Koudela Pál

Játékelmélet a kiberbiztonságban

DOI 10.17047/HADTUD.2019.29.4.39

A védelem- és biztonságpolitika valamint a rendvédelem a virtuális térben zajló konfliktusok modellezésekor hiányos, azaz nem teljes információs környezettel kerül szembe. A hidegháborús környezetben kifejlesztett infrastrukturális környezet és a konfliktusok modellezése ma éli virágkorát. A világháló nyújtotta feltételek és szolgáltatások gyorsuló növekedése és fejlődése, az anonim és önszerveződő hálózatok, valamint a mobileszközök elterjedése új kihívásokat jelent.

A hidegháború amerikai reakciójaként a hatvanas években kifejlesztették a számítógépes hálózatokat, majd 1989-ben Tim Berners-Lee létrehozta a világhálót, amihez a következő évben megírta az első böngészőt is, így az fokozatosan általánosan használt rendszerré vált. A világháló hagyományos felépítése (tűzfal, behatolásérzékelő és vírusirtó szoftverek), egyoldalú, statikus és passzív védelmi rendszere azonban számtalan módon teszi azt sebezhetővé, beleértve a szolgáltatás-megtagadással járó támadást,[1] az elosztott szolgáltatásmegtagadással járó támadást,[2] a „brute force"-támadást, az „Sql injekcióra" épülő akciókat és egyéb támadásokat. Szükségessé vált tehát egy összetettebb védekezési rendszer kidolgozása.

A játékelmélet, különösen a Harsányi János[3] által kidolgozott nem teljes információs elemzés alkalmazása ezen a területen is sikerhez vezetett az elmúlt években.[4]

1 Denial of Service (DoS) vagyis szolgáltatásmegtagadás, illetve az ezzel járó támadás, annak teljes vagy részleges megbénítása, helyes működési módjától való eltérítése.

2 Distributed Denial of Service (DDoS), vagyis elosztott szolgáltatásmegtagadással járó támadás. A célzott hálózatot több helyről származó csomagokkal bombázzák.

3 Harsányi János magyar Nobel-díjas közgazdász és matematikus. 1920-ban született Budapesten, 1945-ben Ausztráliába menekült, majd 1956-tól az Egyesült Államokban élt. 1967–68-ban kidolgozta az információhiányos hidegháborús környezetben döntő fontosságú játékelméleti nem teljes információs modellt, ami máig alapja a nemzetbiztonsági, stratégiai, biztonságpolitikai és más területek játékelméleti modellezésének, s amiért 1994-ben – John Forbes Nashsel és Reinhard Seltennel megosztva – Nobel-díjat kapott.

4 Alpcan, Tansu – Tamer Ba°ar: *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, Cambridge University Press, 2011.

Az egyik legelső megközelítés,[5] a járőrözéshez hasonlóan, a biztonsági erőforrások – az adminisztrátorok ideje – különböző feladatok közötti hatékony elosztásának modellezésére törekedett. A modell a mindenütt jelenlévő támadó és a rendszergazdák közötti interakcióra épül. A modell a mátrixok szinguláris értékek szerinti felbontásával kíséreli meg az egyensúlyi helyzetek kiszámítását a játszmákban.

Stratégiai döntéshozatali modellként a játékelméleti technikákat azért fogadták el, hogy kommunikációs hálózatok protokolltervezési problémáit megoldják, különös tekintettel a hálózatok heterogén ágensei erőforrás-allokációjának elemzésére. Az útvonalterv több szereplő versenyével jár együtt, így a vezetékes hálózatban a játékelméletet széles körben használják az önző útvonaltervezés feltérképezéséhez, és optimalizálják az útválasztási algoritmust a jobb protokolltervezés érdekében.[6] Miután a hálózati torlódási problémák hátterében a versengés és interakció áll, a játékelmélet kiválóan alkalmazhatónak bizonyult. A vezetéknélküli hálózatok megjelenésével pedig tovább bővült annak alkalmazhatósága: például a kommunikációs csatorna állításával, a hálózati csomópontok eltörlésével és a hálózati erőforrás-allokáció optimalizálásával. A vezeték nélküli hálózat jellemzően homogén szerkezete és bizonyos mértékig rögzített konfigurációja miatt a hálózati viselkedés általában „racionális", így a játékelmélet alkalmazása a vezeték nélküli hálózatokban még jobb eredményt is érhet el.

A kiberbiztonság területén alkalmazott nem teljes információs játékelméletben alapvetően kétféle eredményet láthatunk: egyrészt a kibertámadások és kivédésük stratégiai elemzéseit, másrészt magának a kiberbiztonságnak az értékelését. Az előbbi tipikusan a várható támadások előrejelzését szolgálja a támadó és védekező magatartások modellezésével, s az így létrejövő egyensúlyi helyzetek kalkulálásával. Ennek segítségével védelmi stratégiát is kidolgozhatnak, s a védelmi rendszer megbízhatóságát is kiértékelhetik.

Az eljárás kvantitatív jellege miatt összehasonlíthatóság és értékelés szempontjából is ideális eszköz.[7] Jellemzően versengő jellegű, nem kooperatív játszmák elemzéséről van szó, melyek közül némelyik (a biztonsági védelmi beruházások és a védelmi erőforrások elosztása) elemezhető statikus modellekkel, általában azonban, a hálózatok tulajdonságai miatt, dinamikus modellekre van szükség az elemzéshez. A kiberbiztonság területén a támadás/védelem elemzése tehát egyértelműen a nem teljes információs, dinamikus modellezésre épül, melynek máig meghatározó alapjait a Nobel-díjas magyar tudós, Harsányi János a hatvanas években dolgozta ki.

---

5 Andrew Fielder – Emmanouil Panaousis – Pasquale Malacaria – Chris Hankin – Fabrizio Smeraldi: Game Theory Meets Information Security Management. In.: Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, Thierry Sans (eds.) *ICT Systems Security and Privacy Protection. SEC 2014*. IFIP Advances in Information and Communication Technology, vol 428., Berlin, Heidelberg, Springer, 2014. pp. 15–29.

6 Menache, Ishai – Asuman Ozdaglar: *Network Games: Theory, Models, and Dynamics. Synthesis Lectures on Communication Networks*. Berkeley, Morgan & Claypool Publishers, 2011.

7 Yuan Wang – Yongjun Wang – Jing Liu – Zhijian Huang – Peidai Xie: A Survey of Game Theoretic Methods for Cyber Security. In.: *2016 IEEE First International Conference on Data Science in Cyberspace*. Changsha, IEEE, 2016. pp. 631–636.

Az információs hadviselés és az információs biztonság játékelméleti modelljei

A számítógépes támadás összetett hadviselési és bűnözési terület, amely a legnagyobb figyelmet igényli, mivel a számítógép az emberi erőfeszítések különböző területeinek eszköze. A támadás más formáihoz hasonlóan a számítógépes támadás okai sokrétűek, azonban általában olyan tényezőkre vezethetők vissza, amelyek magukban foglalják a pénzügyi nyereséget, a személyes érzelmeket és a bosszúvágyat, valamint az etikai, ideológiai, erkölcsi és környezetvédelmi kérdéseket egyaránt.[8]

A számítástechnikai bűnözés kockázatainak kezelésére szolgáló különböző modellek közé tartozik a Bayes-t Hálózat,[9] az Operationally Critical Threat, Asset and Vulnerability Assessment (OCTAVE),[10] a központi számítástechnikai és távközlési ügynökség kockázatelemzése és kezelése (CRAMM).[11]

A játékelmélet matematikai keretet biztosít a két vagy több egyén közötti konfliktusok és együttműködés modellezéséhez. Alapja az egyének racionális viselkedése. Ez magában foglalja, hogy a céljuk az előnyök optimalizálása, amelyet általában hasznosság-függvénnyel fejeznek ki. A játékos betartja a szabályokat, és a szereplők választhatnak egy sor viselkedési lehetőség közül, illetve megvalósíthatnak egy stratégiát annak érdekében, hogy optimalizálják a legvalószínűbb kimenetelű játékot. Formálisan a játékot *n* játékossal, stratégiai terekkel és kifizetési funkcióikkal írják le, *Si* és *Ui,* valamint minden *i* játékosra ($1 \leq i \leq n$):

$$G = \{n; S1, S2, \ldots, Sn; U1, U2, \ldots, Un\}$$

A leírás alapján a játékelméleti elemzés a játékosok magatartása valószínűségének feltárására összpontosít a stratégia megválasztásával kapcsolatban, ezáltal meghatározva a játék feltételezhető kimenetelét. A játékelméleti alapú modellek

8 Mercer, Edward: Causes of Cyber Crime. *It Still Works*. 2012 https://itstillworks.com/causes-cyber-crime-1846.html

9 Bode, M. A. – Alese, B. K. – Thompson A. F. – Iyare O.: A Bayesian Network Model for Risk Management in Cyber Situation, *World Congress on Engineering and Computer Science*, 22–24 October, San Francisco, USA, Vol. I. 2014; Peng Xie – Jason H Li – Xinming Ou – Peng Liu – Renato Levy: Using Bayesian networks for cyber security analysis. *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*. 2010; Kehe, W. – Shichao, Y. () An Information Security Threat Assessment Model based on Bayesian Network and OWA Operator, *Application of Mathematics in Information Science*, 8(2), 2014, pp. 833-838.; Xiaochun Xiao – Tiange Zhang – Gendu Zhang: Extended Abstract: Access Graph Based Risk Analysis for Network Information System, *2008 International Conference on Security Technology*. 2008; Li J. – Ou X. – Rajagopalan R.: Uncertainty and Risk Management in Cyber Situational Awareness. In.: Jajodia S. – Liu P. – Swarup V. – Wang C. (eds) *Cyber Situational Awareness. Advances in Information Security, vol 46*. Springer, Boston, MA. 2010; Muckin, Michael: A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization. *Lockheed Martin*, 2015, https://pdfs.semanticscholar.org/be09/f7a16eb4a379e698d8f42100fd8a91943a0c.pdf?_ga=2.174468898.1462599916.1542278052-1960495995.1540548768

10 Christopher J. Alberts – Audrey J. Dorofee – James F. Stevens – Carol Woody: *Introduction to the OCTAVE approach.* Software Engineering Institute, 2003.

11 Yazar, Z.: *A qualitative risk analysis and management tool*. CRAMM. SANS Institute, 2002.

teljesítmény- és költségelőnyöket mutatnak a számítógépes rendellenességek kezelésével kapcsolatos egyéb modellekkel szemben.

A továbbiakban néhány játékelméleti alapú számítógépes biztonsági kockázatkezelési modellezést és bizonyos számítógépes biztonsági kockázatkezeléssel foglalkozó kutatási munkák áttekintését mutatjuk be. A játékelméletnek a kiberbiztonsági kockázatkezelésre és a levont következtetésekre vonatkozó erősségeit és gyengeségeit szintén érintjük.

A számítógépes hálózatok biztonságának elemzésére kétszereplős sztochasztikus játszma felvázolásával is született játékelméleti modell. A Carnegie Mellon University munkatársai: Kong-wei Lye és Jeannette M. Wing[12] a Nash-egyensúlyi helyzetet[13] nemlineáris programmal számolták ki, s így alkottak valóságos stratégiákat.

A globális hálózatok drámai változáson mennek keresztül, ami folyamatosan növeli a hálózat méretét, az összekapcsolhatóságát és a hozzáférhetőséget, ennek következtében pedig fokozza azok sebezhetőségét. Számos politikai dokumentum is hangsúlyozta a számítógépes biztonság fontosságát a modern társadalom jóléte szempontjából. Az Egyesült Államok nemzeti biztonsági stratégiája[14] 2001. szeptember 11-ét követően pontosan leírta a kibertér biztosítására a prioritásokat: a fenyegetések és sebezhetőségek csökkentését, a tudatosságot és a képzést, valamint a nemzetbiztonságot és a nemzetközi együttműködést.[15] A kiberbiztonság eléréséhez ugyanakkor fejlett technológiai feltételek is szükségesek.

A Lockheed Martin kötelékébe tartozó ORINCON Information Assurance munkatársa, Samuel N. Hamilton együttműködve más számítástechnikai intézetek munkatársaival[16] felvázolták a játékelmélet azon területeit, amelyek relevánsak az információs hadviselés szempontjából. A tanulmány néhány olyan forgatókönyvet elemzett, amelyek több potenciális cselekvési tervet mutatnak be a várható eredményekkel és esetleges forgatókönyvekkel.

Az Iowa State University kutatói, Anirban Chakrabarti és Govindarasu Manimaran[17] az internet infrastruktúrájára összpontosított a támadások és a biztonság kontextusában. Más kutatásokkal szemben, melyek főként az adatátvitel biztonságára helyezték a hangsúlyt, ez a kutatás a bizalmi kapcsolatok eltérő infrastrukturális ellátottságából adódó biztonsági kérdéseket modellezte.

---

12 Kong-wei Lye – Jeannette Wing: Game Strategies in Network Security. *International Journal of Information Security*, 4(1–2), 2005, pp. 71–86.

13 Egy mátrixjátéknál egyensúlyi helyzetről beszélünk (azaz megtaláltuk a játék Nash egyensúlyi helyzetét), ha egyik játékosnak sem éri meg egyoldalúan változtatni a stratégiáján egyensúlyi helyzet esetében.

14 The National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

15 Roy Sankardas – Charles Ellis – Sajjan Shiva – Dipankar Dasgupta – Vivek Shandilya – Qishi Wu: A survey of game theory as applied to network security. In.: *2010 43rd Hawaii International Conference on System Sciences*. Honolulu, IEEE, 2010. pp. 1–10.

16 Samuel N. Hamilton – Wendy L. Miller – Allen Ott – O. Sami Saydjari: Challenges in Applying Game Theory to the Domain of Information Warfare. In.: *4th Information survivability workshop*. 2002.

17 Chakrabarti Anirban – Govindarasu Manimaran: Internet Infrastructure Security: A Taxonomy. *IEEE Network*, 16(6), 2002, pp. 13–21.

A University of Delaware és a UCLA kutatói, Jelena Mirkovic és Peter Reiher[18] az elosztott szolgáltatás-megtagadással járó támadások és védelemi stratégiák osztályozását végezte el, hangsúlyozva a támadások közötti hasonlóságokat és a támadások stratégiáinak legfontosabb tulajdonságait.

A fizikai felületek támadásai, főként a kommunikációt zavaró és lehallgatásos támadások száma napjainkban gyarapszik, s a vezetéknélküli hálózatokban jelentősége tovább nő. A University of Houston munkatársa, Zhu Han norvég és francia kutatókkal együtt[19] a hasznos adatokat továbbító források és a kommunikációt zavaró[20] nem offenzív szereplők interakcióit elemezte játékelméleti modellek segítségével. Az ilyen adattovábbítást vagy kommunikációt zavaró rendszerek alapvetően szolgáltatóként lépnek fel, s a szolgáltatásukért pénzt kérnek, így köztük piaci verseny alakul ki. A zavarás hatékonyságát és a zavaró szolgáltatási ár beállítását a szerzők a Stackelberg-modellel elemzik.

A fentebb említett Han és munkatársai célja leginkább az volt, hogy egy olyan decentralizált rendszert tervezzenek, amely megvédi a közvetített adatokat, s így lehetetlenné tegye, hogy a lehallgatók megkapják az adatcsomagokat még akkor is, ha ismerik az adó/vevő által használt kódolási/dekódolási sémákat.

A University Of Southern California munkatársai, João P. Hespanha és Stephen Bohacek[21] olyan útvonalválasztó játékokat vizsgáltak meg, amelyekben a támadó megpróbálja keresztezni az adatcsomagok útját egy számítógépes hálózatban. A hálózat tervezőjének olyan útválasztási irányelveket kell kidolgoznia, amelyek elkerülik a támadók felügyelete alatt lévő kapcsolatokat.

A FRIARS számítógépes védelmi döntési rendszert ugyancsak a Lockheed Martin Orincon Corporation munkatársai dolgozták ki az ezredfordulón, John McInerney vezetésével.[22] Ez a visszacsatolásvezérlő rendszer képes önállóan reagálni az automatizált rendszertámadásokra. A szerzők a Markov döntési folyamattal modellezik a rendszert: egy egyszerű játékkal és súlyozott véletlenszerű leválasztással a kiválasztott működtetőktől.

Paul Syverson[23] a U.S. Naval Research Laboratory (az Egyesültállamok Haditengerészetének Kutatólaboratóriuma) munkatársa jó és gonosz csomópontokról ír, és a sztochasztikus játékok használatát javasolja az analízisben. A Stanford University

---

18 Jelena Mirkovic – Peter Reiher: A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communications Review*, 34(2), 2004, pp. 39–54.

19 Zhu Han – Ninoslav Marina – Mérouane Debbah – Are Hjørungnes: Physical layer security game: interaction between source, eavesdropper, and friendly jammer. *EURASIP Journal on Wireless Communications and Networking 2010*. 2009: 452907. https://doi.org/10.1155/2009/452907

20 A zavarás (jamming) a vezetéknélküli hálózatokat kihasználó támadások egyik formája. Lényegében egyszerűen megtagadja a szolgáltatást az engedélyezett felhasználóknak, mivel a törvényes forgalom akadályozza az illegális forgalom azt felülmúló gyakoriságát.

21 Jőao P. Hespanha – Stephan Bohacek: Preliminary Results in Routing Games. *Proceedings of the 2001 American Control Conference*, 2002/3: pp. 1904–1909.

22 McInerney, John – Stephen Stubberud – Saquib Anwar – Stephen Hamilton: FRIARS: A Feedback Control System for Information Assurance. Using a Markov Decision Process. *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology*, 2001, pp. 223–228.

23 Syverson, Paul F.: A different look at secure distributed computation, *Proceedings 10th Computer Security Foundations Workshop*, London, IEEE, 1997. pp. 109–115.

munkatársai Sergio Marti vezetésével[24] a MANET számára egy olyan behatolás-érzékelő rendszersémát[25] javasoltak, amely két különböző modulból áll: a Watchdog időzítőből és az útvonalirányítóból (a biztonságos távoli jelszó, Secure Remote Password bővítményeként).

A Stevens Institute of Technology (Hoboken) munkatársai Yu Liu vezetésével[26] ugyancsak játékelméleti keretet javasoltak a vezeték nélküli ad-hoc hálózatokon keresztül történő támadó–védő csomópontok közötti kölcsönhatások elemzésére. Elemzésük a vezeték nélküli ad-hoc hálózatokban megjelenő biztonsági problémákkal foglalkozik, a potenciálisan rosszindulatú csomópont és a védelmi csomópont közötti interakciók modellezését játékelméleti keret segítségével oldják meg. Minden játékos megpróbálja maximalizálni a nyereményét: a támadó a lehető legnagyobb kárt akarja tenni a hálózatban, miközben a védő az energiaköltségek korlátozásával próbálja maximalizálni védelmezői képességeit, az IDS-sel történő hatalmas adatforgalom figyelemmel kísérése miatt.

Első javaslatuk egy „statikus játék", amely a védő számára áttekintést nyújt a biztonsági helyzetről: a kockázatokról és a megfigyelés költségeiről. A modell alaphelyzetében a védelmező minden versenytársról eleve rosszindulatot feltételez. A csatlakozási pontok típusai – vagyis, hogy tényleg rosszindulatúak vagy normálisak – nem teljes információt jelentenek, azokra tehát a Bayes-i dinamikus keretrendszert[27] alkalmazzák. Így egy visszacsatolást hoznak létre, ami megengedi a védelmezőnek, hogy kiinduló feltételezését módosítsa a megfigyelt akciók fényében. Így jön létre a tökéletes Bayes-i egyensúly, melyben – a monitorozási rendszernek köszönhetően – a rosszindulatú csomópontokra koncentrálódó támadások valószínűsége a védelmező rosszhiszemű előfeltevésének erősödésével együtt nő.

A szolgáltató és a támadó közötti interakciók modellezésére szolgáló behatolás-érzékelő játékokat eredetileg Kodialam és Lakshman,[28] a Bell Laboratories munkatársai dolgozták ki. A kétszemélyes zéróösszegű játszmában a szolgáltató úgy igyekszik maximalizálni a hasznát, hogy a sikeres leleplezés valószínűségét próbálja növelni, miközben a támadó megpróbálja minimálisra csökkenteni annak valószínűségét, hogy az IDS kimutassa jelenlétét.

---

24 Sergio Marti – T.J. Giuli – Kevin Lai – Mary Baker: Mitigating routing misbehavior in mobile ad hoc networks. In.: *MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking*. Boston, 2000. pp. 255–265.

25 Intrusion Detection Systems (IDS) – behatolásérzékelő rendszerek.

26 Yu Liu – Cristina Comaniciu – Hong Man: Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection. *International Journal of Security and Networks*, 1(3–4), 2006. pp. 243–254.

27 A Bayes-játék egy olyan játék, amelyben a játékosok hiányos információval rendelkeznek a többi játékosról. Ilyen hiányos ismeret lehet az ellenfél kifizetéseiről (nyereségek), vagy a támadás valószínűségéről, melyeket feltételezéssel helyettesít a játékos. Amikor a védekezőnek *a priori* statisztikai ismeretei vannak a szomszédok típusairól (barátságos vagy ellenséges), azt statikus Bayesi-játékban lehet modellezni. Az ellenfél tevékenységének megfigyeléséből származó adatokat (támadás vagy annak hiánya) időben elrendezve egy fejlődési modellt kapunk. Ez utóbbit tekintjük dinamikus Bayesi-modellnek.

28 Murali Kodialam – T.V. Lakshman: Detecting Network Intrusions via Sampling: A Game Theoretic Approach. *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*. 2003/3: pp. 1880–1889.

A University of Texas munkatársai Afrand Agah vezetésével[29] a szenzorhálózatban a támadás-védelem problémáját kétszereplős, nem kooperatív, nem zéróösszegű játékként értelmezte. A modell teljes információs, tehát a játékosok nyeresége határozza meg stratégiájukat. Ez a munka azonban éppen a teljes információ feltételezése miatt nem is lett sikeres, számunkra azonban érdekes példa, mely ékesen bizonyítja, hogy a Harsányi megteremtette játékelméleti környezet olyan változást hozott az alkalmazott tudományok területén, melyet nem lehet visszafordítani.

A biztonsági rendszerek Stackelberg-játszmára épülő belső logikája

A biztonsági rendszerek játékelméleti alapmodellje a Stackelberg-játék.[30] Elsőkként tehát a generikus biztonsági problémát, úgy fogalmazzuk meg, mint egy normál formájú Stackelberg-játékot. A biztonság játék két játékosból áll, egy védőből Θ, és egy támadóból Ψ. A játékosok nem szükségképpen egyének, csoportok is lehetnek, ahol a csoporttagok együttműködnek egy közös stratégia megvalósításában, mint például egy fegyveres testület vagy egy terrorista szervezet. Minden játékosnak van egy lehetséges tiszta stratégiákból álló készlete, $\sigma_\Theta \in \Delta_\Theta$ és $\sigma_\Psi \in \Sigma_\Psi$. Egy vegyes stratégia lehetővé teszi a játékos számára, hogy valószínűségi eloszlással tiszta stratégiát játsszon, $\delta_\Theta \in \Delta_\Theta$ és $\delta_\Psi \in \Sigma_\Psi$. Az egyes játékosok kifizetéseit minden lehetséges közös tiszta stratégiájú kimenetre azonos módon határozzuk meg a védő számára, és a támadó számára is: $\Omega_\Theta : \Sigma_\Psi \times \Sigma_\Theta \rightarrow R$. A kifizetési funkciókat a vegyes stratégiákra a szokásos módon állapítjuk meg, átvéve a tiszta stratégiákon alapuló várakozásokat.

Eddig a játék leírása a normál formájú játékot követi. A Stackelberg-játékok sajátossága, hogy az másképpen különbözteti meg a játékosokat: a kezdőt, aki az első lépést teszi és az erre reagáló követőt, aki egy haszon-maximalizáló, önérdekkövető választ ad, s akinek ugyanakkor lehetősége van megfigyelni a kezdő játékos stratégiáját, mielőtt lép. A biztonsági játszmákban a védő a Stackelberg-vezető, a támadó pedig a követő. Ez modellezi a rosszindulatú támadók azon lehetőségét, hogy a támadások tervezésekor felderítést alkalmazzanak. Ebben a modellben a kiszámítható védelmi stratégiák sérülékenyek: ki vannak téve az ellenség felderítő pozíciójának. Formálisan a támadó stratégiája a Stackelberg biztonsági játékban olyan funkció, amely minden kezdő stratégiára megfelelő válaszstratégiát ad: $F_\Psi : \Delta_\Theta \rightarrow \Delta_\Psi$.

A játékelméletben alkalmazott standard megoldás egy Nash-egyensúly: olyan stratégiai profil minden játékos számára, ahol egyetlen játékos sem nyerhet, ha egyoldalúan egy másik stratégiára vált.[31] A Stackelberg-egyensúly a Nash-egyensúly

---

29 Afrand Agah – Sejal K. Das – Kalyan Basu: A Game Theory Based Approach for Security in Wireless Sensor Networks. In.: *IEEE International Conference on Performance, Computing, and Communications, 2004*. Phoenix, 2004. pp. 259–263.

30 A Stackelberg vezetési modell egy stratégiai játék, melyet a közgazdaságban használtak elsőként. A játékban vezető cég lép először, majd sorra lépnek a követő vállalkozások egymás után. A vezető előzetesen tudja, hogy a követő megfigyeli a lépését, a követőnek így nincs lehetősége, hogy egy nem Stackelberg vezetői döntési helyzettel számoljon a jövőben, amit a vezető tud is, és a legjobb válaszlépése is valóban az.

31 Martin J. Osbourne – Ariel Rubinstein: *A Course in Game Theory*. Oxford: Oxford University Press, 1994.

finomított változata, amelyet a Stackelberg-játékokra dolgoztak ki. Ez egy részjáték-tökéletes egyensúly, mivel itt minden játékos kiválasztja a megfelelő választ, azzal az eredeti bármelyik részjátékra Nash-egyensúlyt kap. Ez kizárja az egyensúlyi útvonalon kívül eső (hiteltelen) támadások által létrehozott Nash egyensúlyi profilokat.

A részjáték-tökéletes egyensúly önmagában nem garantálja a Stackelberg-játékok megoldását, mivel a követők számos stratégiával szemben közömbösek lehetnek. Két sajátos Stackelberg-egyensúlyi helyzet létezik, melyeket először George Leitmann,[32] a University of California Berkeley professzora fogalmazott meg a hetvenes években, s melyeket „erős" és „gyenge" stratégiáknak nevezett el.[33] Az erős forma esetén a követő mindig az optimális stratégiát feltételezi a vezetőről, míg a gyenge formában a követő a legrosszabb stratégiát feltételezi a vezetőről. Erős Stackelberg-egyensúly minden Stackelberg-játékban létezik, azonban gyenge Stackelberg-egyensúly nem feltétlenül.[34] A kezdő ráadásul gyakran azzal is kiválthatja az erős formát, hogy lépésével véletlenül kerül közel az egyensúlyi helyzethez.[35] A következőkben az erős Stackelberg-egyensúlyt vesszük alapul, mivel ez a leggyakrabban alkalmazott forma a szakirodalomban.[36]

Egy stratégiapár (δ_Θ, F_Ψ) akkor alkot erős Stackelberg-egyensúlyt, ha a következők igazak rá:

A vezető a legjobb-válasz játszmát játssza:

$$\Omega_\Theta (\delta_\Theta, F_\Psi (\delta_\Theta)) \geq \Omega_\Theta (\delta'_\Theta, F_\Psi (\delta'_\Theta)) \; \forall \; \delta'_\Theta \in \Delta_\Theta.$$

A követő a legjobb-válasz játszmát játssza:

$$\Omega_\Psi (\delta_\Theta, F_\Psi (\delta_\Theta)) \geq \Omega_\Psi (\delta_\Theta, \delta_\Psi) \; \forall \; \delta_\Theta \in \Delta_\Theta, \delta_\Psi \in \Delta_\Psi.$$

A követő optimálisan szakítja meg a kötéseket a vezetővel:

$$\Omega_\Theta (\delta_\Theta, F_\Psi (\delta_\Theta)) \geq \Omega_\Theta (\delta_\Theta, \delta_\Psi) \; \forall \; \delta_\Theta \in \Delta_\Theta, \delta_\Psi \in \Delta^*_\Psi (\delta_\Theta),$$

ahol $\Delta^*_\Psi (\delta_\Theta)$ a követő legjobb-válaszának a készlete.

Az, hogy a kezdő előnyhöz jut-e az elköteleződéssel, attól függ, hogy a vegyes stratégiáknál ez megengedett vagy sem. Egy tiszta stratégia iránti elköteleződés jó vagy rossz is lehet a vezető számára; például a kő–papír–olló játékban a tiszta

32 Leitmann, George: On generalized Stackelberg strategies. *Optimization Theory and Applications*, 26(4), 1978, pp. 637–643.

33 Michele Breton – A. Alj – A. Haurie: Sequential Stackelberg equilibria in two-person games. *Optimization Theory and Applications*, 59(1), 1988, 71–97.

34 Tamer Basar – Geert J. Olsder: *Dynamic Noncooperative Game Theory*. San Diego: Academic Press, 1982.

35 Bernhard von Stengel – Shmuel Zamir: Leadership with commitment to mixed strategies. *Technical Report London School of Economics-Centre for Discrete and Applicable Mathematics* (LSE-CDAM)-2004-01, CDAM Research Report, 2004.

36 Vincent Conitzer – Tuomas Sandholm: Computing the optimal strategy to commit to. In *ACM Conference on Electronic Commerce,* 2006.; Osbourne – Rubinstein, *i.m.*, Paruchuri, P., J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus: Playing games with security: An efficient exact algorithm for Bayesian Stackelberg games. In *AAMAS-08*, pp. 895–902, 2008.

stratégia iránti elköteleződés mindenképpen vesztes stratégia. Azonban a vegyes stratégia melletti kitartás mindig csak gyengén növeli a vezető kifizetését a játszma egyensúlyi profiljában.[37] Egy Stackelberg biztonsági játékban a meghatározott politika a védő (vezető) felelőssége, ugyanakkor egy hiteles véletlenszerűsített biztonság politika előnyt jelent. A bemutatott modellek lehetővé teszik a védekező vegyes stratégiák iránti elkötelezettséget.

Önszerveződő és anonim hálózatok védelme

Amint látható, számtalan területen alkalmazzák a nem teljes információs játékelméleti modellezést a kiberbiztonságban. A személyes adatok védelme, s természetesen a kezdetektől meghatározó gazdasági területek mellett a felhőalapú számítástechnikai biztonsági kérdések egyaránt fontos új fejlődési utakat jelentenek. Az infrastruktúra elleni támadások kivédésén túl, az önszerveződő hálózatok számára biztonsági protokollok kidolgozása céljából, vagy a behatolás-feltárás javítására ugyancsak alkalmasak.

Guanhuan Yan és munkatársai a Los Alamos National Laboratory-ban[38] az elosztott szolgáltatás-megtagadással járó támadások (DDoS) védelmére dolgozott ki egy Bayes-i játékelméleti modellt. Véletlen változók és Bayes-i hálózat segítségével hoztak létre egy összetett, dinamikus modellt. A szimulációjuk azt mutatta ki, hogy a támadó által látszólag nem kapcsolódó védelmi paraméterek végső soron befolyásolják a támadó stratégiai választását, és a védelmi megközelítés különböző szintjei helyettesíthetők egymással, azaz nem szükséges a DDoS-támadásokkal szembeni összes védelmi megközelítések párhuzamos bevezetése. Munkájuk hátterében a valóságos helyzetekben nem működő Nash-egyensúlyi helyzetek helyett a k-szintű modellezés[39] áll.[40]

---

37 Bernhard von Stengel – Shmuel Zamir: Leadership with commitment to mixed strategies. *Technical Report London School of Economics-Centre for Discrete and Applicable Mathematics* (LSE-CDAM)-2004-01, CDAM Research Report, 2004.

38 Guanhua Yan – Ritchie – Alex Kent – David Wolpert: Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense. In.: *Proceedings of the 2012 ACM conference on Computer and communications security*. Raleigh, CCS, 2012. pp. 553–566.

39 A k-szintű modellben a játékosok típusait a furfangosságuk (smartness) szerinti rangsoruk határozza meg, ez analóg az ismételt racionalizáltsági szintekkel. Ennek fontos eleme, hogy az intelligenciát, amit minden döntési modell előfeltételez nagyon nehéz meghatározni, így előzetesen csak egy általánosabb koncepció feltételezhető: a furfang. A játékosok evolúciós modellje tehát egy nagyon egyszerű naiv, nem stratégiai zéró-szintű típussal kezdődik, aki a többi játékos figyelembevétele nélkül lép. A következő lépést meghozó játékos mindenkit naivnak tekint, az azt követő mindenkit első szintűnek tekint, és így tovább. Stahl, Dale O: Evolution of Smartn Players. *Games and Economic Behavior*, 5(4), 1993, pp. 604–617.

40 Valós szereplők sokszor nem úgy döntenek, ahogy a Nash-egyensúly alapján várnánk. Például képzeljünk el, hogy egy osztályteremben minden tanuló 0 és 100 között választ egy számot, s a játékot az nyeri, aki az átlag feléhez legközelebb esik. Természetesen 50 fölött butaság lenne számot választani. Erre a feltevésre alapozva azonban már 25 fölött is értelmetlen lenne számot választani. Még tovább gondolva pedig a 12,5 fölötti számokat lehetne kizárni a választásból. A gondolatsor vége, hogy nullánál nagyobb számot nem érdemes választani. Egy ilyen Nash-egyensúlyi választással ellentétben a valóságban ritkán választják a nullát, ahogy azt kísérletek is kimutatták. A k-szintű elemzés ilyen játékhelyzetekben több eltérő gondolkodásmódot vesz figyelembe.

Az internethez folyamatosan kapcsolódó intelligens mobil eszközök széles körben történő használata számos sikeres helyzetalapú szolgáltatás fejlesztését hívta életre. Annak ellenére, hogy a helymeghatározás hasznos, egyúttal a felhasználók magánéletének csorbulását is okozhatja. A szoftverfejlesztés területén komoly erőfeszítéseket tettek, hogy a helyzet-meghatározással együtt minimalizálhatóvá váljon a személyes információk közlése. Reza Shokri, az Ecole Polytechnique Fédérale de Lausanne munkatársa[41] néhány éve többedmagával a „geotagging"[42] -ból származó kockázatok kivédésére dolgozott ki játékelméleti alapon nyugvó algoritmusokat, melyek kivédik a felhasználó bármilyen típusú bejelentkezéséből származó helyzet-meghatározáshoz kötődő támadási lehetőségeket. Számításba vették azt is, hogy a komoly támadások nem csupán a felhasználók által zavart helyszín-adatokat ismerik, hanem a zavaráshoz használt algoritmust is.

Az anonim hálózatépítés hatékony mód a hálózati felhasználók személyes információinak megőrzésére. Az anonimitás biztosítását azonban nehéz elérni anélkül, hogy közben a hálózati teljesítményt ne csökkentsük.[43] Ezért szükséges az optimális csomópontok megtalálása az adatátviteli sémák módosításához, így az anonimitást a szolgáltatás minőségének csökkentése nélkül maximalizáljuk. Az anonimitás optimalizálásának problematikáját Venkitasubramaniam és Tong,[44] a Lehigh University és a Cornell University munkatársai valamint az Institute of Electrical and Electronics Engineers (IEEE)[45] tagjai, a hálózattervező és a támadó közötti kétszereplős, zéróösszegű játszmaként írták le. Az ellenfél feladata: kiválasztani a csomópontok egy részhalmazát, hogy nyomon követhesse az útvonalak anonimitását. A hálózattervező feladata pedig az anonimitás maximalizálása azáltal, hogy kiválasztja a csomópontok egy részhalmazát, s így, a független átviteli menetrendek létrehozásával, elkerüli az áramlásérzékelést. Ebben a kétszereplős játékban a véges hálózatok általános kategóriájához egyedülálló nyeregpont-egyensúly tartozik. A nyeregpontban a hálózati tervező stratégiája biztosítja, hogy az ellenfél által ellenőrzött csomópontok bármelyik részhalmaza azonos mennyiségű információt tárjon fel az útvonalakról. A párhuzamos reléhálózatok egy adott osztályára vonatkozóan az elméletet az optimális teljesítmény-kompromisszumok és az egyensúlyi stratégiák tanulmányozására alkalmazzák. Amikor a csomópontok adó-irányított jelzést alkalmaznak, az átvitel és az anonimitás közötti kompromisszumot analitikusan jellemzik a hálózati paraméterek és a megfigyelt csomópontok részeinek függvényében. Az eredményeket az anonimitás, a megfigyelt és a nagy hálózatokban rejtett relék részeinek vizsgálatára alkalmazzák.

---

41 Reza Shokri – Jean-Pierre Hubaux – Jean-Yves Le Boudec: Protecting Location Privacy: Optimal Strategy against Localization Attacks. In *Proceedings of the 2012 ACM conference on Computer and communications security*. Raleigh, CCS, 2012. pp. 617–627.

42 Olyan eljárás, amelyben földrajzi azonosító metaadatokat adnak különböző médiafájlokhoz (kép, video, honlap, SMS, QR kód, RSS (Rich Site Summary) hírfolyam frissítésekhez), például amikor egy fényképhez a GPS koordinátákat társítja az eszköz. Így egy térinformatikai metaadat jön létre.

43 Lei Xu – Chunxiao Jiang – Yi Qian – Yong Ren: *Data Privacy Games*. Cham, Springer, 2018.

44 Parv Venkitasubramaniam – Lang Tong: A Game-Theoretic Approach to Anonymous Networking. *IEEE/ACM Transactions on Networking*, 20(3), 2012, pp. 892–905.

45 A világ legnagyobb műszaki szakembereket tömörítő szövetsége, központja New Yorkban található.

Gazdaság és hálózati biztonság

Minthogy a játékelméletet legelsőként a közgazdaságtan számára hozták létre, a kiberbiztonság területén is kiemelkedő a gazdaságtudományi alkalmazása. Számos klasszikus közgazdasági elmélet és modell alkalmazható bizonyos gazdasági problémákra (például a biztonsági beruházásokra, a biztonsági ösztönzőkre és a biztonságpolitikai döntéshozatalra).

Fontos a hálózati infrastruktúrát megvédeni a támadásoktól, hiszen a nagysebességű adatkapcsolat megtámadása a nagyméretű adatok elvesztéséhez vagy késleltetéséhez vezet. Xun Xiao és a City University of Hong Kong további munkatársai[46] az internetszolgáltató korlátozott biztonsági erőforrásainak előzetes allokációjához tervezett játékelméleti modell alapján biztonsági rendszert. A kétszereplős, zérósszegű játékban a nyereségeket a hálózati áramlás maximalizálásával mérték. Mivel egynél több kritikus globális régió bevonásával nincs Nash-egyensúlyi helyzet, kevert stratégiákat alakítottak ki úgy, hogy minden régió egyensúlyi helyzetének a valószínűségi eloszlásával modellezték a maximális nyereségek eléréséhez legmegfelelőbb stratégiát. A Ford–Fulkerson-tételt[47] alkalmazva arra jutottak, hogy ha minden védelmi erőforrást egy minimális vágáshoz rendelnek hozzá, miközben több ilyen készlet is létezik, a kiválasztás „kevert stratégiával" a legoptimálisabb.

Számos kutatás elemezte azokat a hálózati mellékhatásokat, amiket a biztonság területén az önző befektetői magatartás és a kedvezőtlen koordinációs arány[48] okozott, illetve tanulmányozta a hálózati biztonság ösztönző rendszereit.[49] Megvizsgálták a hálózati biztonsági játék egyensúlyi teljesítményét. Ezek a modellek kifejezetten figyelembe vették a hálózati topológiát, a játékosok különböző költségfüggvényeit és egymáshoz viszonyított fontosságát. A stratégiai játékokban a koordinációs arány nagyon nagy lehet, és a hálózat méretével, valamint a játékosok függőségével és egyensúlyhiányával arányosan nő. Mindez az önző beruházások súlyos hatékonysági problémáit mutatja. Nem meglepő, hogy az ismétlődő játékok legjobb egyensúlya általában kedvezőbb teljesítményt nyújt, ahol lehetőség van társadalmi optimum elérésére, ha ez nem ütközik az egyéni érdekekkel. Olyan stratégiákat alkalmazni ismétlődő játékokban, melyek a részjáték-tökéletes Nash-egyensúlyt[50] támogatják, egyben a játékosok közötti jobb kommunikációt és együttműködést igényli.

---

46 Xun Xiao – Minming Li – Jianping Wang – Chunming Qiao: Optimal resource allocation to defend against deliberate attacks in networking infrastructures. *2012 Proceedings IEEE INFOCOM*. Orlando, IEEE, 2012.

47 A Ford és Fulkerson maximális folyam-minimális vágás tétele szerint egy irányított gráfban a maximális folyam nagysága egyenlő a minimális vágás méretével.

48 Az a költség, amit legrosszabb esetben fizethetnek a játékosok a központi koordináció hiányáért, azaz a legkedvezőtlenebb Nash-egyensúly és a legjobb Nash-egyensúly társadalmi költségének az aránya.

49 Libin Jiang – Venkat Anantharam – Jean Walrand: How Bad are Selfish Investments in Network Security? *IEEE/ACM Transactions on Networking*, 19(2), 2011, pp. 549–560.; Lelarge, Marc: Coordination in Network Security Games: A Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications*, 30(11), 2012, pp. 2210–2219.

50 A játékosok stratégiái akkor vannak részjáték-tökéletes egyensúlyban, amennyiben a játék minden részjátékában Nash-egyensúlyt mutatnak.

A felhők, mint infrastruktúra-alapú szolgáltatások

Meglehetősen nehézkes a biztonság olyan új infrastrukturális környezetben, mint a felhőalapú számítástechnika. Több felhasználó egyidejű kiszolgálása, a forrásmegosztás és a kiszervezés (outsourcing) olyan kihívásokat jelentenek, amire a játékelmélet adhat választ. A felhőt használó nyilvános felhasználók olyan közös platformokat vesznek igénybe, mint például a hiperfelügyelő, s más közös erőforrásaik, például az utolsó szintű gyorsítótár (LLC), memória sávszélesség vagy az I/O puffer. Ezek mind olyan eszközök, amik a kölcsönös függőségből adódó kockázatokat tovább növelik. Ilyen helyzetekben bármelyik felhasználó kockázatos magatartása (például biztonság mellőzése) mások számára is veszélyforrást jelent, számos szervezet éppen ezért óvakodik csatlakozni, s a felhő nyújtotta előnyökből részt kérni.[51] A legkézenfekvőbb megoldás, ha a mások döntéseitől való függést úgy csökkentjük, hogy nem egyszerűen elérhetővé tesszük a virtuális számítógépet a fizikai eszközök biztonsági rendszere számára, hanem a szereplők lehetséges magatartásait és kölcsönhatásait modellezzük.

Tovább bonyolítja az interakciós helyzetet, ha a felhő utasítást adhat a számítógépnek. Így valójában három szereplő játszmáját kell modellezni, amiben két eltérő játék alakul ki: egy a támadó és a felhő szolgáltatója között, egy pedig a felhő és a számítógép hagyományos interakciójára épülő jelölő játszmaként.[52] Ráadásul a felhőalapú szolgáltatások sok esetben egyáltalán nem meggyőzőek azok biztonságát illetően, így játszma alakul ki a kliensek és szolgáltatók között, ami egy piaci mechanizmus részévé is válik, tulajdonképpen a szolgáltatók közötti verseny révén.

A biztonság a felhő alapú számítástechnika egyik legfontosabb kérdése. Az a szolgáltató, amelyik meggyőzően biztosítja az ügyfelei számára, hogy azok alkalmazásai biztonságosak lesznek, több ügyfelet szerez. Az University of Victoria kutatói, Abdulaziz Aldribi és Issa Traoré[53] egy dinamikus nem kooperatív játékelméleti modellt alkalmaztak a biztonság átláthatóságára vonatkozó olyan megoldások megfogalmazására és elemzésére, amelyeket a szolgáltató az ügyfélnek felajánlhat, és amely egyben a biztonság nagyobb átláthatóságát követeli meg a szerződés létrejöttéhez. Ráadásul az átláthatósági biztonsági játék egyensúlyi elemzése révén a szolgáltató jobban megértheti az ügyfelek stratégiáit.

---

51 Charles A. Kamhoua – Luke Kwiat – Kevin A. Kwiat – Joon S. Park – Ming Zhao – Manuel Rodriguez: Game Theoretic Modeling of Security and Interdependency in a Public Cloud. In *2014 IEEE 7th International Conference on Cloud Computing*. Anchorage, IEEE, 2014. pp. 514–521.

52 Jeffrey Pawlick – Sadegh Farhang – Quanyan Zhu: Flip the Cloud: Cyber-Physical Signaling Games in the Presence of Advanced Persistent Threats. In Khouzani M., Panaousis E., Theodorakopoulos G. (eds.) *Decision and Game Theory for Security*. GameSec 2015. Lecture Notes in Computer Science, vol 9406. Cham, Springer, 2015. pp. 289–308.

53 Abdulaziz Aldribi – Issa Traore: A Game Theoretic Framework for Cloud Security Transparency. In Meikang Qiu, Shouhuai Xu, Moti Yung, Haibo Zhang (eds.) *Network and System Security*. NSS 2015. Lecture Notes in Computer Science, vol 9408. Cham, Springer, 2015. pp. 488–502.

Záró gondolatok

A felhasználók bizalma nem csupán piaci létkérdése a szolgáltatóknak, hanem a szolgáltatás működésének alapját is jelenti. A Harsányi János munkásságán alapuló nem teljes információs játékelmélet alkalmazása a biztonsági kérdések átláthatóságát illetően új területe a felhőalapú számítástechnikának, de várható, hogy a jövőben is meghatározó lesz abban.

Harsányi János munkáját az tette leginkább időtállóvá, hogy nagyfokú matematikai absztrakciója mellett mégis életszerű maradt. A nemzetbiztonság, katonai elemzések, biztonságpolitika és gazdasági stratégiai kutatások és alkalmazott módszerek alapjait mai napig a nem teljes információs játékelméleti módszerek képezik. Tulajdonképpen a történelem adta feltételek teremtették meg a nem teljes információn alapuló modellezés hátterét a hidegháborúban, ám az azt követő évtizedekben ezek a körülmények egyre meghatározóbbakká váltak nem csupán a résztvevő szereplők egymáshoz való viszonyában, hanem azok technikai eszköztárában is.

FELHASZNÁLT IRODALOM

Agah, Afrand – Sejal K. Das – Kalyan Basu: A Game Theory Based Approach for Security in Wireless Sensor Networks. In.: *IEEE International Conference on Performance, Computing, and Communications, 2004*. Phoenix, 2004. pp. 259–263.

Alberts, C. – Dorofee, A. – Stevens, J. – Woody, C.: *Introduction to the OCTAVE approach*. Software Engineering Institute, 2003.

Abdulaziz Aldribi – Issa Traore: A Game Theoretic Framework for Cloud Security Transparency. In Meikang Qiu, Shouhuai Xu, Moti Yung, Haibo Zhang (eds.) *Network and System Security*. NSS 2015. Lecture Notes in Computer Science, vol 9408. Cham, Springer, 2015. pp. 488–502.

Alpcan, Tansu – Tamer Başar: *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, Cambridge University Press, 2011.

Bernhard von Stengel – Shmuel Zamir: Leadership with commitment to mixed strategies. *Technical Report London School of Economics-Centre for Discrete and Applicable Mathematics* (LSE-CDAM)-2004-01, CDAM Research Report, 2004.

Bode, M. A. – Alese, B. K. – Thompson A. F. – Iyare O.: A Bayesian Network Model for Risk Management in Cyber Situation, *World Congress on Engineering and Computer Science*, 22-24 October, San Francisco, USA, Vol. I. 2014

Breton, Michele – A. Alj – A. Haurie: Sequential Stackelberg equilibria in two-person games. *Optimization Theory and Applications*, 59(1), 1988, 71–97.

Chakrabarti Anirban – Govindarasu Manimaran: Internet Infrastructure Security: A Taxonomy. *IEEE Network*, 16(6), 2002, pp. 13–21.

Conitzer, Vincent – Tuomas Sandholm: Computing the optimal strategy to commit to. In *ACM Conference on Electronic Commerce,* 2006.

Fielder, Andrew – Emmanouil Panaousis – Pasquale Malacaria – Chris Hankin – Fabrizio Smeraldi: Game Theory Meets Information Security Management. In.: Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, Thierry Sans (eds.) *ICT Systems Security and Privacy Protection. SEC 2014*. IFIP Advances in Information and Communication Technology, vol 428., Berlin, Heidelberg, Springer, 2014. pp. 15–29.

Hamilton, Samuel N. – Wendy L. Miller – Allen Ott – O. Sami Saydjari: Challenges in Applying Game Theory to the Domain of Information Warfare. In.: *4th Information survivability workshop*. 2002.

Han, Zhu – Ninoslav Marina – Mérouane Debbah – Are Hjørungnes: Physical layer security game: interaction between source, eavesdropper, and friendly jammer. *EURASIP Journal on Wireless Communications and Networking 2010*. 2009: 452907. https://doi.org/10.1155/2009/452907

Hespanha, Jõao P. – Stephan Bohacek: Preliminary Results in Routing Games. *Proceedings of the 2001 American Control Conference*, 2002/3: pp. 1904–1909.

Jiang, Libin – Venkat Anantharam – Jean Walrand: How Bad are Selfish Investments in Network Security? *IEEE/ACM Transactions on Networking*, 19(2), 2011, pp. 549–560.

Kamhoua, Charles A. – Luke Kwiat – Kevin A. Kwiat – Joon S. Park – Ming Zhao – Manuel Rodriguez: Game Theoretic Modeling of Security and Interdependency in a Public Cloud. In *2014 IEEE 7th International Conference on Cloud Computing*. Anchorage, IEEE, 2014. pp. 514–521.

Kehe, W. – Shichao, Y: An Information Security Threat Assessment Model based on Bayesian Network and OWA Operator, *Application of Mathematics in Information Science*, 8(2), 2014, pp. 833–838.

Kodialam, Murali – T.V. Lakshman: Detecting Network Intrusions via Sampling: A Game Theoretic Approach. *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*. 2003/3: pp. 1880–1889.

Leitmann, George: On generalized Stackelberg strategies. *Optimization Theory and Applications*, 26(4), 1978, pp. 637–643.

Lelarge, Marc: Coordination in Network Security Games: A Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications*, 30(11), 2012, pp. 2210–2219.

Li J. – Ou X. – Rajagopalan R.: Uncertainty and Risk Management in Cyber Situational Awareness. In.: Jajodia S., Liu P., Swarup V., Wang C. (eds) *Cyber Situational Awareness. Advances in Information Security, vol 46*. Springer, Boston, MA. 2010

Liu, Yu – Cristina Comaniciu – Hong Man: Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection. *International Journal of Security and Networks*, 1(3-4), 2006. pp. 243–254.

Lye, Kong-wei – Jeannette Wing: Game Strategies in Network Security. *International Journal of Information Security*, 4(1–2), 2005, pp. 71–86.

Marti, Sergio – T.J. Giuli – Kevin Lai – Mary Baker: Mitigating routing misbehavior in mobile ad hoc networks. In.: *MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking*. Boston, 2000. pp. 255–265.

Osbourne, Martin J. – Ariel Rubinstein: *A Course in Game Theory*. Oxford: Oxford University Press, 1994.

McInerney, John – Stephen Stubberud – Saquib Anwar – Stephen Hamilton: FRIARS: A Feedback Control System for Information Assurance. Using a Markov Decision Process. *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology*, 2001, pp. 223–228.

Menache, Ishai – Asuman Ozdaglar: *Network Games: Theory, Models, and Dynamics*. *Synthesis Lectures on Communication Networks*. Berkeley, Morgan & Claypool Publishers, 2011.

Mercer, Edward: Causes of Cyber Crime. *It Still Works*. 2012
https://itstillworks.com/causes-cyber-crime-1846.html

Mirkovic, Jelena – Peter Reiher: A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communications Review*, 34(2), 2004, pp. 39–54.

Muckin, Michael: A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization. *Lockheed Martin*, 2015,
https://pdfs.semanticscholar.org/be09/f7a16eb4a379e698d8f42100fd8a91943a0c.pdf?_ga=2.174468898.1462599916.1542278052-1960495995.1540548768

Paruchuri, P. – J. P. Pearce – J. Marecki – M. Tambe – F. Ordonez – S. Kraus: Playing games with security: An efficient exact algorithm for Bayesian Stackelberg games. In AAMAS-08, pp. 895–902, 2008.

Pawlick, Jeffrey – Sadegh Farhang – Quanyan Zhu: Flip the Cloud: Cyber-Physical Signaling Games in the Presence of Advanced Persistent Threats. In Khouzani M., Panaousis E., Theodorakopoulos G. (eds.) *Decision and Game Theory for Security*. GameSec 2015. Lecture Notes in Computer Science, vol 9406. Cham, Springer, 2015. pp. 289–308.

Peng Xie – Jason H Li – Xinming Ou – Peng Liu – Renato Levy: Using Bayesian networks for cyber security analysis. *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*. 2010

Roy, Sankardas – Charles Ellis – Sajjan Shiva – Dipankar Dasgupta – Vivek Shandilya – Qishi Wu: A survey of game theory as applied to network security. In.: *2010 43rd Hawaii International Conference on System Sciences*. Honolulu, IEEE, 2010. pp. 1–10.

Shokri, Reza – Jean-Pierre Hubaux – Jean-Yves Le Boudec: Protecting Location Privacy: Optimal Strategy against Localization Attacks. In.: *Proceedings of the 2012 ACM conference on Computer and communications security*. Raleigh, CCS, 2012. pp. 617–627.

Stahl, Dale O: Evolution of Smartn Players. *Games and Economic Behavior*, 5(4), 1993, pp. 604–617.

Stengel, Bernhard von – Shmuel Zamir: Leadership with commitment to mixed strategies. *Technical Report London School of Economics-Centre for Discrete and Applicable Mathematics* (LSE-CDAM)-2004-01, CDAM Research Report, 2004.

Syverson, Paul F.: A different look at secure distributed computation, *Proceedings 10th Computer Security Foundations Workshop*, London, IEEE, 1997. pp. 109–115.

Tamer Basar – Geert J. Olsder: *Dynamic Noncooperative Game Theory*. San Diego: Academic Press, 1982.

The National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Venkitasubramaniam, Parv – Lang Tong: A Game-Theoretic Approach to Anonymous Networking. *IEEE/ACM Transactions on Networking*, 20(3), 2012, pp. 892–905.

Wang, Yuan – Yongjun Wang – Jing Liu – Zhijian Huang – Peidai Xie: A Survey of Game Theoretic Methods for Cyber Security. In.: *2016 IEEE First International Conference on Data Science in Cyberspace*. Changsha, IEEE, 2016. pp. 631–636.

Xiao, Xun – Minming Li – Jianping Wang – Chunming Qiao: Optimal resource allocation to defend against deliberate attacks in networking infrastructures. *2012 Proceedings IEEE INFOCOM*. Orlando, IEEE, 2012

Xiaochun Xiao – Tiange Zhang – Gendu Zhang: Extended Abstract: Access Graph Based Risk Analysis for Network Information System, *2008 International Conference on Security Technology*. 2008

Xu, Lei – Chunxiao Jiang – Yi Qian – Yong Ren: *Data Privacy Games*. Cham, Springer, 2018.

Yan, Guanhua – Ritchie – Alex Kent – David Wolpert: Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense. In.: *Proceedings of the 2012 ACM conference on Computer and communications security*. Raleigh, CCS, 2012. pp. 553–566.

Yazar, Z.: *A qualitative risk analysis and management tool*, CRAMM. SANS Institute, 2002.