https://doi.org/10.4467/27204383TER.23.017.18319

https://orcid.org/0000-0002-5288-0324
https://orcid.org/0000-0002-3907-2242
https://orcid.org/0000-0001-6390-1402

TOMASZ P. MICHALAK
MICHAŁ T. GODZISZEWSKI
ANDRZEJ NAGÓRKO

Ochrona infrastruktury krytycznej z wykorzystaniem teorii gier, technik optymalizacji i algorytmów sztucznej inteligencji

Abstrakt

Aktualna sytuacja geopolityczna doprowadziła do wzrostu zagrożeń, z jakimi muszą się mierzyć podmioty odpowiedzialne za bezpieczeństwo w Polsce i Europie. Jednak pomimo zwiększenia czujności, poziomu nakładów i inwestycji zasoby ochrony wciąż pozostają ograniczone w stosunku do dynamicznie rosnących potrzeb. Taka sytuacja sprawia, że stała ochrona każdego potencjalnego celu ataku jest po prostu nieosiągalna. Kluczowe staje się zatem efektywne wykorzystanie już istniejących zasobów ochrony. Przedmiotem niniejszego artykułu jest omówienie zaawansowanych metod, które ułatwiają zautomatyzowane podejmowanie decyzji w zakresie alokacji zasobów bezpieczeństwa. Tego rodzaju metody obejmują wykorzystanie sztucznej inteligencji,

Słowa kluczowe:

optymalizacja,
gry bezpieczeństwa,
sztuczna inteligencja,
infrastruktura krytyczna

teorii gier oraz technik optymalizacji. Wdrożenia podobnych rozwiązań w zakresie ochrony wybranych obiektów infrastruktury krytycznej w Stanach Zjednoczonych Ameryki dowodzą ich skuteczności. W artykule został przedstawiony również skrócony przegląd tego obszaru badań oraz rozwiązania i oprogramowanie opracowane przez zespół „AI dla bezpieczeństwa" utworzony w ramach instytutu badawczego IDEAS NCBR w celu ochrony infrastruktury krytycznej w Polsce i Europie.

Wprowadzenie

Międzynarodowe lotnisko w Los Angeles (ang. Los Angeles International Airport, LAX) jest jednym z największych i najbardziej ruchliwych portów lotniczych na świecie. Stanowi ważny węzeł komunikacyjny dla tej aglomeracji i jej okolic. Pod względem liczby pasażerów jest ok. czterokrotnie większe od Lotniska Chopina w Warszawie – największego polskiego portu lotniczego. Lotnisko LAX zajmuje rozległy obszar i ma cztery równoległe pasy startowe oraz dziewięć terminali, z których każdy obsługuje różne linie lotnicze i miejsca docelowe. Największym z nich jest Tom Bradley International Terminal przeznaczony do obsługi lotów międzynarodowych. Centralny obszar terminalu jest jednocześnie środkowym węzłem ciągów komunikacyjnych łączących wszystkie terminale. Obejmuje on złożoną sieć dróg, parkingów oraz usług transportowych, takich jak transport wahadłowy i taksówki, których celem jest ułatwienie pasażerom poruszania się po lotnisku.

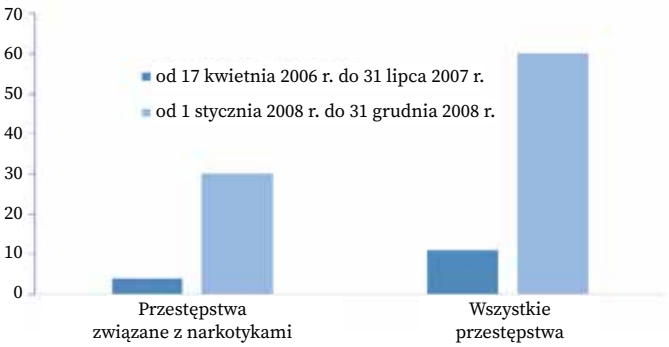
Z uwagi na znaczenie i rozmiar LAX jest jednym z głównych obiektów na Zachodnim Wybrzeżu USA, które są zagrożone potencjalnym atakiem. Ochrona tak złożonego i rozległego obiektu rodzi konieczność zachowania równowagi między środkami bezpieczeństwa a wydajnością operacyjną. Niestety, całodobowa ochrona każdego ważnego obszaru jest niewykonalna ze względu na ograniczone zasoby bezpieczeństwa, którymi dysponuje lotnisko. Jako przykład można wskazać psy służbowe o konkretnej specjalizacji, np. psy mające umiejętność wykrywania materiałów wybuchowych lub narkotyków. Ich liczba jest zawsze za mała w stosunku do potrzeb i stanowczo za mała, aby można było patrolować przez cały czas

wszystkie newralgiczne punkty lotniska. W praktyce oznacza to, że zapewnienie stałej obecności patroli z psami służbowymi na każdym terminalu w LAX jest po prostu niemożliwe. Mimo to patrole z psami szkolonymi do wykrywania narkotyków okazały się w 2008 r. znacznie skuteczniejsze niż w latach poprzednich. Przez 15 miesięcy, tj. od kwietnia 2006 r. do lipca 2007 r., odnotowano tylko cztery przestępstwa związane z narkotykami, a w ciągu 2008 r. – 30 takich czynów.

U źródeł tak dużej poprawy wykrywalności leży system ARMOR (ang. *Assistant for Randomized Monitoring Over Routes*, pol. asystent randomizowanego monitorowania ciągów komunikacyjnych). Jest to innowacyjne narzędzie programistyczne opracowane przez Milinda Tambego i współpracowników z Uniwersytetu Południowej Kalifornii (ang. University of Southern California)[1], w ramach pierwszego Uniwersyteckiego Centrum Doskonałości wspieranego przez Departament Bezpieczeństwa Wewnętrznego (ang. University Center of Excellence at the Department of Homeland Security). Głównym celem systemu ARMOR jest udzielanie pracownikom ochrony wsparcia, aby mogli podejmować lepsze i bardziej efektywne decyzje dzięki zoptymalizowaniu użycia dostępnych zasobów z uwzględnieniem posiadanej oceny ryzyka. W tym celu ARMOR wykorzystuje sztuczną inteligencję (ang. *Artificial Intelligence*, AI), teorię gier oraz techniki optymalizacji. System pozwala siłom bezpieczeństwa na rozmieszczenie ich ograniczonych zasobów w najbardziej efektywny sposób i osiągnięcie maksymalnej skuteczności. Utrudnia to przeciwnikowi takie zaprojektowanie ataku, aby przedostać się przez istniejące systemy bezpieczeństwa.

Wdrożenie systemu ARMOR na lotnisku LAX zaowocowało poprawą poziomu ochrony, zwiększeniem wydajności alokacji zasobów oraz ograniczyło możliwości potencjalnych agresorów. Jego wprowadzenie spowodowało ponadtrzykrotny wzrost liczby wszystkich wykrytych przestępstw (wykres). System ten jest przykładem tego, jak zaawansowana technologia i podejścia oparte na sztucznej inteligencji mogą przyczynić się do zwiększenia poziomu bezpieczeństwa lotnisk oraz przebywających na nich pasażerów.

[1] J. Pita i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57. https://doi.org/10.1609/aimag.v30i1.2173.



Wykres. Liczba wykrytych przestępstw, w tym tych związanych z narkotykami, na lotnisku LAX w Los Angeles w okresie 15 miesięcy przed wprowadzeniem (ciemne słupki) i 12 miesięcy po wprowadzeniu (jasne słupki) systemu ARMOR.

Źródło: opracowanie własne na podstawie: J. Pita i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57.

Sukces, jaki przyniosło zastosowanie ARMOR, wzbudził duże zainteresowanie. Kilka systemów opartych na podobnych zasadach zostało wdrożonych w USA w celu ochrony innych obiektów infrastruktury krytycznej. Są to:

- IRIS[2] – służący do optymalizacji tras i harmonogramu ochrony w ramach programu U.S. Air Marshals (pracownicy służb bezpieczeństwa zatrudnieni na pokładach samolotów);
- PROTECT[3] – służący do optymalizacji bezpieczeństwa portów i wybrzeży w Bostonie i Nowym Jorku;
- TRUSTS[4] – stworzony w celu zapobiegania wyłudzeniom przejazdów i przeznaczony dla systemu transportu kolejowego w Los Angeles.

[2] J. Tsai i in., *Iris – a tool for strategic security allocation in transportation networks*, w: *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2009), s. 37–44 (materiały z poszczególnych konferencji AAMAS są dostępne na: https://dl.acm.org/conference/aamas/proceedings – dop. red.).

[3] E. Shieh i in., *Protect: A deployed game theoretic system to protect the ports of the United States*, w: *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2012), t. 1, s. 13–20.

[4] Z. Yin i in., *Trusts: Scheduling randomized patrols for fare inspection in transit systems*, w: *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence* (AAAI 2012), t. 26, nr 2, s. 2348–2355 (materiały z poszczególnych konferencji i sympozjów AAAI są dostępne na: https://aaai.org/aaai-publications/aaai-conference-proceedings/ – dop. red.).

Wykorzystanie systemu ARMOR jest zalecane również w obszarze cyberbezpieczeństwa[5]. Rośnie także liczba jego zastosowań w sferze cywilnej, np. w ochronie zagrożonych gatunków w parkach narodowych (systemy PAWS[6] i MIDAS[7]). We wszystkich przedstawionych przypadkach znacznie zwiększono poziom bezpieczeństwa, jednak nie przez wprowadzenie dodatkowych środków bezpieczeństwa, a dzięki lepszemu wykorzystaniu już istniejących zasobów.

Jest to ważna lekcja dla Europy, a zwłaszcza dla Polski. Z uwagi na niedawne wydarzenia geopolityczne, przede wszystkim rosyjską pełnoskalową inwazję na Ukrainę w lutym 2022 r., rosną obawy dotyczące bezpieczeństwa infrastruktury. Europa doświadczyła już kilku takich ataków[8]. Z tego względu pytaniem, które należy sobie zadać, nie jest to, czy kolejne ataki nastąpią, lecz to, kiedy do nich dojdzie.

Niestety, problem ochrony przed atakami pogłębia się ze względu na poziom zaawansowania technologicznego infrastruktury krytycznej. Nowoczesne technologie komunikacyjne, obliczeniowe i kontrolne poprawiają wydajność, ale jednocześnie zwiększają poziom skomplikowania istniejących systemów, jak również ich podatność na celowe ataki i przypadkowe awarie. Tego rodzaju ataki mogą przybierać różne formy, mieć różne nasilenie i skalę – od zamachów terrorystycznych wymierzonych w infrastrukturę lokalną po poważne ataki kinetyczne w czasie wojny, takie, do jakich dochodzi podczas trwającej od 2022 r. rosyjskiej inwazji na Ukrainę. Nowe technologie, takie jak drony, również zwiększają możliwości potencjalnych napastników.

W obliczu ewoluującego i rozszerzającego się katalogu zagrożeń, pomimo zwiększonego zainteresowania bezpieczeństwem infrastruktury i nowych inwestycji w tej sferze, zasoby bezpieczeństwa pozostaną ograniczone. To uniemożliwia zapewnienie stałej ochrony wszystkich obiektów.

---

5 Y. Zhang, P. Malacaria, *Bayesian Stackelberg games for cyber-security decision support*, „Decision Support Systems" 2021, t. 148, art. 113599. https://doi.org/10.1016/j.dss.2021.113599.

6 R. Yang i in., *Adaptive resource allocation for wildlife protection against illegal poachers*, w: *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2014), s. 453–460.

7 W. Haskell i in., *Robust protection of fisheries with COmPASS*, w: *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence* (AAAI 2014), t. 28, nr 2, s. 2978–2983.

8 Na przykład celowe przecięcie 8 października 2022 r. dwóch światłowodów systemu komunikacji Deutsche Bahn, które wstrzymało ruch kolejowy w północnych Niemczech na ok. trzy godziny.

W związku z tym strategiczna alokacja zasobów bezpieczeństwa staje się koniecznością. Przykład lotniska LAX oraz inne wspomniane wcześniej przykłady z USA pokazują, że takie dobrze zaprojektowane, strategiczne podejmowanie decyzji jest niezwykle korzystne, a co najważniejsze – znacznie poprawia bezpieczeństwo.

W niniejszym artykule omówiono podstawy zaawansowanych metod ochrony infrastruktury krytycznej, dokonano krótkiego przeglądu badań prowadzonych w tym obszarze, a następnie przedstawiono rozwiązania i oprogramowanie opracowywane przez zespół „AI dla bezpieczeństwa" z instytutu badawczego IDEAS NCBR.

Gry bezpieczeństwa – obrońca kontra atakujący

Teoria gier bada interakcje pomiędzy inteligentnymi podmiotami, takimi jak jednostki, firmy czy państwa. W rozważanym kontekście te podmioty mogą reprezentować „obrońców", np. siły bezpieczeństwa, policję, wojsko, oraz „napastników", np. przestępców, terrorystów czy aktorów państwowych. Podejścia oparte na teorii gier pomagają zrozumieć, w jaki sposób strony wchodzą w interakcje, przy założeniu, że postępują racjonalnie (co najmniej w pewnym stopniu), mają zdolność przewidywania i mogą reagować na wrogie działania. Dzięki wykorzystaniu teorii gier można opracować strategię efektywnej dystrybucji ograniczonych zasobów bezpieczeństwa w celu ochrony infrastruktury krytycznej, przy czym to podejście pozwala uwzględnić znaczenie różnych celów oraz sposób, w jaki przeciwnicy mogą reagować na określone strategie ochrony.

Gra niekooperacyjna jest definiowana przez zbiór graczy, zbiór strategii dla każdego gracza i funkcję użyteczności, która przypisuje każdemu graczowi wypłatę dla każdej kombinacji strategii. Każdej grze towarzyszą zasady, np. taka, zgodnie z którą gracze poruszają się jednocześnie lub sekwencyjnie.

W tabeli 1 przedstawiono przykładową grę opisaną w publikacji Pity i in.[9] W tym przypadku przedstawiono dwóch graczy, z których każdy ma dwie strategie do wyboru: $\{A,B\}$ oraz odpowiednio $\{C,D\}$. Wartości funkcji użyteczności są określone przez pary liczb wskazane w macierzy, w której każda komórka odpowiada danej kombinacji strategii. Dla przykładu, jeżeli

[9] J. Pita i in., *Using game theory for Los Angeles Airport...*

gracz 1 stosuje strategię *A*, gracz 2 stosuje strategię *C*, gracz 1 otrzymuje wypłatę 2, a gracz 2 otrzymuje wypłatę 1.

W niektórych przypadkach istnieje możliwość określenia, w jaki sposób racjonalni gracze (gdzie racjonalność jest eksplikowana za pomocą ścisłej matematycznej formuły) faktycznie graliby w grę, uwzględniając jej zasady. Tego rodzaju kombinację strategii graczy nazywa się równowagą gry. Niewątpliwie najbardziej rozpowszechnioną koncepcją równowagi jest równowaga Nasha (ang. *Nash equilibrium*). Kombinacja strategii będzie stanowiła równowagę Nasha, w przypadku gdy żaden z graczy nie będzie dążył do zmiany swojej strategii, przy założeniu, że strategie wybrane przez przeciwników pozostaną niezmienione. Na przykład kombinacja strategii przedstawiona w tabeli 1 (*A*,*D*) nie może zostać określona jako równowaga Nasha, gdyż gracz 2 chciałby zmienić swoją strategię z *D* na *C*, przy założeniu, że gracz 1 trzyma się strategii *A*. I odwrotnie, kombinacja strategii (*A*,*C*) będzie traktowana jako równowaga w rozumieniu Nasha, ponieważ dla gracza 1 najlepszą strategią będzie *A*, w przypadku gdy gracz 2 działa na zasadzie *C*, a dla gracza 2 najlepszą strategią będzie *C*, jeśli gracz 1 gra *A*.

Tabela 1. Macierz wypłat dla przykładowej gry.

		Gracz 2	
		C	*D*
Gracz 1	*A*	(2,1)	(4,0)
	B	(1,0)	(3,2)

Źródło: J. Pita i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57.

W ramach gry niekooperacyjnej gracze nie muszą się ograniczać do pojedynczych strategii. Zamiast wybrać jedną strategię z pewnością (tj. z prawdopodobieństwem równym 1), gracz może wybrać jedną strategię z określonym (niezerowym i niestuprocentowym) prawdopodobieństwem lub inną strategię z innym (lub takim samym) prawdopodobieństwem (także niezerowym i niestuprocentowym) itd. Innymi słowy gracze mogą przypisać prawdopodobieństwo każdej dostępnej strategii. Na przykład gracz 1 może wybrać strategię *A* z określonym prawdopodobieństwem, oznaczonym jako *p*, oraz strategię *B* z prawdopodobieństwem 1 – *p*. Analogicznie, gracz 2 może przypisać prawdopodobieństwa do strategii *C* oraz *D*. Stosując powyższe tzw. strategie mieszane, gracze wprowadzają element losowości

do własnego procesu decyzyjnego. Pojęcie równowagi Nasha rozszerza się także do gier w strategiach mieszanych.

Rozważmy grę z macierzą wypłat określoną w tabeli 2.

Tabela 2. Przykład macierzy wypłat dla gry bez zachowania równowagi Nasha w przypadku przyjęcia niezmienionych strategii oraz z zachowaniem równowagi Nasha w przypadku strategii mieszanych.

		Gracz 2	
		C	*D*
Gracz 1	*A*	(2,1)	(1,2)
	B	(1,2)	(3,1)

W niniejszej grze nie istnieje równowaga Nasha w strategiach czystych, ponieważ każdy profil strategii charakteryzuje się tym, że któryś gracz – przy ustaleniu strategii drugiego gracza – osiągałby wyższą wypłatę, gdyby zmienił swoją strategię. Istnieje jednak równowaga Nasha w strategiach mieszanych:

- strategia mieszana gracza 1: *A* z prawdopodobieństwem $\frac{1}{2}$, *B* z prawdopodobieństwem $\frac{1}{2}$;
- strategia mieszana gracza 2: *C* z prawdopodobieństwem $\frac{2}{3}$, *D* z prawdopodobieństwem $\frac{1}{3}$.

Oczekiwana wypłata dla gracza 1 w stanie równowagi wynosi:

$$\frac{1}{2}\times\frac{2}{3}\times 2+\frac{1}{2}\times\frac{1}{3}\times 1+\frac{1}{2}\times\frac{2}{3}\times 1+\frac{1}{2}\times\frac{1}{3}\times 3=\frac{5}{3}$$

Oczekiwana wypłata dla gracza 2 wynosi:

$$\frac{1}{2}\times\frac{2}{3}\times 1+\frac{1}{2}\times\frac{1}{3}\times 2+\frac{1}{2}\times\frac{2}{3}\times 2+\frac{1}{2}\times\frac{1}{3}\times 1=\frac{3}{2}$$

Powyższy model ma uproszczony charakter. Zwłaszcza w przypadku ochrony infrastruktury krytycznej można zakładać, że gracze nie będą poruszali się jednocześnie. Wynika to z tego, że atakujący może mieć możliwość obserwowania taktyki obronnej (strategii) stosowanej przez obrońcę. W celu rozwiązania tego problemu zostanie rozważony model ekonomiczny zaproponowany przez Heinricha Stackelberga[10], w którym gra toczy się pomiędzy dwoma graczami – liderem i śledzącym. To oznacza, że w przeciwieństwie do poprzedniego przykładu gra Stackelberga jest rozgrywana

[10] H. von Stackelberg, *Marktform und Gleichgewicht*, J. Springer 1934.

w trybie ruchów następujących po sobie sekwencyjnie, a nie wykonywanych jednocześnie. W takim przypadku lider najpierw wybiera strategię, a jego wybór jest obserwowany przez śledzącego, który następnie odpowiednio określa swój własny ruch.

Na model Stackelberga zwrócono szczególną uwagę w aspekcie zastosowań w sferze bezpieczeństwa, ze względu na możliwość uchwycenia za jego pomocą dynamiki interakcji na linii obrońca–atakujący. W tym kontekście gry Stackelberga często są nazywane grami bezpieczeństwa.

Należy wyróżnić następujące własności tego modelu:

- obrońca, który w grze Stackelberga przyjmuje rolę lidera, przydziela ograniczone zasoby bezpieczeństwa do ochrony wyznaczonego zestawu celów. Uznając, że przeciwnicy mają zdolność obserwowania strategii obronnych i wykorzystywania zaobserwowanych wzorców, obrońca w sposób naturalny wybiera strategię mieszaną (losową). Na przykład w przypadku lotniska LAX kadra kierownicza odpowiedzialna za psy patrolowe określała częstotliwość oraz rodzaj patrolu prowadzonego w każdym terminalu w danym tygodniu. Innymi słowy ustalała rozkład prawdopodobieństwa dla każdego typu patrolu we wszystkich terminalach;
- atakujący, działając w grze Stackelberga jako śledzący, obserwuje próbkę z wybranej przez obrońcę strategii, tj. próbkę z rozkładów prawdopodobieństwa odpowiadających wybranej strategii mieszanej. Przyjęcie takiego założenia powoduje wdrożenie ostrożnego i realistycznego scenariusza, w którym zakłada się, że napastnik jest inteligentny i przed opracowaniem i przeprowadzeniem ataku bada infrastrukturę krytyczną oraz jej ochronę;
- po uzyskaniu wiedzy o prawdopodobieństwach wybranych przez broniącego napastnik strategicznie wybiera optymalny dla siebie sposób działania, a następnie odpowiednio wykonuje swój ruch.

Należy podkreślić, że atakujący ma możliwość obserwowania rozkładu prawdopodobieństwa wybranego przez obrońcę, nie ma natomiast możliwości prześledzenia faktycznego ruchu. Dla zilustrowania podanego przykładu można wskazać scenariusz z udziałem amerykańskiej straży przybrzeżnej (ang. United States Coast Guard, USCG) odpowiedzialnej za patrolowanie Zatoki Meksykańskiej w celu zwalczania przemytu narkotyków za pomocą łodzi. Przemytnicy mogą obserwować częstotliwość patroli na określonych obszarach morskich oraz to, jak często łodzie patrolowe zmieniają swój kurs. To oznacza, że atakujący znają rozkład

prawdopodobieństwa. Niemniej jednak nie są w stanie przewidzieć, czy łódź patrolowa w danym momencie zmieni kurs czy też nie. W związku z tym nie mogą czekać, aż łódź patrolowa odpłynie, ponieważ istnieje niezerowe prawdopodobieństwo, że może natychmiast powrócić. Trzeba w tym miejscu ponownie wspomnieć o opartym na grze Stackelberga systemie PROTECT, który został wprowadzony przez USCG w celu zwiększenia bezpieczeństwa portów i wybrzeży (jest używany m.in. przez funkcjonariuszy w Nowym Jorku).

Można stwierdzić, że obrońcy infrastruktury krytycznej znajdują się w niekorzystnej sytuacji, ponieważ poruszają się jako pierwsi (decydują o alokacji zasobów obronnych i rozkładach prawdopodobieństwa strategii czystych), a ich ruch jest obserwowany przez atakującego. Jednak dokładniejsza analiza ujawnia, że to właśnie obrońca, wykonując ruch jako pierwszy, może mieć znaczny wpływ na wybory dokonywane przez atakującego. Upraszczając, to obrońca może zmusić atakującego do wybrania danej strategii, a nie innych.

Dla przykładu rozważmy grę o macierzy wypłat określonej w tabeli 3 i załóżmy, że gracz 1 jest liderem w grze Stackelberga.

Tabela 3. Macierz wypłat dla przykładowej gry.

		Gracz 2	
		C	*D*
Gracz 1	*A*	(1,1)	(3,0)
	B	(0,0)	(2,1)

Źródło: D. Korzhyk i in., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, „Journal of Artificial Intelligence Research" 2011, t. 41, nr 2, s. 297–327.

Należy zwrócić uwagę, że jeśli gracze poruszają się jednocześnie, to jedyną równowagą Nasha (w strategiach czystych – na mocy definicji – każda równowaga Nasha w strategiach czystych jest również równowagą Nasha w strategiach mieszanych) jest profil strategii (A,C), co daje graczowi 1 oczekiwaną wypłatę równą 1. Natomiast jeśli gracz 1 może poruszyć się jako pierwszy, to może wybrać strategię mieszaną polegającą na grze A i B z prawdopodobieństwami $\frac{1}{2}$ zamiast A z prawdopodobieństwem 1 i B z prawdopodobieństwem 0, jak w przypadku równowagi Nasha dla gry jednoczesnej. Wybór dokonany przez lidera sprawia, że śledzący (gracz 2) wybiera

strategię *D* zamiast *C*[11]. W rezultacie, będąc liderem, gracz 1 może uzyskać oczekiwaną wypłatę w wysokości $\frac{5}{2}$ zamiast 1, co stanowi istotną różnicę.

W załączniku A na końcu artykułu zostało przedstawione bardziej sformalizowane wprowadzenie do gier w obszarze bezpieczeństwa.

Gry bezpieczeństwa – wyzwania i podejścia

Podejście oparte na teorii gier opisane w poprzedniej części artykułu ma ugruntowaną pozycję w literaturze. Jednak dopiero w ciągu ostatnich dwóch dekad koncepcje teoriogrowe zostały skutecznie wdrożone w celu ochrony infrastruktury krytycznej. Powodem opóźnień we wdrożeniu były przede wszystkim wyzwania obliczeniowe związane z grami bezpieczeństwa. W tej części artykułu omówiono te wyzwania oraz opisano sposoby, dzięki którym techniki optymalizacji i sztucznej inteligencji stały się skutecznymi narzędziami do ich pokonywania. Ponadto przedstawiono krótki przegląd istniejących kierunków badań nad grami bezpieczeństwa, aby przybliżyć wyzwania związane z opracowywaniem praktycznych i możliwych do zrealizowania rozwiązań.

Wyzwania obliczeniowe

W rzeczywistych zastosowaniach gry Stackelberga stanowią poważne wyzwanie obliczeniowe ze względu na następujące czynniki:

- przestrzenie decyzyjne w złożonych i wielkoskalowych środowiskach infrastruktury krytycznej są ogromne, co oznacza, że liczba możliwych strategii i działań, które mogą zostać podjęte przez graczy, np. obrońców i napastników, może być bardzo duża. Przykładem takiej złożonej infrastruktury jest system metra w Nowym Jorku, będący jedną z największych i najbardziej ruchliwych sieci transportu publicznego na świecie, obsługującą codziennie miliony osób. Ta sieć składa się z ponad 800 mil (1287 km) torów łączących 472 stacje. Istnieją nie tylko różne metody stosowania środków ochrony (tj. ogromna przestrzeń strategii obrońcy), lecz także bardzo szeroki wachlarz możliwości ataku (tj. ogromna przestrzeń strategii atakującego). Tak rozległe przestrzenie decyzyjne

[11] W grach Stackelberga zakłada się, że jeśli śledzący pozostaje bezczynny, remis jest rozstrzygany na korzyść lidera, ponieważ w przeciwnym razie optymalne rozwiązanie przyjmuje się jako źle zdefiniowane.

wymagają efektywnych algorytmów zarówno do ich eksploracji, jak i optymalizacji;
- niepewność i niekompletność informacji na temat intencji, zdolności i działań przeciwników. Istnieją narzędzia teoriogrowe, tzw. bayesowskie gry bezpieczeństwa (ang. *Bayesian security games*, por. załącznik A), które stanowią narzędzie do modelowania powyższej niepewności przy użyciu narzędzi probabilistycznych. Zwiększa to jednak poziom złożoności obliczeniowej problemu;
- rzeczywiste sytuacje są często dynamiczne i stale ewoluują. Przeciwnicy mogą dostosowywać swoje strategie, a obrońcy muszą odpowiednio reagować. Modelowanie i optymalizacja strategii w takich dynamicznych środowiskach wymagają rozwiązywania powtarzających się (wielorundowych) lub sekwencyjnych gier, co dodatkowo zwiększa wyzwania obliczeniowe.

W literaturze naukowej obserwuje się kilka sposobów radzenia sobie z tego rodzaju wyzwaniami obliczeniowymi. Jednym z podstawowych jest zastosowanie metod optymalizacji matematycznej w celu efektywnego rozwiązywania tych gier. Badacze opracowali liczne algorytmy i techniki optymalizacji, które mogą obsługiwać modele gier na dużą skalę i dostarczać rozwiązań w rozsądnych ramach czasowych. Metody optymalizacji wykorzystują strukturę gry w celu zmniejszenia obciążenia obliczeniowego i poprawy efektywności algorytmów. Posiłkują się one zwłaszcza programowaniem matematycznym, programowaniem liniowym, programowaniem całkowitoliczbowym i innymi metodami optymalizacji w celu znalezienia optymalnych strategii i alokacji zasobów.

Ze względu na inherentną złożoność tych gier znalezienie dokładnych rozwiązań dla scenariuszy na dużą skalę jest często niewykonalne. Dlatego badacze i praktycy często opracowują algorytmy służące do obliczeń przybliżonych, aby sprostać wyzwaniom obliczeniowym przy zachowaniu rozsądnego poziomu dokładności.

Narzędziem mogącym odegrać dużą rolę w poprawie efektywności algorytmów optymalizacyjnych są techniki sztucznej inteligencji. Wykorzystywanie jej do optymalizacji algorytmów w ogóle, a zwłaszcza zagadnień optymalizacyjnych, od wielu lat prowadzi do zwiększania stanu wiedzy w zakresie rozwiązywania trudnych problemów obliczeniowych. Sztuczna inteligencja umożliwia lepsze skalowanie istniejących podejść i może być stosowana w wielu różnych kontekstach, m.in. w kontekście gier

optymalizacyjnych[12]. Ponadto modele sztucznej inteligencji mogą szybko i niezawodnie przybliżać wyniki kosztownych procesów obliczeniowych, pozwalając zrobić więcej przy tej samej ilości zasobów. Na przykład przy podejmowaniu decyzji, jaką interwencję zastosować w celu poprawy odporności i bezpieczeństwa, niektóre alternatywy będą dawały mało satysfakcjonujące wyniki. Modele sztucznej inteligencji mogą pomóc szybko i znacznie mniejszym kosztem zidentyfikować takie gorsze interwencje, nawet jeśli weźmie się pod uwagę niepewność związaną z odnajdywaniem rozwiązań przybliżonych. Ten sam rodzaj technik pozwala systemom takim jak AlphaGO na zbadanie ogromnej przestrzeni możliwych działań w ciągu kilku sekund. W kontekście gier bezpieczeństwa techniki te są wykorzystywane np. w systemach przeznaczonych do odstraszania kłusowników[13].

Inną możliwością jest skorzystanie z technik obliczeń równoległych i rozproszonych. Rozkładając obciążenie obliczeniowe na wiele procesorów lub maszyn, można obsługiwać znacznie większe modele gier. W tym przypadku dużą rolę odgrywają postępy w technologii sprzętowej, które poprawiają możliwości realizacji obliczeń równoległych.

Krótki przegląd literatury

Krótki przegląd na temat gier Stackelberga wraz z obrazowymi przykładami można znaleźć w pracy Sinhy i in.[14] Obszerniejszy przegląd aktualnej literatury dotyczącej gier bezpieczeństwa znajduje się w artykule autorstwa Hunta i Zhuanga[15]. W tym przeglądzie zbadano obecny stan wiedzy w zakresie modelowania teoriogrowego dla scenariuszy atakujący–obrońca oraz przeanalizowano literaturę w kontekście najczęstszych obszarów zastosowań, podejścia do modelowania i metody rozwiązywania gier. Dodatkowo wskazano istotne luki w literaturze przedmiotu. Interesująca jest również zawarta w tym artykule szeroka dyskusja na temat przyszłych kierunków

[12] F. Hutter i in., *Boosting Verification by Automatic Tuning of Decision Procedures*, w: *Proceedings of the 19th International Conference on Computer Aided Verification* (CAV 2007), s. 27–34.

[13] S. Gholami i in., *Adversary models account for imperfect crime data: Forecasting and planning against real-world poachers*, w: *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2018), s. 823–831.

[14] A. Sinha i in., *Stackelberg security games: Looking beyond a decade of success*, w*: Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI 2018), s. 5494–5501.

[15] K. Hunt, J. Zhuang, *A review of attacker-defender games: Current state and paths forward*, „European Journal of Operational Research" 2023, w druku. https://doi.org/10.1016/j.ejor.2023.04.009.

badań. Inne obszerne badania dotyczące gier bezpieczeństwa zostały opisane w tekście Fang i Nguyen[16], jak również w innym artykule współautorstwa Nguyen[17], gdzie wskazano, że niektóre instytucje zajmujące się bezpieczeństwem regularnie wykorzystują w ramach procesu decyzyjnego narzędzia oparte na teorii gier w celu optymalizacji alokacji ograniczonych zasobów bezpieczeństwa przeciwko strategicznie działającym przeciwnikom, jak również że unikalne cechy tego rodzaju zastosowań wymagają innowacyjnych rozwiązań w postaci systemów sztucznej inteligencji.

Ważnymi punktami odniesienia na granicy teorii gier i bezpieczeństwa stały się dwie klasyczne już monografie. Książka Tambego[18] koncentruje się na postępie dokonanym w dziedzinie projektowania i analizy algorytmów oraz stosowaniu przez organy rządowe oprogramowania opartego na teorii gier. Z kolei w monografii Bier i Azaieza[19] przedstawiono kompilację prac łączących teorię gier i analizę ryzyka w dziedzinie bezpieczeństwa.

Gry Stackelberga są coraz częściej wykorzystywane do badania szerokiego zakresu zagadnień związanych z bezpieczeństwem – od scenariuszy dotyczących systemów obrony przeciwrakietowej[20], terroryzmu[21], bezpieczeństwa publicznego[22], po bezpieczeństwo sieci komputerowych[23].

Przez ostatnie lata gry bezpieczeństwa były przedmiotem szeroko zakrojonych badań i istnieje obszerna literatura poświęcona różnym problemom z nimi związanym. Przykładem może być model alokacji zasobów,

---

[16] F. Fang, T.H. Nguyen, *Green security games: Apply game theory to addressing green security challenges*, „ACM SIGecom Exchanges" 2016, t. 15, nr 1, s. 78–83. https://doi.org/10.1145/2994501.2994507.

[17] T.H. Nguyen i in., *Towards a science of security games*, w: *Mathematical Sciences with Multidisciplinary Applications*, B. Toni (red.), Springer Cham 2016, s. 347–381.

[18] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*, Cambridge 2011.

[19] V.M. Bier, M.N. Azaiez, *Game Theoretic Risk Analysis of Security Threats*, Springer 2008. https://doi.org/10.1007/978-0-387-87767-9.

[20] G. Brown i in., *A Two-Sided Optimization for Theater Ballistic Missile Defense*, „Operations Research" 2005, t. 53, nr 5, s. 745–763. https://doi.org/10.1287/opre.1050.0231.

[21] T. Sandler, *Terrorism & Game Theory*, „Simulation & Gaming" 2003, t. 34, nr 3, s. 319–337. https://doi.org/10.1177/1046878103255492.

[22] N. Gatti i in., *Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form*, w: *Proceedings of the 2008 conference on ECAI 2008: 18th European Conference on Artificial Intelligence* (ECAI 2008), s. 403–407. https://doi.org/10.3233/978-1-58603-891-5-403.

[23] K-w. Lye, J. Wing, *Game Strategies in Network Security*, „International Journal of Information Security" 2005, t. 4, s. 71–86. https://doi.org/10.1007/s10207-004-0060-x.

w ramach którego np. władze rządowe dążą do optymalizacji przydziału zasobów obronnych między określonymi celami (np. lotniska lub dworce kolejowe), a przeciwnik chce zaatakować niektóre z nich. W artykule autorstwa An i in.[24] przedstawiono opis wspomnianego systemu PROTECT, wykorzystywanego przez USCG do planowania patroli w portach w Bostonie i w Nowym Jorku (zdjęcie). Co najważniejsze, system nie zakłada, że przeciwnicy działają w sposób w pełni racjonalny, co pozwala na tworzenie bardziej realistycznych i skuteczniejszych scenariuszy. Istotne jest także to, że pozytywna ocena zastosowania systemu PROTECT w porcie w Bostonie przyczyniła się do jego wdrożenia również w porcie w Nowym Jorku. Podstawą systemu PROTECT jest właśnie model gry atakujący–obrońca opracowany przez Stackelberga. Zaprojektowanie i wdrożenie tego systemu wymagało poniesienia znacznych nakładów, przeznaczonych m.in. na rozwinięcie teoretycznych podstaw takich zastosowań modelu oraz na jego kompleksową ocenę naukową.

Zdjęcie. System PROTECT został wdrożony przez USCG w celu ochrony trasy promowej Staten Island obsługiwanej przez Departament Transportu miasta Nowy Jork. Na zdjęciu jest widoczna łódź USCG chroniąca jeden z promów.

Warto zauważyć, że istnieje wiele stochastycznych gier Stackelberga, w których zdolności decyzyjne przeciwnika są zmniejszone z powodu tzw. ograniczonej racjonalności. Większość systemów opartych na grach Stackelberga co do zasady opiera się na przyjętym założeniu, zgodnie z którym przeciwnicy są doskonale racjonalni, i taki standard jest opisywany

[24] B. An i in., *A Deployed Quantal Response-Based Patrol Planning System for the U.S. Coast Guard*, „Interfaces" 2013, t. 43, nr 5, s. 400–420. https://doi.org/10.1287/inte.2013.0700.

w literaturze. To założenie może jednak niedokładnie odzwierciedlać zachowania rzeczywistych przeciwników, ponieważ ludzie często postępują w sposób nie w pełni racjonalny. Z tego powodu badacze (np. Yang i in.[25]), czerpiąc inspirację z psychologicznych i behawioralnych modeli ekonomicznych, skupili się na badaniu w tych grach sparametryzowanych modeli ograniczonej racjonalności. Modele te oferują wszechstronne podejście do włączania ograniczonej racjonalności do założeń dowolnej gry, dzięki czemu można je zastosować do szerokiej palety gier wykraczających poza te zdefiniowane przez Stackelberga. Przykładem takiego podejścia jest zastosowanie opisane w pracy Nguyen i in.[26], w którym zamiast wybierać pojedynczy cel jako optymalną odpowiedź na indukowane pokrycie celów przez zasoby obronne (to pokrycie jest oznaczone symbolem C, od ang. *cover*), odpowiedź przeciwnika h(C) pociąga za sobą wybór celu *t* na podstawie prawdopodobieństwa q_t związanego z tym celem.

Na zakończenie należy zauważyć, że istnieje wiele innych potencjalnych zastosowań gier Stackelberga w modelowaniu scenariuszy bezpieczeństwa. Obejmują one m.in. następujące koncepcje:

- gry patrolowe (Vorobeychik i in.[27]) – zaprojektowane w celu symulowania sytuacji, w których środowiska muszą być patrolowane, aby odstraszyć intruzów. Tego rodzaju gry czerpią inspirację z powszechnie uznanego modelu pościgu i ucieczki, ale zostały rozszerzone na różne sposoby, w tym przez włączenie systemów alarmowych;
- gry typu „z interwencją w planowanie" (Vorobeychik i Pritchard[28]), w których obrońca ma za zadanie wybrać strategię ograniczania ryzyka, aby uprzedzić potencjalne działania atakującego, podczas gdy ten ostatni w odpowiedzi opracowuje optymalny plan ataku, który próbuje ominąć zaimplementowane środki zaradcze. Model

---

[25] R. Yang i in., *Improving Resource Allocation Strategy Against Human Adversaries in Security Games*, w: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* (IJCAI 2011), s. 458–464.

[26] T.H. Nguyen i in., *Analyzing the effectiveness of adversary modeling in security games*, w: *Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2013), nr 1, s. 718–724.

[27] Y. Vorobeychik, B. An, M. Tambe, *Adversarial Patrolling Games*, w*: Papers from the 2012 AAAI Spring Symposium*, t. 3, s. 91–98.

[28] Y. Vorobeychik, M. Pritchard, *Plan interdiction games*, w: *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia i in. (red.), Springer Cham 2020, s. 159–182. https://doi.org/10.1007/978-3-030-33432-1_8.

ten znajduje zastosowanie w kontekście przeciwników działających w obszarze cyberbezpieczeństwa;

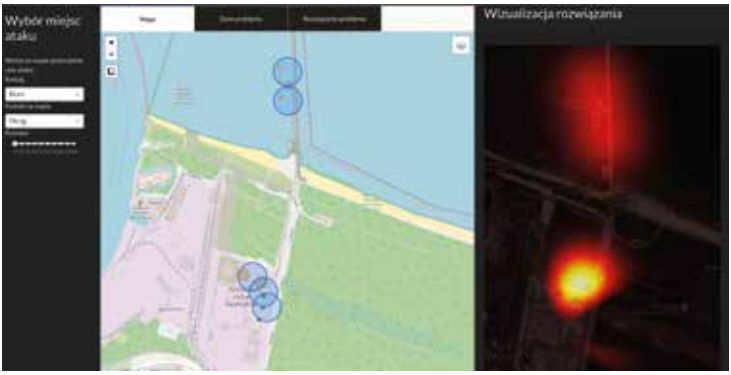
- gry audytowe (Blocki i in.[29]) – badające aspekty ekonomiczne związane z projektowaniem mechanizmów audytu, ze szczególnym naciskiem na efektywną alokację zasobów i odpowiednie systemy kar. Model gry audytowej rozszerza model gry bezpieczeństwa poprzez wprowadzenie dodatkowego parametru związanego z karą. Modele te znajdują praktyczne zastosowanie w audytach, których celem jest zapewnienie w różnych instytucjach, w tym w szpitalach, zgodności z polityką prywatności;
- koalicyjne gry bezpieczeństwa (Guo i in.[30]) – zajmujące się kwestią optymalizacji zapobiegania koalicjom atakujących, w których atakujący mają możliwość tworzenia sojuszy. Koncepcja ta jest szczególnie ważna w przypadku takich działań, jak zakłócanie sieci terrorystycznych, rozbijanie komórek tych sieci lub zapobieganie zmowie wielu napastników.

Prace zespołu „AI dla bezpieczeństwa"

Zespół „AI dla bezpieczeństwa" w instytucie badawczym IDEAS NCBR buduje modele Stackelberga dla różnych typów infrastruktury krytycznej. Aktualnie zespół koncentruje się na opracowywaniu oprogramowania do ochrony portów, terminali LNG, sieci kolejowych i energetycznych. Rysunek przedstawia podstawowy interfejs tworzonego oprogramowania.

[29] J. Blocki i in., *Audit games with multiple defender resources,* w: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI 2015), t. 29, nr 1, s. 791–797.

[30] Q. Guo i in., *Coalitional security games,* w*: Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2016), s. 159–167.



Rysunek. Zrzut z interfejsu oprogramowania do ochrony portów, terminali LNG, sieci kolejowych i energetycznych. Zrzut przedstawia mapę terminalu LNG w Świnoujściu. Czerwone okręgi oznaczają cele (rozmiar okręgu odpowiada znaczeniu celu), niebieskie – rozmieszczenie patroli i ich pole widzenia. Po prawej stronie jest pokazane względne prawdopodobieństwo, określające, które części terenu powinny być patrolowane (optymalna strategia obrońcy). Powyższa wizualizacja służy wyłącznie celom demonstracyjnym.

Celem jest opracowanie systemu mającego następujące cechy:

- ocena ryzyka – system powinien przeprowadzać ciągłą ocenę ryzyka poprzez analizę różnych źródeł danych, bieżących i historycznych oraz raportów wywiadowczych. Aby zoptymalizować alokację zasobów bezpieczeństwa, należy wziąć pod uwagę takie elementy, jak poziomy zagrożenia, pożądane cele i słabe punkty;
- losowość proponowanych strategii – system powinien wykorzystywać losowe strategie w celu określenia optymalnych tras patrolowych dla pracowników ochrony w połączeniu z optymalnym rozmieszczeniem oddziałów ochrony. Losując trasy, system zwiększa trudność potencjalnych przeciwników w przewidywaniu wzorców bezpieczeństwa, co potęguje tym samym element zaskoczenia i odstrasza potencjalnych agresorów;
- dynamiczna adaptacja – system powinien uwzględniać ewoluujące zagrożenia i dostosowywać się do zmieniających się scenariuszy bezpieczeństwa. Powinien mieć zdolność do dynamicznego modyfikowania tras patrolowych i przydzielania zasobów w odpowiedzi na informacje w czasie rzeczywistym, takie jak pojawiające się dane wywiadowcze, które aktualizują wiedzę o zagrożeniach. Ma to na celu zapewnienie optymalnego zasięgu i zwiększenie zdolności reagowania;

- współpraca i koordynacja – system powinien ułatwiać współpracę między różnymi agencjami czy też zespołami bezpieczeństwa działającymi na chronionym obszarze. Powinien on umożliwiać dzielenie się informacjami, koordynację działań oraz wymianę danych wywiadowczych w czasie rzeczywistym w celu zwiększenia świadomości sytuacyjnej i osiągnięcia lepszych wyników w zakresie bezpieczeństwa;
- ocena wydajności i informacje zwrotne – system powinien zawierać mechanizmy oceny wydajności, umożliwiające pracownikom ochrony analizę jego skuteczności i odpowiednie dostosowanie strategii. System powinien oferować informacje zwrotne, identyfikując obszary wymagające poprawy i rozpoznając wzorce, które mogą wymagać uwagi.

W ostatnim czasie członkowie zespołu „AI dla bezpieczeństwa" na jednej z czołowych konferencji informatycznych, tj. 39th Conference on Uncertainty in Artificial Intelligence (UAI 2023, Pittsburgh, USA), zaprezentowali pracę *Two-phase attacks in security games*[31]. Dotyczyła ona ataku, który przebiegał dwuetapowo (dwufazowo). Zazwyczaj atak w grach bezpieczeństwa jest modelowany jako jednorazowy ruch, podczas którego atakujący nie ma szansy na aktualizację swojej strategii, nawet jeśli w trakcie tego procesu są zdobywane nowe i cenne informacje. Jest to oczywiście daleko idące uproszczenie, niepasujące do realiów w wielu sytuacjach. Odejście od niego było celem omawianej pracy. Został w niej zaproponowany model, w którym w pierwszej fazie atakujący wykonuje wstępny ruch, aby uzyskać dodatkowe informacje na temat bieżących działań obrońcy (np. czy dany odcinek granicy jest patrolowany czy nie). Następnie, w drugiej fazie, ta wiedza jest wykorzystywana do wyboru optymalnego ruchu podczas właściwego ataku.

Niedawnym przykładem rzeczywistej sytuacji, która jest bezpośrednio modelowana w opisywanej dwufazowej grze, są działania reżimu Łukaszenki wykorzystującego imigrantów do sondowania granicy Białorusi z Ukrainą[32]. Naraża to życie imigrantów na skrajne niebezpieczeństwo zarówno ze względu na bardzo trudny teren, jak i trwającą wojnę. Zwłaszcza północno-zachodnia granica Ukrainy o długości prawie 900 km to

[31] A. Nagórko, P. Ciosmak, T. Michalak, *Two-phase security games*, w*: Proceedings of the Thirty-Nine Conference on Uncertainty in Artificial Intelligence* (UAI 2023), s. 1489–1498.

[32] V. Romanenko, *Belarus uses migrants for intelligence on border with Ukraine*, Ukrainska Pravda, 6 XII 2022 r., https://www.pravda.com.ua/eng/news/2022/12/6/7379514/ [dostęp: 25 VI 2023].

mocno zalesiony obszar pełen niebezpiecznych mokradeł. Jest tam także Strefa Wykluczenia wokół Czarnobylskiej Elektrowni Jądrowej. Co więcej, granica – która została przekroczona przez armię rosyjską w lutym 2022 r., a następnie przywrócona przez ukraińską kontrofensywę – jest obecnie silnie ufortyfikowana okopami, zasiekami i polami minowymi.

Niestety, nie zważając na te niebezpieczeństwa, białoruska straż graniczna organizuje i koordynuje działania grup imigrantów planujących nielegalne przekroczenie granicy. Celem białoruskich służb jest ujawnienie i zakłócenie ukraińskiej obrony, która jest zmuszona reagować na wszelkie próby przekroczenia granicy ze względu na zagrożenie stwarzane przez rosyjskich dywersantów.

Z uwagi na zastosowanie zaawansowanych, elektronicznych środków bezpieczeństwa większość przekroczeń granicy jest wykrywana. Należy jednak zauważyć, że wykrycie nie gwarantuje obecności patrolu wystarczająco blisko, aby zapobiec nieautoryzowanemu przekroczeniu granicy. To oznacza, że granica nie jest zupełnie nie do przejścia. Niemniej jednak, nawet w przypadkach, gdy określony odcinek granicy jest niestrzeżony w momencie wjazdu, ukraińskie dowództwo niezwłocznie wysyła tam zespół. W związku z tym kolejne próby przekroczenia tego samego odcinka granicy są bardzo mało prawdopodobne, biorąc pod uwagę szybką reakcję odpowiednich służb.

Rozważmy uproszczony model problemu, z czterema odcinkami granicy białorusko-ukraińskiej (S_1, S_2, S_3, i S_4) i dwiema jednostkami patrolowymi. Problem tego rodzaju można modelować jako standardową grę bezpieczeństwa podobną do tej wykorzystywanej na lotnisku w Los Angeles[33]. Zbiór ukraińskich ruchów obejmuje możliwe przydzielenie patroli do odcinków granicy:

$$I = \{S_1S_2, S_1S_3, S_1S_4, S_2S_3, S_2S_4, S_3S_4\}$$

Przyjmijmy założenie, że istnieją dwa możliwe typy napastników: przemytnicy (ludzi) o niskim i wysokim profilu (zaawansowania). Zostaną oni oznaczeni odpowiednio: typ 1 oraz typ 2. Atakujący o wysokim profilu zadają znacznie większe straty obrońcy, ponieważ organizują znacznie większe grupy. Oba typy mają tę samą przestrzeń strategii, tj. atakujący każdego typu może wybrać jedną z czterech sekcji granicy lub wycofać się, tj. $J_1 = J_2 = \{S_1, S_2, S_3, S_4, \varnothing\}$. Wypłaty obu stron, w zależności od typu

[33] J. Pita i in., *Using game theory for Los Angeles Airport…*

atakującego, rosną liniowo wraz z S_i – dla atakującego o wysokim profilu przydzielane punkty wynoszą odpowiednio 50, 100, 150 i 200, a dla atakującego o niskim profilu są przyznawane punkty pięciokrotnie mniejsze. Punkty obrońcy są alokowane przeciwnie, z niewielkim losowym szumem dodawanym równomiernie z przedziału [–5,5].

Zakładając, że prawdopodobieństwo ataków tych dwóch typów wynosi $p_1 = 0{,}8$ dla atakującego o niskim profilu i $p_2 = 0{,}2$ dla napastnika o wysokim profilu, optymalną strategią dla obrońcy jest następująca:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (0\%, 50\%, 0\%, 0\%, 50\%, 0\%)$$

Zgodnie z tą strategią sekcje graniczne S_1 i S_2 nigdy nie są chronione jednocześnie. Taka sytuacja jest typowa dla równowagi Stackelberga (ang. *Stackelberg equilibrium*) w grach jednofazowych i atakujący może to łatwo wykorzystać, przeprowadzając atak dwufazowy.

Omówiona zostanie teraz koncepcja ataku dwufazowego. Załóżmy, że bez wiedzy obrońcy atakujący ma niezbędne zasoby i możliwości przemytnika ludzi zarówno o niskim, jak i wysokim profilu. W związku z tym atakujący może próbować naruszyć dwie sekcje granicy sekwencyjnie, tj. atak będzie miał dwie fazy.

Na podstawie powyżej wyprowadzonej optymalnej strategii dla ataku jednofazowego rozważmy scenariusz, w którym w pierwszej fazie mało znany przemytnik podejmuje próbę przekroczenia granicy na odcinku S_1. Ta początkowa faza zapewnia atakującemu cenne informacje, bez względu na obecne rozmieszczenie obrońcy (tj. czy dany odcinek granicy jest patrolowany w tej chwili czy nie). Wynika to z tego, że po przeprowadzeniu takiego ataku atakujący ma dużo lepszą wiedzę (zna warunkowy rozkład prawdopodobieństwa dotyczący zasobów obrońcy).

Przyjmijmy, że $t \in \{0\%, 17\%, 33\%, 50\%, 67\%, 83\%, 100\%\}$ to prawdopodobieństwa napotkania dwufazowego napastnika, $(1 - t)$ x 80% to prawdopodobieństwo napotkania napastnika o niskim profilu, a $(1 - t)$ x 20% to prawdopodobieństwo napotkania napastnika o wysokim profilu. W przypadku $t = 0\%$ jest to standardowy model jednofazowy, podczas gdy $t = 100\%$ opisuje czysty atak dwufazowy.

W tabeli 4 pokazano, że obecność dwufazowego atakującego znacznie zmienia równowagę Stackelberga w grze. Na przykład dla 33-procentowego prawdopodobieństwa ataku dwufazowego (z 53-procentową szansą na jednofazowy atak o niskim profilu i 13-procentową szansą na jednofazowy

atak o wysokim profilu, utrzymując stosunek 4:1 niskiego profilu do wysokiego profilu) optymalną strategią obrońcy staje się następująca:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (12\%, 15\%, 17\%, 17\%, 18\%, 21\%)$$

Zgodnie z tabelą 4 dwufazowe równowagi Stackelberga są znacznie bardziej odporne na zmiany profili napastników.

Tabela 4. Każdy wiersz przedstawia optymalną mieszaną strategię obrońcy przeciwko grupie atakujących z daną szansą na napotkanie dwufazowego ataku. Zgodnie z ostatnim wierszem bez obecności dwufazowych napastników równowaga Stackelberga jest istotnie niedostosowana do losowego szumu w macierzach punktacji.

S_1S_2	S_1S_3	S_1S_4	S_2S_3	S_2S_4	S_3S_4	Szansa na atak dwufazowy
0,085	0,11	0,12	0,2	0,25	0,23	100%
0,085	0,11	0,12	0,2	0,25	0,23	83%
0,12	0,11	0,12	0,2	0,25	0,23	67%
0,12	0,15	0,17	0,17	0,18	0,21	50%
0,12	0,15	0,17	0,17	0,18	0,21	33%
0,15	0,15	0,17	0,16	0,18	0,18	17%
0	0,5	0	0	0,5	0	0%

Ruchy obrońcy (rozmieszczenie patroli)

W tabeli 5 pokazano, jak zmieniają się wypłaty obrońców w zależności od składu grup atakujących. Na przykład oczekiwana punktacja obrońcy przeciwko atakowi jednofazowemu spada do –175, gdy strategia jednofazowa jest stosowana przeciwko atakującemu dwufazowemu.

Tabela 5. Oczekiwana wypłata obrońcy na etapie gry ze strategią z tabeli 4 przeciwko danej szansie na atak dwufazowy. W ostatniej kolumnie widać, że strata poniesiona w wyniku grania strategią, która ignoruje możliwość ataku dwufazowego, jest o rząd wielkości większa niż zbyt ostrożna ochrona przed takimi atakami.

-16,2	-16,2	-16,2	-20,3	-20,3	-24,9	-175	100%
-14,8	-14,8	-14,8	-17,3	-17,3	-20,9	-146	83%
-13,4	-13,4	-13,4	-14,3	-14,3	-16,9	-116	67%
-12	-12	-12	-11,3	-11,3	-12,8	-87,1	50%
-10,7	-10,7	-10,7	-8,36	-8,36	-8,84	-57,9	33%
-9,27	-9,27	-9,27	-5,38	-5,38	-4,83	-28,6	17%
-7,89	-7,89	-7,89	-2,41	-2,41	-0,816	0,7	0%
100%	83%	67%	50%	33%	17%	0%	

Szansa na atak dwufazowy

Strategia obrońcy

W celu eliminacji przedmiotowej usterki autorzy proponują nowy model, który pozwala na jednoczesne uwzględnienie napastników jedno- i dwufazowych. W tym modelu bezpieczeństwa oczekiwana punktacja przeciwko skoordynowanym atakującym znacznie się zmienia, z –175 do –16,2 (obrońca nadal znajduje się w niekorzystnej sytuacji). Optymalna strategia:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (8{,}5\%, 11\%, 12\%, 20\%, 25\%, 23\%)$$

zmusza atakującego o niskim profilu do zaatakowania S_1, a atakującego o wysokim profilu do wycofania się, jeśli S_1 nie był patrolowany. Należy zauważyć, że wiąże się to z kosztami – w przypadku nieskoordynowanego (jednofazowego) ataku, gdy atakujący o niskim i wysokim profilu działają niezależnie, ta strategia daje obrońcy wypłatę –7,89 (spadek z 0,7).

Podsumowanie

W niniejszym artykule przedstawiono zaawansowane metody poprawiające bezpieczeństwo infrastruktury krytycznej, obejmujące połączenie teorii gier, technik optymalizacji i algorytmów sztucznej inteligencji. Skuteczność tych metod została wykazana poprzez ich wdrożenie w kilku obiektach czy też zastosowaniach w USA. Należy podkreślić, że tego rodzaju ulepszenia zostały osiągnięte nie przez zwiększenie zasobów służb bezpieczeństwa (i kosztów), lecz przez optymalizację wykorzystania dostępnych zasobów. Prace zespołu „AI dla bezpieczeństwa" w instytucie badawczym IDEAS NCBR koncentrują się na rozszerzeniu tych wyników i zastosowaniu ich do różnych rodzajów infrastruktury krytycznej oraz do zagrożeń bezpieczeństwa, które ostatnio pojawiły się ponownie w Europie. Zespół dąży do ich szybkiego wdrożenia, aby zoptymalizować ochronę polskich obiektów i systemów infrastruktury krytycznej.

Załącznik A

Załącznik jest poświęcony formalnemu opisowi gier bezpieczeństwa, który podąża za nowoczesnym podejściem[34]. Następnie została opisana szersza klasa gier Stackelberga, zwana bayesowskimi grami Stackelberga, która stanowi podstawę dla modelu dwufazowego omówionego w poprzedniej części artykułu. Wprowadzono także sformalizowany opis problemu optymalizacyjnego, który można wykorzystać do rozwiązania tych gier.

A.1 Gry bezpieczeństwa

Gry bezpieczeństwa są rozgrywane przez dwóch graczy – obrońcę i atakującego. Obrońca ma ograniczoną liczbę zasobów bezpieczeństwa i dąży do alokacji tych zasobów w celu ochrony n celów ze zbioru $[n] = \{1,2,\ldots,n\}$. Strategia czysta obrońcy to podzbiór celów, które są chronione (pokrywane) w ramach wykonalnej alokacji tych zasobów. Reprezentacją strategii czystej jest wektor binarny $e \in \{0,1\}^n$, gdzie wyrazy o wartości 1 określają cele pokryte ochroną. Symbol $E \subseteq \{0,1\}^n$ oznacza zbiór wszystkich dostępnych strategii czystych obrońcy. Strategia mieszana obrońcy to rozkład prawdopodobieństwa x określony na elementach E. Strategia czysta atakującego jest celem $i \in [n]$. Strategia mieszana atakującego jest oznaczana

[34] H. Xu, *The Mysteries of Security Games: Equilibrium Computation Be-Comes Combinatorial Algorithm Design*, w: *Proceedings of the 2016 ACM Conference on Economics and Computation* (ACM EC 2016), s. 497–514.

przez $y \in \Delta_n$, gdzie Δ_n jest n-wymiarowym sympleksem. W tym przypadku y_i oznacza prawdopodobieństwo ataku na cel i.

W najbardziej ogólnym ujęciu gry bezpieczeństwa są formą gry dwuliniowej. Gra dwuliniowa jest określana przez parę macierzy (A,B) i wielościanów (P,Q). Zakładając, że gracz 1 gra zgodnie z $x \in P$, a gracz 2 gra zgodnie z $y \in Q$, wypłaty dla gracza 1 i 2 wynoszą odpowiednio $x^T Ay$ oraz $x^T By$.

Możemy teraz podać różne pojęcia równowag dla gier bezpieczeństwa. Profil strategii (x,y) jest równowagą Nasha (NE), jeśli:

$$\forall x' \in P \ \forall y' \in Q \ x^T Ay \geq x'^T Ay \ \& \ x^T By \geq x^T By'$$

Zgodnie z twierdzeniem Nasha dla każdej gry dwuliniowej istnieje co najmniej jedna NE w strategiach mieszanych (może ich istnieć więcej niż jedna).

Gdy jeden gracz porusza się przed innym graczem, bardziej odpowiednią koncepcją rozwiązania jest równowaga Stackelberga. Dwuosobowa gra Stackelberga jest rozgrywana pomiędzy liderem i śledzącym. Lider wykonuje ruch jako pierwszy lub, równoważnie, zagrywa zgodnie z pewną strategią mieszaną jako pierwszy. Gracz śledzący obserwuje strategię lidera i reaguje na nią zgodnie z dostępnymi sobie strategiami. Optymalna strategia lidera wraz z najlepszą odpowiedzią śledzącego tworzy równowagę.

Niech

$$y_x = \arg\max_{y' \in Q} x^T By'$$

oznacza najlepszą odpowiedź gracza śledzącego na strategię lidera $x \in P$. Profil strategii (x, y) jest silną równowagą Stackelberga (ang. *strong Stackelberg equilibrium*, SSE), gdy:

$$x = \arg\max_{x' \in P} x'^T Ay_{x'} \quad \text{oraz} \quad y = y_x$$

Gdy $B = -A$, to dwuliniowa gra jest grą o sumie zerowej. W takich grach zarówno NE, jak i SSE są równoważne równowadze minimaksowej (ang. *minimax equilibrium*, ME).

Profil strategii (x, y) stanowi z kolei **równowagę minimaksową**, jeśli

$$\forall x' \in P \forall y' \in Q \ x^T Ay \geq x'^T Ay \ \& \ x^T Ay \leq x^T Ay'$$

W przypadku gdy (x, y) jest równowagą minimaksową, strategia x będzie oznaczała strategię optymalną gracza 1, a strategia y – strategię minimaksową gracza 2.

Wartość gry będzie w takim przypadku następująca:

$$V = x^T Ay = \max_{x' \in \mathcal{P}} \min_{y' \in Q} x'^T Ay'$$

Przejdźmy do opisu struktury wypłat w grze, zakładając, że atakujący atakuje cel i:

- obrońca otrzymuje nagrodę r_i, jeśli cel i zostanie ochroniony, lub ponosi koszt c_i, jeśli i zostanie bez ochrony (odkryty),
- atakujący ponosi koszt ξ_i, jeśli cel i jest pokryty (ochroniony), lub nagrodę ρ_i, jeśli i pozostanie odkryty,
- obaj gracze otrzymują wypłatę 0 na pozostałych $n - 1$ nieatakowanych celów.

Przyjmujemy tu kluczowe założenie: dla wszystkich $i \in [n]$ ustalmy, że:

$$r_i > c_i \quad \text{oraz} \quad \rho_i > \xi_i$$

Oznacza to, że:

- ochrona danego celu jest dla obrońcy bardziej korzystna niż jego odsłanianie,
- atakujący woli zaatakować cel, gdy jest on niepokryty.

Definicja 1 (gra bezpieczeństwa).

Gra bezpieczeństwa G z liczbą celów n to gra (r,c,ρ,ξ,E), która spełnia $r_i > c_i$ oraz $\rho_i > \xi_i$ dla wszystkich $i \in [n]$.

Użyteczność (wypłatę) obrońcy można zdefiniować w następujący sposób:

$$U^d(e,i) = r_i e_i + c_i(1 - e_i)$$

Przy założeniu $p \in \Delta_{|E|}$ oraz $y \in \Delta_n$ oczekiwana wypłata obrońcy wynosi:

$$U^d(p,y) = \sum_{e\in\mathcal{E}} \sum_{i\in[n]} p_e\, y_i U^d(e,i) =$$

$$= \sum_{e\in\mathcal{E}} \sum_{i\in[n]} p_e\, y_i\big(r_i e_i + c_i(1-e_i)\big) =$$

$$= \sum_{i\in[n]} y_i \sum_{e\in\mathcal{E}} p_e\big(r_i e_i + c_i(1-e_i)\big) =$$

$$= \sum_{i\in[n]} y_i \left(r_i \sum_{e\in\mathcal{E}} p_e\, e_i + c_i \left(1 - \sum_{e\in\mathcal{E}} p_e\, e_i \right) \right)$$

Gdy $p \in \Delta_{|\mathcal{E}|}$ i $y \in \Delta_n$, oczekiwana użyteczność obrońcy wynosi:

$$U^d(p,y) = \sum_{i\in[n]} y_i \left(r_i \sum_{e\in\mathcal{E}} p_e\, e_i + c_i \left(1 - \sum_{e\in\mathcal{E}} p_e\, e_i \right) \right)$$

Przyjmując następującą konwencję notacyjną:

$$x_i := \sum_{e\in\mathcal{E}} p_e\, e_i$$

tj. używając symbolu x_i na oznaczenie krańcowego (tzw. marginalnego) prawdopodobieństwa pokrycia celu i, dostajemy równoważne określenie oczekiwanej użyteczności obrońcy jako:

$$U^d(p,y) = \sum_{i\in[n]} y_i\big(r_i x_i + c_i(1-x_i)\big)$$

W przypadku przyjęcia założenia, że $x = (x_1,\ldots,x_n)^T$ oznacza prawdopodobieństwo krańcowe dla wszystkich celów wywołanych przez strategię mieszaną p. Powyższe równanie pokazuje, że oczekiwana użyteczność obrońcy może być zwięźle wyrażona jako postać dwuliniowa:

$$U^d(x,y) = \sum_{i\in[n]} y_i\big(r_i x_i + c_i(1-x_i)\big)$$

Widać, że $U^d(x, y)$ ma postać dwuliniową

$$x^T Ay + ax$$

dla pewnej nieujemnej macierzy diagonalnej A.

Zwróćmy uwagę, że wypukła otoczka zbioru E jest wielościanem wszystkich wykonalnych (tj. możliwych do wdrożenia przez strategię mieszaną obrońcy) prawdopodobieństw krańcowych:

$$\mathcal{P} = \{x = \sum_{e \in \mathcal{E}} p_e \, e : p \in \Delta_{|\mathcal{E}|}\}$$

W tym przypadku można więc zinterpretować punkt $x \in P$ jako strategię mieszaną i – jak wyżej – oznaczyć użyteczność obrońcy poprzez: $U^d(x, y)$.

Analogicznie, oczekiwana użyteczność atakującego może być zwięźle przedstawiona w następującej formie:

$$U^a(x, y) = \sum_{i \in [n]} y_i(\rho_i(1 - x_i) + \xi_i x_i)$$

Widać też, że $U^a(x, y)$ ma również postać dwuliniową

$$x^T By + \beta y$$

dla pewnej niedodatniej macierzy diagonalnej B.

W grach o sumie zerowej wszystkie wyżej wymienione standardowe pojęcia równowagi są tym samym co równowaga minimaksowa, a zadaniem polegającym na rozwiązaniu gry jest obliczenie równowagi minimaksowej w czasie wielomianowym.

W przypadku, gdy gra nie ma sumy zerowej, głównym rozwiązaniem jest silna równowaga Stackelberga – obrońca odgrywa rolę lidera i może przyjąć strategię mieszaną, zanim atakujący wykona ruch. Atakujący obserwuje mieszaną strategię obrońcy i stara się reagować na nią w możliwie najlepszy sposób. W tym przypadku zadanie algorytmiczne polega na obliczeniu optymalnej strategii mieszanej dla obrońcy (należy zwrócić uwagę, że atakujący nie jest w stanie obserwować rozmieszczenia obrońcy w czasie rzeczywistym, tj. próbkowanej czystej strategii, ponieważ musi zaplanować atak przed próbkowaniem czystej strategii obrońcy w czasie rzeczywistym).

A.2 Bayesowskie gry bezpieczeństwa

Omówione w artykule rozwiązanie wdrożone na lotnisku LAX opierało się na szerszej klasie gier zwanych Bayesian Security Games (pol. bayesowskie gry bezpieczeństwa) lub Bayesian Stackelberg Games (bayesowskie gry Stackleberga). W opisie tej klasy gier podążamy za układem i notacją z pracy Nagórki i in.[35] oraz używamy omówionego wcześniej problemu ochrony granicy Białoruś–Ukraina jako przykładu ilustrującego działanie tego modelu.

W bayesowskiej grze Stackelberga obrońca gra przeciwko grupie atakujących n różnych typów. W każdej rundzie obrońca gra przeciwko jednemu atakującemu typu $1 \leq t \leq n$ losowo, z prawdopodobieństwem wynoszącym p_t. Atakujący mogą mieć do dyspozycji różne zestawy ruchów, które wyrządzają różne szkody obrońcy. W naszym przykładzie przedstawiamy atakującego o niskim profilu ($t = 1$) i atakującego o wysokim profilu ($t = 2$) wynoszącym

$$p_1 = {}^4\!/_5 \text{ i } p_2 = {}^1\!/_5.$$

Przyjmijmy, że I oznacza zbiór ruchów obrońcy. W omawianym przykładzie patrol graniczny przydziela dwie jednostki patrolujące do czterech segmentów granicy, a zatem $I = \{S_1S_2, S_1S_3, S_1S_4, S_2S_3, S_2S_4, S_3S_4\}$.

W bayesowskiej grze Stackelberga w pierwszej kolejności obrońca wybiera własną strategię mieszaną x. W przykładzie $x = \{x_i\}_{(i \in I)}$ stanowi miarę prawdopodobieństwa na I, oznaczaną przez $x \in Prob(I)$ z

$$Prob(I) = \{x: I \rightarrow R: \sum_{i \in I} x_i = 1 \, , x \geq 0\}$$

Strategia x nie zależy od t, ponieważ obrońca nie zna typu napastnika, którego napotka.

Przez J_t oznaczmy zbiór ruchów atakującego typu t. W tego rodzaju przykładzie $J_1 = J_2 = \{S_1, S_2, S_3, S_4, \varnothing\}$ atakujący mogą zaatakować jeden z segmentów granicznych lub wycofać się. Atakujący wybiera swoją strategię jako drugi, znając strategię obrońcy x. Chociaż na początku może się to wydawać sprzeczne z intuicją, dla obrońcy korzystne będzie ujawnienie atakującemu swojej strategii mieszanej (ale nie swoich aktualnych pozycji obronnych). Ujawnianie informacji w takich scenariuszach jest dość

[35] A. Nagórko, P. Ciosmak, T. Michalak, *Two-phase security games*...

powszechne, aby zmusić przeciwnika do korzystnej reakcji, czego przykładem jest akcja „Znicz" przeprowadzana co roku przez polską Policję[36].

W każdej rundzie gry obaj gracze poruszają się niezależnie, zgodnie ze strategiami x i $y^t(x)$, które wybrali wcześniej. Symbol $r_{i,t,j}$ oznacza wypłatę obrońcy przy zagraniu ruchu $i \in I$ przeciwko atakującemu typu $1 \leq t \leq n$, który zagrał ruch $j \in J_t$. Symbol $c_{i,t,j}$ oznacza wypłatę atakującego (która może różnić się od $-r_{i,t,j}$), ponieważ nie zakładamy, że gry mają sumę zerową.

Użyteczności graczy można zwięźle przedstawić za pomocą macierzy wypłat. W przedmiotowym przykładzie macierze wypłat dla ataku o wysokim profilu są następujące:

	S_1		S_2		S_3		S_4			∅
S_1S_2	51,	-50	102,	-100	-152,	150	-211,	200	0,	0
S_1S_3	55,	-50	-123,	100	175,	-150	-221,	200	0,	0
S_1S_4	59,	-50	-108,	100	-169,	150	206,	-200	0,	0
S_2S_3	-69,	50	101,	-100	168,	-150	-221,	200	0,	0
S_2S_4	-55,	50	113,	-100	-170,	150	212,	-200	0,	0
S_3S_4	-75,	50	-123,	100	166,	-150	211,	-200	0,	0

Pierwsza liczba w wierszu i i kolumnie j to punktacja obrońcy $r_{i,t,j}$ (w tym przypadku 1 oznacza atakującego o wysokim profilu $t = 1$). Druga liczba to $c_{i,1,j}$. Niskoprofilowy atak przynosi następujące wypłaty:

		S_1		S_2		S_3		S_4		∅
S_1S_2	14,	-10	23,	-20	-34,	30	-42,	40	0,	0
S_1S_3	10,	-10	-20,	20	32,	-30	-43,	40	0,	0
S_1S_4	12,	-10	-23,	20	-33,	30	44,	-40	0,	0
S_2S_3	-11,	10	24,	-20	31,	-30	-41,	40	0,	0
S_2S_4	-11,	10	20,	-20	-31,	30	42,	-40	0,	0
S_3S_4	-11,	10	-21,	20	34,	-30	44,	-40	0,	0

Atakujący t wybiera optymalną strategię $\overline{y}^t = \overline{y}^t(x)$, zależącą od znanej strategii obrońcy x, która maksymalizuje również oczekiwaną wypłatę

[36] *Policyjne działania Znicz*, https://policja.pl/pol/aktualnosci/210088,Policyjne-dzialania-ZNICZ.html [dostęp: 25 VI 2023].

$$\bar{c} = \sum_{i \in I} \sum_{j \in J_t} x_i \bar{y}_j^t c_{i,t,j}$$

Wypłata jest maksymalizowana przez zagranie zgodne ze strategią czystą, tj. y^t jest optymalna wtedy i tylko wtedy, gdy

$$\bar{c} \geq \sum_{i \in I} x_i c_{i,t,j}$$

Obrońca działa tak, aby zmaksymalizować swoją oczekiwaną wypłatę w stosunku do optymalnych strategii atakujących, tj. wybiera optymalną strategię *x*, która maksymalizuje jego oczekiwaną punktację:

$$\sum_{i \in I} \sum_{t=1}^{n} \sum_{j \in J_t} p_t x_i \bar{y}_j^t r_{i,t,j}$$

Stąd rozwiązanie bayesowskiej gry Stackelberga jest zadane przez następujący kwadratowy problem optymalizacyjny:

$$\max_{x, y^t} \sum_{i \in I} \sum_{t=1}^{n} \sum_{j \in J_t} p_t x_i y_j^t r_{i,t,j}$$

przy ograniczeniach:

$$\sum_{i \in I} x_i = 1$$

$$\sum_{j \in J_t} y_j^t = 1 \text{ dla każdego } 1 \leq t \leq n,$$

$$\sum_{i \in I} \sum_{j \in J_t} x_i y_j^t c_{i,t,j} \geq \sum_{i \in I} x_i c_{i,t,j} \text{ dla każdego } 1 \leq t \leq n, j \in J_t,$$

$$x \geq 0, y^t \geq 0 \text{ dla każdego } 1 \leq t \leq n$$

Opisana formalizacja w połączeniu z techniką linearyzacji prowadzi do sformułowania mieszanego całkowitoliczbowego programowania liniowego (ang. *mixed integer linear programming*) dla bayesowskich gier Stackelberga, opublikowanego w pracy Paruchuriego i in.[37] jako słynny algorytm DOBSS.

[37] P. Paruchuri i in., *Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games*, w: *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), t. 2, s. 895–902.

Bibliografia

An B. i in., *A Deployed Quantal Response-Based Patrol Planning System for the U.S. Coast Guard*, „Interfaces" 2013, t. 43, nr 5, s. 400–420. https://doi.org/10.1287/inte.2013.0700.

Bier V.M., Azaiez M.N., *Game Theoretic Risk Analysis of Security Threats*, Springer 2008, https://doi.org/10.1007/978-0-387-87767-9.

Blocki J. i in., *Audit games with multiple defender resources*, w: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI 2015), t. 29, nr 1, s. 791–797.

Brown G. i in., *A Two-Sided Optimization for Theater Ballistic Missile Defense*, „Operations Research" 2005, t. 53, nr 5, s. 745–763. https://doi.org/10.1287/opre.1050.0231.

Fang F., Nguyen T.H., *Green security games: Apply game theory to addressing green security challenges*, „ACM SIGecom Exchanges" 2016, t. 15, nr 1, s. 78–83. https://doi.org/10.1145/2994501.2994507.

Gatti N. i in., *Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form*, w: *Proceedings of the 2008 conference on ECAI 2008: 18th European Conference on Artificial Intelligence* (ECAI 2008), s. 403–407. https://doi.org/10.3233/978-1-58603-891-5-403.

Gholami S. i in., *Adversary models account for imperfect crime data: Forecasting and planning against real-world poachers*, w: *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2018), s. 823–831.

Guo Q. i in., *Coalitional security games*, w: *Proceedings of the 2016 15th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2016), s. 159–167.

Haskell W. i in., *Robust protection of fisheries with COmPASS*, w: *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence* (AAAI 2014), t. 28, nr 2, s. 2978–2983.

Hunt K., Zhuang J., *A review of attacker-defender games: Current state and paths forward*, „European Journal of Operational Research" 2023, w druku. https://doi.org/10.1016/j.ejor.2023.04.009.

Hutter F. i in., *Boosting Verification by Automatic Tuning of Decision Procedures*, w: *Proceedings of the 19th International Conference on Computer Aided Verification* (CAV 2007), s. 27–34.

Korzhyk D. i in., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, „Journal of Artificial Intelligence Research" 2011, t. 41, nr 2, s. 297–327.

Lye K-w., Wing J., *Game Strategies in Network Security*, „International Journal of Information Security" 2005, t. 4, s. 71–86. https://doi.org/10.1007/s10207-004-0060-x.

Nagórko A., Ciosmak P., Michalak T., *Two-phase security games*, w: *Proceedings of the Thirty-Nine Conference on Uncertainty in Artificial Intelligence* (UAI 2023), s. 1489–1498.

Nguyen T.H. i in., *Analyzing the effectiveness of adversary modeling in security games*, w: *Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2013), nr 1, s. 718–724.

Nguyen T.H. i in., *Towards a science of security games*, w: *Mathematical Sciences with Multidisciplinary Applications*, B. Toni (red.), Springer Cham 2016, s. 347–381.

Paruchuri P. i in., *Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games*, w: *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), t. 2, s. 895–902.

Pita J. i in., *Using game theory for Los Angeles Airport security*, „AI Magazine" 2009, t. 30, nr 1, s. 43–57. https://doi.org/10.1609/aimag.v30i1.2173.

Sandler T., *Terrorism & Game Theory*, „Simulation & Gaming" 2003, t. 34, nr 3, s. 319–337. https://doi.org/10.1177/1046878103255492.

Shieh E. i in., *Protect: A deployed game theoretic system to protect the ports of the United States*, w: *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2012), t. 1, s. 13–20.

Sinha A. i in., *Stackelberg security games: Looking beyond a decade of success*, w: *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI 2018), s. 5494–5501.

Stackelberg H. von, *Marktform und Gleichgewicht*, J. Springer 1934.

Tambe M., *Security and game theory: algorithms, deployed systems, lessons learned*, Cambridge 2011.

Tsai J. i in., *Iris – a tool for strategic security allocation in transportation networks*, w: *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2009), s. 37–44.

Vorobeychik Y., An B., Tambe M., *Adversarial Patrolling Games*, w: *Papers from the 2012 AAAI Spring Symposium*, t. 3, s. 91–98.

Vorobeychik Y., Pritchard M., *Plan interdiction games*, w: *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia i in. (red.), Springer Cham 2020, s. 159–182. https://doi.org/10.1007/978-3-030-33432-1_8.

Xu H., *The Mysteries of Security Games: Equilibrium Computation Be-Comes Combinatorial Algorithm Design*, w: *Proceedings of the 2016 ACM Conference on Economics and Computation* (ACM EC 2016), s. 497–514.

Yang R. i in., *Adaptive resource allocation for wildlife protection against illegal poachers*, w: *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2014), s. 453–460.

Yang R. i in., *Improving Resource Allocation Strategy Against Human Adversaries in Security Games*, w: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* (IJCAI 2011), s. 458–464.

Yang R. i in., *Improving resource allocation strategies against human adversaries in security games: An extended study*, „Artificial Intelligence" 2013, t. 195, s. 440–469. https://doi.org/10.1016/j.artint.2012.11.004.

Yin Z. i in., *Trusts: Scheduling randomized patrols for fare inspection in transit systems*, w: *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence* (AAAI 2012), t. 26, nr 2, s. 2348–2355.

Zhang Y., Malacaria P., *Bayesian Stackelberg games for cyber-security decision support*, „Decision Support Systems" 2021, t. 148, art. 113599. https://doi.org/10.1016/j.dss.2021.113599.

Źródła internetowe

Policyjne działania Znicz, https://policja.pl/pol/aktualnosci/210088,Policyjne-dzialania-ZNICZ.html [dostęp: 25 VI 2023].

Romanenko V., *Belarus uses migrants for intelligence on border with Ukraine*, Ukrainska Pravda, 6 XII 2022 r., https://www.pravda.com.ua/eng/news/2022/12/6/7379514/ [dostęp: 25 VI 2023].

Dr Tomasz P. Michalak

Lider samodzielnego zespołu badawczego w IDEAS NCBR oraz wykładowca na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Absolwent Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego. W czasie kariery naukowej prowadził badania na Wydziale Informatyki Uniwersytetu Oksfordzkiego, w Szkole Inżynierii i Informatyki Uniwersytetu w Southampton, na Wydziale Informatyki Uniwersytetu w Liverpoolu oraz Wydziale Ekonomii Stosowanej Uniwersytetu w Antwerpii, na którym otrzymał tytuł doktora ekonomii.

Dr Michał T. Godziszewski

Specjalista w zakresie logiki i jej zastosowań (w matematyce, filozofii i informatyce), sztucznej inteligencji (specjalność – teoria systemów wieloagentowych: algorytmiczna teoria gier, analiza sieciowa, obliczeniowa teoria wyboru społecznego) i informatyki teoretycznej. Obecnie zajmuje się przede wszystkim analizą algorytmiczną sieci społecznych i gier Stackelberga, złożonością obliczeniową w teorii gier oraz ich zastosowaniami do modelowania systemów bezpieczeństwa.

Dr Andrzej Nagórko

Adiunkt na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Były pracownik Instytutu Matematycznego Polskiej Akademii Nauk oraz uniwersytetów w Stanach Zjednoczonych i Izraelu. Od lat stosuje metody optymalizacji matematycznej w różnych dziedzinach – od sztucznej inteligencji poprzez teorię gier po geometryczną teorię grup. W IDEAS NCBR pracuje nad zastosowaniami tych metod do ochrony infrastruktury krytycznej.