne zaangażowanie najwyższego kierownictwa jest niezbędne do skutecznego zarządzania bezpieczeństwem informacji. Kierownictwo powinno aktywnie wspierać inicjatywy związane z cyberbezpieczeństwem oraz promować kulturę bezpieczeństwa w całej organizacji. Po drugie, regularne szkolenia i podnoszenie świadomości pracowników na temat znaczenia bezpieczeństwa informacji są kluczowe. Pracownicy powinni być świadomi zagrożeń oraz procedur, które mają na celu ochronę danych. Szkolenia powinny być dostosowane do różnych poziomów wiedzy i odpowiedzialności w organizacji. Po trzecie, inwestowanie w odpowiednie technologie i narzędzia wspierające zarządzanie ryzykiem i bezpieczeństwem informacji jest niezbędne. Organizacje powinny korzystać z najnowszych rozwiązań technologicznych, aby skutecznie chronić swoje zasoby informacyjne przed zagrożeniami. Po czwarte, regularne przeprowadzanie audytów wewnętrznych i zewnętrznych jest kluczowe dla monitorowania zgod-ności z normami i standardami. Audyty pozwalają na identyfikację słabych punktów oraz wdrożenie działań naprawczych, które poprawiają poziom bezpieczeństwa informacji. Na koniec, ciągłe doskonalenie procesów i procedur związanych z zarządzaniem bezpieczeństwem informacji jest niezbędne, aby dostosować się do zmieniających się zagrożeń i wymagań regulacyjnych. Organizacje powinny być elastyczne i gotowe na wprowadzanie zmian, które zwiększą poziom ochrony danych. Artykuł składa się z kilku kluczowych części. Wprowadzenie przedstawia tło i cel badania, podkreślając znaczenie certyfikowanego SZBI w kontekście cyberbezpieczeństwa. Przegląd literatury analizuje istniejące badania i teorie dotyczące SZBI oraz zgodności z regulacjami prawnymi. Metodologia opisuje zastosowane metody badawcze, w tym analizę dokumentów, wywiady z ekspertami oraz audyty wewnętrzne. Wyniki badań prezentują główne odkrycia dotyczące korzyści i wyzwań związanych z certyfikowanym SZBI. Dyskusja interpretuje wyniki, porównując je z wcześniejszymi badaniami i wskazując na praktyczne implikacje. Studium przypadku ilustruje praktyczne zastosowanie SZBI w organizacji. Wnioski podsumowują główne ustalenia, podkreślając znaczenie certyfikowanego SZBI w cyberbezpieczeństwie oraz przedstawiają rekomendacje dla przyszłych badań i praktyk.

A21

Piotr Stąpor, Ryszard Antkiewicz

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: piotr.stapor@wat.edu.pl

Metoda oceny odporności podmiotów krytycznych

Przedmiotem pracy jest metoda oceny odporności podmiotów krytycznych na występowanie różnych zagrożeń. Podmiotem krytycznym, zgodnie z Dyrektywą Parlamentu Europejskiego I Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych, nazywa się „podmiot (…), świadczący co najmniej jedną usługę kluczową", czyli taką, „która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska". Odporność definiowana jest jako „zdolność podmiotu (…) do zapobiegania incydentowi, ochrony przed nim, odpowiedzi na niego, stawiania mu oporu, łagodzenia i absorbowania incydentu oraz adaptacji i odtworzenia po incydencie". Incydent zaś, to „zdarzenie, które może znacząco zakłócić lub które zakłóca świadczenie usługi kluczowej, w tym, gdy wpływa ono na krajowe systemy chroniące praworządność". Infrastruktura krytyczna „oznacza składnik, obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci lub systemu, niezbędne do świadczenia usługi kluczowej". Jednym z najtrudniejszych problemów w ochronie infrastruktury krytycznej jest ocena i łagodzenie skutków kaskadowych awarii infrastruktury krytycznej. Wystąpienie incydentu powoduje obniżenie poziomu dostarczanej usługi, a tym samym może obniżyć zdolności innych infrastruktur do świadczenia usług. Niniejsza praca, prezentuje symulacyjno–analityczną metodę oceny odporności infrastruktur krytycznych na występowanie incydentów. Podmioty krytyczne zostały podzielone na: producentów – zdolnych przetwarzać usługi otrzymane od pozostałych wytwórców w usługi nowego rodzaju oraz kluczowych odbiorców, których zaopatrzenie jest niezbędne. Każdego z producentów cechuje różny stopień efektywności, poziom maksymalnej zdolności produkcyjnej, a także zakres możliwych odbiorców wytwarzanej przez niego usługi. Stan sprawności każdego z podmiotów – producentów został

opisany dyskretnym w czasie modelem stochastycznym. Odporność systemu powiązanych podmiotów krytycznych mierzona jest z wykorzystaniem wskaźników, których wartości są estymowane na podstawie eksperymentów symulacyjnych. W procesie symulacji wykorzystywane są dwa zadania optymalizacji alokacji usług krytycznych. Pierwsze zakłada pełną sprawność wszystkich podmiotów i możliwości pełnego zaspokojenia wszystkich zapotrzebowań. Funkcją celu jest tu koszt dostarczania usług. W przypadku wystąpienia incydentu, rozwiązywane jest zadnie minimalizujące zarówno stopień niezaspokojenia usług jak i koszt ich dostarczania. To podejście stanowi innowację, w stosunku do innych modeli symulacyjnych. W pracy zaprezentowano model matematyczny, model symulacyjny zadania optymalizacji wraz z metodami ich rozwiazywania. Przedstawiono również wyniki przeprowadzonych eksperymentów symulacyjnych. Dalszy rozwój zakłada zdefiniowanie problemu predykcji występowania awarii oraz wprowadzenie do modelu rezerw. Przewiduje się również uwzględnienie modelu przestrzennego, z uwzględnieniem „incydentów wspólnych" dotyczących wielu podmiotów, o podobnej lokalizacji (np. powódź).

A22

Przemysław Szatan, Szymon Winczewski

Politechnika Gadańska
Narutowicza 11/12, 80-233 Gdańsk
e–mail: maciejwisniewski2@mon.gov.pl

Simulations of chemical vapor deposition of a graphene layer on a copper substrate

Graphene's exceptional mechanical, thermal, and electronic properties [1 - 3] make it
a highly attractive material for numerous applications [4, 5]. Among the available synthesis techniques, chemical vapor deposition (CVD) on copper substrates is one of the most promising methods for producing high-quality graphene on a large scale. [6] However, modeling this process at the atomistic level with limited time and computational resources makes simulation infeasible. Combining molecular dynamics (MD) time-stamped force-bias Monte Carlo (tfMC) with an appropriate interatomic interaction description enables the simulation of fast atomic collisions and slower surface relaxation processes.

This work used a hybrid simulation method (MD + tfMC), proposed by Winczewski et al. [7], to investigate the CVD growth of graphene from atomic carbon on a Cu(111) substrate under various temperatures (500 K, 900 K, and 1300 K). Additionally, including the energy and angular distributions of the incident atoms allowed for more accurate modeling of the deposition process.

The simulations demonstrate that the hybrid method successfully captures key stages of graphene formation, including nucleation, grain merging, and the development of long-range sp^2 hybridized domains. The temperature significantly influences both the growth kinetics and structural order. Higher temperatures promote the formation of well-ordered monolayers, while lower temperatures facilitate faster growth but result in more structural defects. The results align well with experimental trends reported in the literature, especially with respect to temperature-dependent coverage.

To validate the efficacy of tfMC in accelerating time evolution, additional simulations were executed where both the deposition and relaxation were handled by MD. Despite the theoretical advantage of tfMC in sampling slow relaxation processes, the time gain was marginal in practice. This finding provides critical insights into the method's limitations.

A23

Kamil Wacławik, Norbert Waszkowiak

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: kamil.waclawik@wat.edu.pl

Symulatory i trenażery w zastosowaniach szkoleniowych z wykorzystaniem sprzętu do symulacji wirtualnej i poszerzonej

W wystąpieniu zaprezentowane zostały możliwości szkolenia wojsk w zakresie działań na polu walki z wykorzystaniem wirtualnej symulacji.
Dostępny w zasobach Akademii sprzęt oraz oprogramowanie symulacyjne pozwala na realizacje szkolenia w wielu kluczowych aspektach pola walki, redukując diametralnie koszty, ograniczając resurs uzbrojenia i straty sprzętowe.
Wykorzystanie okularów VR, platform ruchu oraz zintegrowanych środowisk symulacyjnych pozwala na wierne odtworzenie misji bojowych, szkolenie aspektów niemożliwych do realizacji w czasie pokoju oraz przeprowadzenie zadań z współdziałania wielu rodzajów wojsk. Symulacja może być zrealizowana na obszarach dokładnie odtworzonych w środowisku wirtualnym, wyjątkowo ważnych ze względów bezpieczeństwa i obronności państwa.

A24

Szymon Winczewski

Politechnika Gadańska
Narutowicza 11/12, 80-233 Gdańsk
e–mail: szywincz@pg.edu.pl

A novel method for realistically simulating the deposition of thin films from the gas phase

Properties of thin films (TFs) often differ considerably from those of bulk materials of the same composition. By offering new functionalities and capabilities, TFs find applications in many areas, such as electronics, optics, and electrochemistry, attracting continuously growing attention.
Physical vapour deposition (PVD) is a widely used technique for fabricating TFs. It is known that the properties of a TF strongly depend on how the deposition process is carried out. However, the limitations of experimental techniques prevent a better understanding of the mechanisms governing the deposition of very thin films. This, in turn, hinders the understanding of how the parameters of the manufacturing process translate into the characteristics of the produced TF and its resultant properties.
Atomistic simulations constitute an indispensable tool for predicting the behaviour of matter and interpreting experimental observations. The molecular dynamics (MD) method permits prediction of the time evolution of an interacting atomic system and, therefore, constitutes a powerful tool for studying deposition from the gas phase. In fact, the MD method has already been used many times for simulating PVD [1–4]. However, the deposition simulations carried out to date have a number of limitations. The most important are the use of extremely high deposition rates — exceeding those used in experiments by several orders of magnitude — and the lack of adequate accounting for long-time relaxation, which occurs in the growing TF as a result of, e.g., diffusion.
During the talk, we will present a new approach [5] that solves the above problems, allowing for a more realistic simulation of the deposition of thin films from the gas phase. The developed method combines two simulation techniques: MD and time-stamped force-bias Monte Carlo (tfMC) [6, 7]. Within the proposed simulation protocol, MD is used to simulate the

collisions of incident atoms with the substrate and to model the fast relaxation occurring immediately after the collisions. tfMC is used to simulate long-time relaxation, significantly extending the time scale. The proposed approach also accounts for other aspects essential for realistic modelling of deposition. Among others, the energies and angles of the incident atoms follow realistic distributions known from theory and experiments.

The proposed method was implemented from scratch and applied to simulate the growth of a thin (3 nm thick) Au film on the dc-Si (001) substrate. The use of the tfMC method allowed reaching the microsecond scale in the simulation, obtaining a deposition rate that was three orders of magnitude lower than those used by other authors [1–4]. Consequently, the carried-out simulation provided a much more realistic TF. This was confirmed by a detailed analysis, which showed that the TF obtained from the hybrid MD+tfMC simulation has much lower energy and is more ordered than the TF obtained from purely MD simulations. The carried-out simulations also allowed characterization of the growth process. It was found that the deposition of Au on crystalline Si consists of four distinct stages: (i) initial degradation of the Si substrate, (ii) formation of a mixed Au–Si interface layer, (iii) nucleation and growth of a polycrystalline Au layer, proceeding in a fashion close to the Frank–van der Merwe mode (layer-by-layer growth), and (iv) post-deposition relaxation of the microstructure.

A25

Maciej Wiśniewski, Szymon Rosowski, Paweł Hołownia, Paweł Moszczyński

Wojskowa Akademia Techniczna, Wydział Cybernetyki
ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e–mail: maciejwisniewski2@mon.gov.pl

Narzędzie AI do generowania wykładów

W dobie dynamicznego rozwoju sztucznej inteligencji rośnie znaczenie jej zastosowań w edukacji, szczególnie w kontekście personalizacji procesu nauczania, która umożliwia dostosowanie tempa, treści oraz formy przekazu do indywidualnych potrzeb i stylu uczenia się każdego ucznia. Tendencję tę ilustruje eksperyment przeprowadzony podczas Certyfikowanego Programu Edukacyjnego „Sztuczna Inteligencja i Cyberbezpieczeństwo w nowoczesnych Siłach Zbrojnych", który odbył się w dniach 16–17 kwietnia 2025 r. w Wojskowej Akademii Technicznej. W jego ramach zaprezentowano wykład wygenerowany przez narzędzie AI opracowane przez Koło Zainteresowań Cybernetycznych Wydziału Cybernetyki. Zastosowane rozwiązanie wykorzystuje architekturę agentową wspieraną przez mechanizm RAG (Retrieval-Augmented Generation), umożliwiający dynamiczne dostosowywanie treści do konkretnych zapytań użytkowników, co stanowi przykład praktycznego wykorzystania AI w środowisku edukacyjnym.
Celem eksperymentu było porównanie efektywności dwóch form przekazu wiedzy: wykładu ogólnego oraz wykładu dostosowanego dynamicznie do pytań i potrzeb uczestników. Analiza wyników sprawdzianów wykazała wyraźną przewagę formy spersonalizowanej, co wskazuje na realny potencjał adaptacyjnych technologii AI w poprawie skuteczności nauczania. W artykule została omówiona metodologia eksperymentu oraz wnioski i perspektywy dalszych prac nad zastosowaniem sztucznej inteligencji w edukacji wojskowej i cywilnej.

Wydawca:
Politechnika Gdańska
w porozumieniu z
Polskie Towarzystwo Symulacji Komputerowej

e-ISBN : 978-83-974103-0-5