ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

HABILITÁCIÓS TÉZISFÜZET

PROF. DR. CSISZÁR PÉTER
EGYETEMI TANÁR, FŐISKOLAI DOCENS

IKT és mesterséges intelligencia az információbiztonság funkciójában

BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA

Budapest, 2022.09.22.

Tartalomjegyzék

I. A kutatás előzményei 3

II. Új tudományos eredmények 4

III. A kutatás és a bemutatott eredmények hatása, visszhangja 12

IV. Irodalmi hivatkozások listája 16

V. A tézispontokhoz kapcsolódó tudományos közlemények 21

VI. További tudományos közlmények 23

I. A kutatás előzményei

A Villamosmérnöki Kar (távközlési szak) elvégzése után a „Telekom Szerbia” állami távközlési vállalatnál helyezkedtem el, ahol a gyakorlatban a modern digitális távközlési rendszerek számos aktuális problémáival és kihívásaival találkoztam, illetve azok hatékony megoldásának szükségességével. A különböző informatikai területek rohamos fejlődése és távközlési alkalmazása, valamint az IT biztonság egyre aktuálisabb problémái meghatározták tudományos érdeklődésem irányát. Először a magiszteri dolgozat (23), majd a doktori értekezés (24) közvetlenül kapcsolódott a kellő szintű infrastrukturális biztonság biztosításának problematikájához a mobilbanki és az elektronikus üzletviteli internetes forgalom területén. A telekommunikációs szférában eltöltött 20 év után a belgrádi Bűnügyi- és Rendőrtudományi Egyetemre kerültem, ahol a szokásos távközlési és informatikai témák mellett intenzív alkalmazásukkal is találkoztam olyan speciális területeken, mint a digitális nyomtan, kiberbűnözés, hacker-ellenes eszközök, támadásérzékelő és -megelőzési rendszerek és mások.

Tudományos munkámat a fentiek figyelembevételével 4 területre lehet osztani: információ (IT) biztonság, számítógépes és telekommunikációs hálózatok, alkalmazott informatika, valamint a mesterséges intelligencia és a gépi tanulás alkalmazása - a számítógépes hálózatok biztonságának biztosításában.

Az IT biztonság részeként a számítógépes hálózatok biztonságának – hálózati szintű – kérdéskörét kutattam, különös tekintettel a behatolásjelző és megelőző rendszerekre, valamint a tűzfalakra. Ezenkívül, foglalkoztam a biztonság alkalmazási szintű megvalósításának módjaival is.

Érdeklődésem másik területe a számítógépes és a telekommunikációs hálózatok, és ezen belül a szórt spektrumú technikákra helyeztem a hangsúlyt (a modern mobil távközlésben való széleskörű alkalmazásuk miatt), a szoftveresen definiált hálózatokra, valamint a drónellenes megoldásokra.

Kutatásaim harmadik területe az alkalmazott informatika. Ezen belül számos olyan gyakorlati problémát elemeztem, amely megfelelő szoftvereszközök alkalmazásával megoldható. Például, a tanulók tudásának értékelése adaptív tesztekkel, optimalizálási feladatok megoldása immunológiai algoritmusokkal, arcfelismerési és -azonosítási módszerek kép alapján, fizikai objektumok térbeli elhelyezkedésének feltárása, valamint a virtuális valóság alkalmazása multimédiás rendszereken belül.

A mesterséges intelligencia alkalmazása számos előnnyel jár az informatikai biztonság területén. Ennek értelmében, elemeztem a gépi tanulás szempontjait az internetes tűzfaladatokon, a fuzzy logika előnyeit a hálózati anomáliák kimutatásának funkciójában, valamint a mesterséges immunhálózatok alkalmazását a folytonos funkciók optimalizálására.

II. Új tudományos eredmények

A tudományos opuszomat alkotó területeken több publikációm is megjelent, amelyek bemutatják az elért tudományos eredményeket.

IT biztonság

Ezen a területen belül a hálózati forgalmi anomáliák felderítésének különböző megközelítéseivel foglalkoztam, a támadások felderítése céljából [Fengmin, 2003; Siris, 2004]. Egyik közülük egy fix küszöbű algoritmus, amely az első deriválton alapul (V.1. cikk). Ez egy hálózatfigyelő szoftverrel könnyen megvalósítható, beépített aktiválási („triggerelési") funkciókat használó algoritmus, amelynek bizonyos betanítási periódusra van szüksége ahhoz, hogy normál forgalmi körülmények között minél pontosabban meghatározza a forgalmi görbe első deriváltjának maximális értékét.

A folyamatfigyelés exponenciálisan súlyozott mozgó átlag (*Exponentially Weighted Moving Average*-EWMA) statisztikája a V.2. cikk kutatásunk tárgyát képezte, azzal a céllal, hogy meghatározzuk annak alkalmasságát a behatolásészlelésben való alkalmazásra [Ye, Chen and Borror, 2004]. A korábban támadás nélküli tesztforgalmi mintán a szintezési tényező optimalizálása után, a hálózati router által kapott forgalmi mintákon ellenőriztük az algoritmus működését. A cél az volt, hogy olyan paraméterértékeket kapjunk, amelyek nem vezetnek hamis pozitív eredményhez (a támadást észlelő riasztás, amely a valóságban nem történt meg), ami a kutatás végén sikerült is.

A rendelkezésre álló irodalom nem teljesen biztos abban, hogy a valószínűség -eloszlás milyen típusai legjobban modellezik a számítógépes hálózati forgalmat [Lazarevic, Kumar and Srivastava, 2005]. Így például az egyenletes, a *Poisson*, a lognormal, a *Pareto* és a *Rayleigh* eloszlások voltak használva különböző alkalmazásokban. A V.3. cikkben bemutatott statisztikai elemzés célja annak bemutatása, hogy a hálózati forgalmi minták ferdesége és kurtózisa a megfigyelt időintervallumban kritérium lehet a megfelelő eloszlási típus kiválasztására. A cikkben a hisztogram létrehozása és a hálózati forgalmi minták valószínűség eloszlása szintén meg vannak vitatva és analizálva egy valós eseten. Az elemzett eloszlási

típusok közül, a kurtózis és a ferdeség mint a hálózati forgalom leírásának kritériumai alapján, a megfelelő eloszlások az egyenletes, a normál, a *Poisson*, a lognormál és a *Rayleigh* eloszlás. Azt is ki van kimutatva, hogy a hisztogramban a leggyakoribb hálózati minta megközelítőleg megegyezik a forgalom átlagával.

A futásidejű alkalmazások önvédelmi technológiája (*Runtime Application Self-Protection Technology*-RASP) egy viszonylag új biztonsági hozzáállás, amelynek szélesebb körű bevezetése a közeljövőben várható. Ennek a technológiának a középpontjában jelenleg a Java és a .NET platformok sebezhetősége áll [Paul and Evans, 2015]. A V.4. cikk, a tipizálás mellett, bemutatta a RASP előnyeit és hátrányait. A kétségtelen előnyök ellenére, nem egy független és átfogó megoldás a szoftver biztonságának biztosítására [Lane, 2016]. A kipróbált és bevált hagyományos biztonsági módszerekkel kombinálva a RASP hatékony megoldást jelent a rosszindulatú tevékenységek megelőzésére.

A behatolásészlelés a számítógépes hálózati rendszerekbe történő behatolások (támadások) monitorozására és rögzítésére szolgál, amelyek megpróbálják veszélyeztetni azok biztonságát. Számos különböző megközelítés létezik a statisztikai behatolásészlelésre [Spathoulas and Katsikas, 2010]. Az egyik a viselkedésanalízis, és ennek megfelelően egy modell alapú algoritmus be van mutatva. A V.5. cikk foglalkozik a reguláris forgalom szabályozási határainak meghatározásával is, leíró statisztikák használatával. Ezen túlmenően, a cikk még foglalkozik a hálózati forgalom átlagos és maximális értéke közötti összefüggés statisztikai megfogalmazásával, és tárgyalja a behatolásészlelés időtényezőjét.

Távközlés és számítógép-hálózatok

A szórt spektrum egy távközlési jelek továbbítására használt technika [Singh, 2013; Pickholtz, Schilling and Milstein, 1982]. Ez a téma viszonylag összetett, és kihívást jelenthet a hallgatók számára. Így az *Octave* programozási nyelv bekerült a távközlési rendszerek tantervébe, mint egyik hatékony eszköz, amely segíti a hallgatókat a szórt spektrum elveinek megértésében [Chen 2009; Westall 2003]. A V.6. cikk célja a szórt spektrumtechnika oktatási módszerének és távközlési alkalmazásának kidolgozása volt, azzal a céllal, hogy a téma érthető legyen a hallgatók számára. A szórt spektrum elméletének megértéséhez szükséges előzetes tudás tesztelésére előtesztet végeztünk, amely a távközlés alapjaiból általános fogalmakra utal. Az e területről szükséges elmélet mélyebb megismerése érdekében a hallgatóknak mérnöki gyakorlatból származó példákat kellett megoldaniuk nyílt forráskódú *Octave* szoftverrel [Baeza-Baeza, Perez-Pla and Coque, 2015], valamint számítási feladatokat mindkét módszerre

vonatkozóan a szórt spektrum technológiában [Chen, 2009]. Bebizonyosodott, hogy a megfelelő anyag vizualizálásának köszönhetően a kísérleti csoport tanulói részletesebben megértették a szórt spektrumú jelek generálásának módszerét és az egyes paraméterek hatását a részjelekre, azon tanulók vonatkozásában, akiknek nem volt lehetőségük használja az *Octave*-ot. A kutatás eredményei arra engednek következtetni, hogy az *Octave*-hoz hasonló szoftvereket a hagyományos tanítási és tanulási módszerek kiegészítéseként be kell illeszteni az olyan kurzusokba, mint a Távközlési rendszerek.

A V.7. cikk áttekintést és elemzést ad a szoftver által definiált technológiákról a hagyományos számítógépes hálózatok aktuális problémáival összefüggésben [Tiwari, 2013; Stallings, 2013]. A virtualizációs folyamat a szoftver által meghatározott hálózati architektúra alapja. Analizálva voltak a szoftveresen definiált hálózatok alapkoncepciói, valamint a felhőkörnyezetben való megvalósítása és konfigurálása *OpenStack* nyílt forráskódú szoftverrel *Microsoft Hyper*-V hypervisorral. A kutatás gyakorlati része kimutatta, hogy egy szoftveresen definiált hálózat implementálása egy meglévő szabványos hálózatba viszonylag egyszerűen megvalósítható, folyamatosan nyílt forráskódú keretrendszerben maradva. Az összes létező hálózati funkció megmarad, és lehetőség van további hálózati műveletek, például forgalomfigyelés biztosítására is teljesen nyílt forráskódú környezetben.

Az 5G (ötödik generáció) a mobilhálózati technológia legújabb generációját képviseli, amelynek bevezetése több országban folyamatban van, vagy már be van fejezve. Ennek a mobilrendszernek tagadhatatlan előnyei vannak elődeihez képest [Hussain et al, 2019; Basin et al, 2018]. A V.8. cikk áttekintést ad az 5G hálózatok biztonsági szempontjairól a rendelkezésre álló szakirodalomból származó adatok alapján. A hitelesítés és a kulcskezelés alapvető folyamatok a mobilhálózatok biztonsága szempontjából. Éppen ezért a hangsúly a cikkben ezen biztonsági módszerek kidolgozására és a szolgáltatások korábbi 4G rendszerrel való összehasonlítására helyeződik [Shaik et al., 2016]. Az 5G hitelesítési összetevői eltérnek a 4G-től az új szolgáltatásalapú architektúra miatt. Ezenkívül a 3GPP és a nem-3GPP hozzáférési hálózatok egyenlőbb bánásmódban részesülnek. Ezenkívül, 5G esetén a felhasználói készülék az otthoni hálózat nyilvános kulcsát használja az állandó azonosító titkosításához, mielőtt azt hálózatba küldené. A 4G-ben ez az azonosító tiszta szövegként (titkosítatlan) kerül elküldésre. A kulcsstruktúra hosszabb az 5G-ben, mint a 4G-ben a két további kulcs megvalósítása miatt. Az 5G-hitelesítés számos területen javítja a 4G-hitelesítést, beleértve az egységes hitelesítési struktúrát, a jobb felhasználói identitásvédelmet, az otthoni hálózat jobb vezérlését és a kulcsok

nagyobb szétválasztását. Az 5G hitelesítés azonban nem hiányosságoktól mentes. A felhasználókövetési képesség például az 5G-ben továbbra is megvalósítható.

A V.9. cikk bemutatja a drónok gyártása során alkalmazott technológiákat és elvek széles választékát. Ezt figyelembe véve megállapítható, hogy a védekezés ellenük nagyon összetett feladat [Hauzenberger, 2015; Rodday, 2016]. Ez gyakorlatilag azt jelenti, hogy nincs egyetlen megbízható védekezési megoldás sem, de ahhoz, hogy minél nagyobb sikereket érjünk el ezen a területen, célszerű több megközelítést kombinálni. A drón-ellenes sikeres védelemben az elsődleges szerep az észlelésük. Ebben az értelemben a megfelelő radarrendszer, más érzékelőkkel kombinálva, nagyon hatékony. A cikk további jelentősége a tényleges drónellenes technológiák műszaki jellemzőinek elemzésében rejlik. Ezek ismerete lehetővé teszi, hogy az adott védelmi követelményektől függően, bizonyos megoldásokra összpontosítsunk. A cikk arra is rámutatott, hogy a drónészlelés kognitív megközelítése nagyobb pontosságot és alkalmazkodóképességet tesz lehetővé, köszönhetően a radartechnológiákban alkalmazott tanulóalgoritmusoknak.

A már ismert fogalmak mellett, a V.10. cikk különböző simítási sémák összehasonlító elemzését mutatja be. A statisztika optimalizálási lehetőségek is meg vannak tárgyalva [Douglas, 2005; Statistical Quality Control, 2006]. Az exponenciális simítás folyamatának javítása érdekében, a mozgó trimmelt átlag és a mozgó medián viselkedését számítógépes hálózati környezetben vizsgáltuk a leggyakrabban használt mozgóátlaghoz viszonyítva. Ebből a célból többféle eloszlás van alkalmazva a hálózati forgalom modellezésére. A Matlab szoftvercsomag segítségével véletlenszerű számsorozatokat generáltunk minden eloszlási típushoz, a hálózati forgalom szimulálására. Meg van mutatva, hogy a mozgóátlag és a mozgó trimmelt átlag jobban követi az eredeti forgalom görbéjét. Ugyanakkor, a kiugrók és a kiugrók-nélküli helyzetet összehasonlítva, az átlagos négyzetes hiba (*Mean Squared Error* - MSE) legkisebb relatív ugrását a mozgóátlagra és a mozgó mediánra határoztuk meg. Ez a következtetés indokolja alkalmazásukat a kiugró értékek negatív hatásának kiküszöbölésére, és pozitívan befolyásolja a számítógépes hálózatok forgalomszabályozásának általános szintjét.

Alkalmazott informatika

A V.11. cikk bemutatja és elemzi a számítógépes adaptív tesztelés alkalmazásának eredményeit a C++ programnyelv tudásértékelésében [Carlson, 1994; Eggen, 2017; Takacs, Szakal and Csikos Pajor, 2002]. A kutatás résztvevői egy műszaki főiskola számítástechnika szakos hallgatói voltak, átlagéletkoruk 20 év. A kutatás két éven keresztül zajlott. A kutatásban

összesen 199 hallgató vett részt. A hallgatók két csoportját, a kísérleti és a kontrollcsoportot figyelték meg. A kísérleti csoport hallgatói a számítógépes adaptív tesztet, a kontrollcsoport hallgatói pedig a papír-ceruza tesztet végezték el. A számítógépes adaptív teszt tudásértékelésre való alkalmazásának hatásainak meghatározására az adaptív teszt a Matlab szoftvercsomagban volt megvalósítva [Ju and Bork, 2005]. A teszt feleletválasztós kérdésekből állt, öt válaszlehetőséggel. A teszt kérdései három csoportba voltak osztva, nehézségi szint szerint (könnyű, közepes és nehéz). A pontszámot a nehézségi szint alapján számítottuk ki. A nehéz kérdések több pontot értek, mint a könnyűek. A vizsgázók ugyanannyi kérdésre válaszolhattak helyesen, de a vizsgázó jobb pontszámot kap, ha feltételezi, hogy helyesen válaszolt a nehezebb kérdésekre. A kutatás eredményei azt mutatták, hogy statisztikailag szignifikáns különbség volt a kontroll és a kísérleti csoport eredményei között. A számítógép-adaptív tesztet végző hallgatók magasabb átlagpontszámot értek el, mint a hagyományos tesztet teljesítők.

A V.12. cikkben javasolva van egy technikai rendszer egyszerű koncepciója és megvalósítása, fizikai objektumok térbeli helymeghatározására, alacsony minőségű hardverek optimalizálási módszereivel. Ez a számítógépes rendszer számítógépekből, szoftveralkalmazásokból, videokamerákból, számítógépes hálózatból, aktív és passzív hálózati berendezésekből állt [T'Orazio, Guaragnella and Leo, 2004]. A rendszer alapötlete a háromszögelés elve legalább 4 nagy képkocka/másodperc számú kamera vizuális képei és időadatai alapján. A rendszer ezután a számított térbeli helyadatok felhasználásával fotorealisztikus grafikus 3D animációt készít az objektum pályájáról és a térről [Kirillov, 2017]. A kísérleti eredmények és egy valós rendszer számítógépes szimulációja azt mutatta, hogy a javasolt koncepció javítja az objektumok térbeli helymeghatározását és a 3D grafikát közepes minőségű műszaki berendezéseken.

A számítógépek csökkenő költségeiért felelős technológiai fejlődés, valamint a számítógépes adaptív szoftverek fejlődése elősegítette a számítógépes adaptív tesztelést (*Computer Adaptive Testing*-CAT) a felsőoktatásban, alternatívát kínálva a hagyományos papír-és ceruzavizsgák helyett. A tétel-válasz elmélet segítségével statisztikailag lebonyolított CAT-tesztelési folyamat képes reagálni az egyes vizsgázókra, a megfelelő nehézségi fokú tesztelemekkel célban tartva a vizsgázókat. Az adaptív számítógépes tesztek alapvető célja, hogy a vizsgázó kérdéseket elég nagy kihívás elé állítsa, de ne legyen túl nehéz, ami frusztrációhoz és zűrzavarhoz vezetne [Jacobsen et al., 2011; Carlson 1994; Eggen, 2017]. A V.13. cikk egy *Matlab*-ban megvalósított CAT rendszert mutat be, annak fejlesztési lépéseivel együtt. Az alkalmazás futhat *Matlab* parancsablakból, vagy lehet önálló alkalmazást is készíteni, amelyhez nem szükséges a *Matlab* telepítése. A kérdések .txt fájlba vannak írva. Ez lehetővé teszi a vizsgáztató számára, hogy

könnyedén módosítsa és bővítse a kérdésadatbázist, anélkül, hogy bármilyen programozási nyelv szintaxisát ismerné. Az egyetlen követelmény, hogy a vizsgáztató (csak ez kötelező) egy előre meghatározott kérdésírási formátumot kövessen. A program lehetővé teszi a hallgatói tudás tesztelését C++ nyelven.

A V.14. cikk globális áttekintést ad a mesterséges immunrendszerekről a számítástechnikában és azok megvalósításáról [de Castro and Timmis, 2002; de Castro and von Zuben, 2000; Lopez, Morales and Nino, 2013]. Az immunológiai algoritmus teljesítményét az optimalizálási problémák megoldásában az *Optimization Algorithm Toolkit* segítségével elemeztük, különös tekintettel a paraméterértékek hatásának meghatározására. Kimutattuk, hogy az ilyen típusú algoritmusok különösen érzékenyek az algoritmus működését befolyásoló paraméterek kiválasztására.

A V.15. cikk elemzést ad néhány számítástechnikai optimalizálási algoritmusról és azok megvalósításáról a bináris karakterfelismerés problémájának megoldásában [Weinman, Learned-Miller and Hanson, 2009; Yokobayashi and Wakahara, 2006; Gerkey and Thrun, 2005]. Ezen algoritmusok teljesítményét az *Optimization Algorithm Toolkit* segítségével elemztük, különös tekintettel a paraméterértékek hatásának meghatározására. Kimutattuk, hogy az ilyen típusú algoritmusok az algoritmusok szignifikáns érzékenységet mutattak a paraméterek kiválasztását illetően, ami hatással volt az algoritmus működésére. Ilyen értelemben az optimális érték meglétét, valamint a rendkívül elfogadhatatlan értékeket megállapítottuk.

A digitális kriminalisztika elengedhetetlen a számítógépes bûnözés sikeres ellenállásához. Számos kihíváshoz kapcsolódik, beleértve a számítógépes és digitális eszközök gyors változásait, a számítógépes rendszerek és hálózatok elleni kifinomultabb támadásokat, valamint az ICT-rendszerekkel való visszaélések gyors növekedését. Ahhoz, hogy a törvényszéki vizsgálat sikeres legyen, számos fontos lépést meg kell fontolni és meg kell tenni. Mivel a digitális kriminalisztika viszonylag új terület a többi kriminalisztikai tudományághoz képest, folyamatos erőfeszítések folynak a vizsgálati szabványok kidolgozására és a digitális kriminalisztikai vizsgálatok szerkezetének kialakítására [Kruse and Heiser, 2002; Reith, Carr and Gunsch, 2002]. A V.16. cikk áttekintést ad a digitális kriminalisztikai vizsgálatok várható globális fejlődési irányairól, valamint a terület aktuális trendjeiről.

A megfelelő hardver és szoftver platformok fejlődése az olyan alkalmazások intenzív növekedését eredményezte, amelyek a virtuális világban helyezték el tevékenységüket. Ez

különleges élményt tesz lehetővé a felhasználók számára – a virtuális valóság (*Virtual Reality*-VR) élményét. A VR fejlesztésére szolgáló szoftver sok szempontból specifikus és igényes [Cruz–Neira, Fernandez and Portales, 2018; Sutcliffe and Gault, 2004; Pant and Neelakantam, 2017]. A V.17. cikk nagy sokszínűségét szem előtt tartva, áttekintést ad a kategorizálásról, az általános jellemzőkről és az értékelési módszerekről. Ezen túlmenően a VR-szoftverfejlesztés általános alapelvei is különösen kidolgozottak, hangsúlyt fektetve a játékok létrehozására és tesztelésére.

Sok olyan behatolás, amely a számítógépes és hálózati rendszerek biztonságát próbálja veszélyeztetni, az események intenzitásának változásában nyilvánul meg. Mivel az exponenciálisan súlyozott mozgóátlag (EWMA) statisztika képes figyelni az események előfordulási gyakoriságát azok intenzitása alapján, ez a technika megfelelő a kontrol határokon alapuló algoritmusokban való megvalósításhoz [Hunter, 1986; Lucas and Saccucci, 1990; Ye et al. 2003]. A V.18. cikkben található kutatás kimutatta, hogy ennek az algoritmusnak a szokásos alkalmazása a számítógépes hálózati forgalomra, ahogyan azt az ipari folyamatokban alkalmazzák, nem ad elfogadható eredményeket. Ez a cikk a lehetséges optimalizálási módszereket is áttekinti.

A mesterséges intelligencia és a gépi tanulás

A V.19. cikk mesterséges immunhálózatok alkalmazásával foglalkozik a folytonos funkció optimalizálásban [Brownlee, 2007; Ulutas, 2011]. Az immunológiai algoritmusok teljesítménye az *Optimization Algorithm Toolkit* segítségével volt elemezve. Meg volt mutatva, hogy a CLIGA algoritmus rendelkezik messze a leggyorsabb konvergenciával, a legjobb eredménnyel - a szükséges iterációk számát tekintve az elemzett folytonos függvényen. A teszteredmények alapján arra a következtetésre lehetett jutni, hogy a meghatározott futási idő alatt a legalacsonyabb iterációszámot az opt-IA algoritmus érte el, ezt követik a CLONALG és CLIGA algoritmusok.

A neurális hálózatok (*Neural Networks* - NN) számos megvalósítása a gépi tanulás részeként, a hálózati tűzfalszabályok modellezése [Maloof, 2006; Kalita 2013; Kunal 2019]. Erre a célra egy megfelelő adatkészlet volt használva, amely szabványos forgalmi attribútumokat, valamint a *Weka* szoftvercsomag többrétegű perceptronok (*multilayer perceptron*-MLP) modellezésére és tesztelésére alkalmas képességét tartalmazza. A V.20. cikk célja az internetes tűzfal NN modelljének létrehozása és vizsgálata volt, és paramétereinek optimalizálása, amely a legjobban szimulálja a szabályok működését. Megállapítást nyert, hogy a rejtett rétegekben lévő neuronok

száma, a tanulási sebesség, a momentum és a tanulási iterációk száma (*epochs*) befolyásolja a pontosságot, míg a százalékos felosztás és a kötegméret (*batch size*) hatása figyelmen kívül hagyható. Emellett el volt végezve a különböző aktiválási funkciók veszteségének értékelése NN környezetben, előre meghatározott optimális paraméterekkel. Ezenkívül ki volt mutatva, hogy a következő algoritmusok biztosítják a legnagyobb pontosságot a tűzfaladatkészlet osztályozási problémáinak megoldásában: Random Forest, J48 és MLP. A tűzfal adatok klaszterezésének lehetőségét tekintve a cikk azt találta, hogy a k-means algoritmus nagyobb pontosságot és sebességet mutat, mint az EM és DBSCAN algoritmusok.

A V.21. cikk analizálja a mesterséges intelligencia (*Artificial Intelligence*-AI) megközelítésének általános jellemzőit a számítógépes infrastruktúra megfelelő szintű kiberbiztonságának biztosítása érdekében [Ganesh Babu et al., 2021]. Hangsúlyozza e tudományos terület biztonsági területen való alkalmazásának előnyeit, hátrányait és korlátait. A cikk emellett a mesterséges intelligencia különböző kategóriáira (például szakértői rendszerek, fuzzy logika és mesterséges neurális hálózatok) és az adatbányászatra összpontosít, és rámutat ezek sajátosságaira a behatolásészlelésben. Ezeket a funkciókat szem előtt tartva, meg lehet állapítani, hogy az AI még messze van attól, hogy az univerzális kiberbiztonsági megoldás legyen. Addig is a legjobb megközelítés a bevált kártevő-elhárító szoftverek és mesterséges intelligencia eszközök kombinációja lenne, így a kritikus infrastruktúráért felelősöknek ezt szem előtt kell tartaniuk a kiberbiztonsági stratégia kidolgozásakor.

Az anomália-észlelés a hálózati rendszerek forgalmi anomáliáinak figyelésére és rögzítésére szolgál. Számos anomália nyilvánul meg a hálózati események intenzitásának változásában. Mivel az EWMA vezérlődiagram képes figyelni az események előfordulási gyakoriságát azok intenzitása alapján, ez a statisztika megfelelő a szabályozási határokon alapuló algoritmusokban való megvalósításhoz. A szabványos EWMA algoritmus teljesítménye hatékonyabbá tehető az adaptív küszöb algoritmus logikájával és a fuzzy elmélet megfelelő alkalmazásával [Yu and Tsai, 2006; Senturk et al. 2014]. A V.22. cikk elemzi az EWMA statisztika és a fuzzy logika alkalmazásának elméleti lehetőségét a hálózati anomáliák kimutatására. Meg voltak vitatva a fuzzy szabályok különböző aspektusai, valamint a különböző tagsági funkciók, megpróbálva megtalálni a legmegfelelőbb választást. Ki volt mutatva, hogy a fuzzy logika bevezetése az anomáliák észlelésére szolgáló szabványos EWMA-algoritmussal megnyitja a hálózati támadások előzetes figyelmeztetésének lehetőségét. Emellett a fuzzy logika lehetővé teszi a rizikó mértékének pontos meghatározását.

III. A kutatás és a bemutatott eredmények hatása, visszhangja

A fent említett területeken végzett tudományos tevékenység és a publikált cikkek egyik eredményeként 4 tankönyvet és 2 monográfiát megjelentettem.

Emellett, az intézményben ahol dolgozom, 20 olyan hallgató mesterdolgozatának mentora voltam, akiket tematikusan a tudományos érdeklődési köröm inspirált:

1. V. Aksentijević, téma: *Electronic service for the prevention of the consequences of adverse meteorological conditions, air pollution and uv index on human health*

2. D. Milovanović, téma: *Implementation of (re)active IDS/IPS systems using mikrotik router os software*

3. D. Erlenvajn, téma: *Implementation of software defined networks using open code solutions*

4. Đ. Brenjo, téma: *Security of network systems using Nessus software*

5. M. Živković, téma: *Ethical hacking with Kali Linux operating system*

6. M. Kutlić, téma: *Comparative analysis of antimalware tools: Kaspersky, Avg and Nod*

7. J. Lukić, téma: *Network tools for ensuring security against DDOS attacks*

8. D. Vorkapić, téma: *Detecting network attacks by implementing Suricata software*

9. L. Rudan, téma: *Interception and monitoring of digital network traffic*

10. S. Vasilijević, téma: *Functionality of the Wireshark tool in a wireless environment - detection of the preparatory phase of an attack*

11. D. Mitrović, téma: *Testing the optimal wpa2-psk password strength for logging in a wireless environment using "Kali Linux" software tools*

12. S. Škrbić, téma: *Installation and use of keystroke logging software*

13. I. Košanin, téma: *Security aspects of mobile chat applications*

14. T. Aćimović, téma: *Digital forensics of e-mail for the purposes of detecting rigged offers in public procurement procedures*

15. Lj. Oluški, téma: *Data center architecture and security for processing and storing classified data*

16. V. Jovanović, téma: *Botnet network - principles of management and control, detection and prevention*

17. N. Ždraljević, téma: *Firewall in the function of computer network protection*

18. M. Radisavljević, téma: *Digital video surveillance systems: resistance to cyber attacks and protection methods*

19. A. Simić, téma: *Security aspects of 5G mobile networks*

20. P. Vukašinović, téma: *Enumeration of computer networks and assessment of their vulnerability by comparative analysis of open-source network scanners*

A szakterületemről bizonyos tantárgyak akkreditálva és bevezetve lettek az intézményem tantervébe.

Ezen kívül több mint 400 hivatkozás szerepel az MTMT adatbázisában (https://m2.mtmt.hu/gui2/?type=authors&mode=browse&sel=10083211), ebből több mint 50 doktori disszertáció. A terjedelem miatt, az alábbi szövegben csak három idézett közleményt sorolok fel, a többi az MTMT adatbázisában található:

1. P. Čisar; S. Maravić Čisar, *Optimized EWMA Control Charts in Function of Intrusion Detection*, In: Anon, A (eds.) Proceedings of the 9th International Symposium of Hungarian Researchers on Computational Intelligence (CINTI 2008), Bp, Hungary: BMF, Magyar Fuzzy Társaság (2008), pp. 387-396.

Szabadalom:

- C. Knittle: *Adaptive bit rate for data transmission*, US 8904027B2, https://patents.google.com/patent/US8904027B2/en

2. P. Čisar; S. Maravić Čisar: *Password - a Form of Authentication*, In: Szakál, A (eds.) SISY 2007, 5th International Symposium on Intelligent Systems and Informatics, Bp, Hungary: Budapesti Műszaki Főiskola (2007) pp. 29-32.

Doktori tézisek:

- Ruba: *A study of password recall, perceived memorability, and strength using BCIs* (2018),

https://www.proquest.com/openview/e76360e05bcad45c909d58929060be25/1?pq-origsite=gscholar&cbl=18750&diss=y

- H. Moritz: *Generating and Managing Secure Passwords for Online Accounts* (2018), https://tuprints.ulb.tu-darmstadt.de/7003/1/Generating%20and%20Managing%20Secure%20Passwords%20for%20Online%20Accounts.pdf
- L. Charlott: *On User Perception of Authentication in Networks* (2014), https://www.diva-portal.org/smash/get/diva2:834224/FULLTEXT01.pdf

3. P. Čisar; S. Maravić Čisar, *Skewness and Kurtosis in Function of Selection of Network Traffic Distribution*, Acta Polytechnica Hungarica Vol. 7, No. 2, pp. 95-106. (2010)

Mesterdolgozatok:

- H. Bai: *An Examination of Customers' Adoption of Restaurant Search Mobile Applications* (2015), http://orapp.aut.ac.nz/bitstream/handle/10292/9254/BaiH.pdf?sequence=3&isAllowed=y
- S. Atieno Wanga: *Sustainability of Kenya's Total Public Debt* (2013), http://erepository.uonbi.ac.ke/bitstream/handle/11295/93751/Wanga_Sustainability%20of%20Kenya%20s%20total%20public%20debt.pdf?sequence=1
- J. You: *Application of Machine Learning in the Big Data for Broiler Breeders Recorded by a Precision Feeding System* (2021), https://era.library.ualberta.ca/items/c2fedba8-5470-4db1-9958-9b246e7683a1
- R. Devonport: *Understanding perceptions of Human Resource competencies and effectiveness in the New Zealand and Australian hotel industry* (2016), https://openrepository.aut.ac.nz/bitstream/handle/10292/10575/DevonportR.pdf?sequence=3&isAllowed=y

Doktori tézisek:

- Y. S. Shuen: *Safety communication, safety culture, and safety leadership on safety participation among manufacturing employees* (2018), https://core.ac.uk/download/pdf/199242908.pdf
- N. N. Bekwa: *The development and evaluation of africanised items for multicultural cognitive assessment* (2016),

https://uir.unisa.ac.za/bitstream/handle/10500/23591/thesis_bekwa_nn.pdf?sequence=1&isAllowed=y

- C. Chipeta: *Analysis of South Africa's financial market relationship with business cycle indicators for financial stability* (2020), http://repository.nwu.ac.za/bitstream/handle/10394/34704/Chipeta_C_24705233.pdf?sequence=1
- Nyokangi, C. O. *Relative performance of the single index versus mean variance optimization in equity portfolio construction in Kenya* (2016), http://su-plus.strathmore.edu/handle/11071/4770
- F. Omelogo Obiora: *Effect of Neighborhood Features on BMI of African American adolescents in South Los Angeles* (2015), https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=2365&context=dissertations
- F. Galea: *The Development of an English-Maltese Assessment of Speed of Handwriting* (2021), https://www.um.edu.mt/library/oar/bitstream/123456789/92252/1/21PHDHS003.pdf
- B. Schneiderman Tuttle: *Examining the Correlation of Self-Compassion and Compassion Fatigue in Social Work Interns* (2022), https://www.proquest.com/openview/e8677504942a911ac10b5d35890e0231/1?pq-origsite=gscholar&cbl=18750&diss=y
- M. Kaumbuthu Harun: *Institutional Factors and Strategy Implementation in Public Secondary Schools in Selected Counties in Kenya* (2021), http://repository.kemu.ac.ke:8080/xmlui/bitstream/handle/123456789/1190/1.%20MUTEA%20-THESIS%20%20FINAL%205.10.21.pdf?sequence=1&isAllowed=y
- J. Ganesan: *Employer Perceptions of Factors Affecting Trade Union Effectiveness in Peninsular Malaysia*, (2015), https://www.proquest.com/openview/d0e1d710eb653044412114f221fde06e/1?pq-origsite=gscholar&cbl=2026366

IV. Irodalmi hivatkozások listája

G. Fengmin: *Deciphering Detection Techniques: Part II Anomaly – Based Intrusion Detection*, White Paper, McAfee Security, 2003

M. Douglas: *Introduction to Statistical Quality Control*, 5th Edition, John Wiley & Sons, 2005

Statistical Quality Control, www.wiley.com/college/reid/0471347248/samplechapter/ch06.pdf

L. de Castro, J. Timmis: *Artificial Immune Systems: A New Computational Intelligence Approach*, Springer, pp. 57–58, ISBN 978-1-85233-594-6, 2002

L. de Castro, F. von Zuben, *Artificial Immune Systems: Part II - A Survey of Applications*, Technical Report DCA-RT 02/00, 2000

G.Q. López, L.A. Morales, L.F. Niño: *Chapter 23-Immunological computation,* 2013, https://www.ncbi.nlm.nih.gov/books/NBK459484/

J. Brownlee: *Clonal Selection Algorithms*, CIS Technical Report 070209A, 2007

B. Ulutas, S. Kulturel-Konak: *A Review of Clonal Selection Algorithm and its Applications*, Artificial Intelligence Review, Springer, 2011

A. Greg, T. Chan: *Artificial Intelligence and National Security.* Cambridge, MA 02138: Belfer Center for Science and International Affairs, 2017

R. Ganesh Babu, M. Vijay, G. Parameswaran, C. Anandhan, S. Maurya: *Intrusion Detection Using Machine Learning in Sensor Network*. IOP Conf. Series: Materials Science and Engineering, 2021, doi:10.1088/1757-899X/1055/1/012089

K. Kalita: *Network Anomaly Detection: A Machine Learning Perspective*, 2013

Kunal, M. Dua: *Machine Learning Approach to IDS: A Comprehensive Review*. 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 117-121, 2019, doi:10.1109/ICECA.2019.8822120.

M. A. Maloof: *Machine Learning and Data Mining for Computer Security*, 2006. London: Springer-Verlag London Limited.

N. Ye, Q. Chen and C.M. Borror: *EWMA forecast of normal system activity for computer intrusion detection*. IEEE Transactions on Reliability, Vol. 53, Issue 4, 2004, pp. 557-566.

A. Kirillov, *Motion Detection Algorithms*, 2017. http://www.codeproject.com/Articles/10248/Motion-Detection-Algorithms.

T'Orazio, C. Guaragnella, M. Leo, *Pattern Recognition, A New Algorithm for Ball Recognition Using Circle Hough Transform And Neural classifier*, Institute_of_Intelligent_Systems_for_Automation_I ISSIA, Rome Italy, 2004.

G. Spathoulas, S. Katsikas: *Reducing false positives in intrusion detection systems*. Computers & Security, Vol. 29, Issue 1, 2010, pp. 35-44.

H.H.W.J. Bosman: *Anomaly detection in networked embedded sensor systems*. University of Technology, Eindhoven, 2016

Z. Yu, J. Tsai: *Fuzzy Model Tuning for Intrusion Detection Systems*. International Conference on Autonomic and Trusted Computing (ATC), 2006, pp. 193-204.

S. Senturk, N. Erginel, I. Kaya and C. Kahraman: *Fuzzy exponentially weighted moving average control chart for univariate data with a real case application*. Applied Soft Computing, Vol. 22, 2014, pp. 1-10.

N. Paul and D. Evans, *Comparing Java and .NET Security: Lessons Learned and Missed*, 2015

A. Lane, *Understanding and Selecting RASP: Technology Overview*, 2016

V. Tiwari, *SDN and OpenFlow for beginners with hands on labs*, M.M. D.D. Multimedia LLC., Kindle Edition, Northville, 2013

W. Stallings, *Software-Defined Networks and OpenFlow*. The Internet Protocol Journal. Vol. 16, No. 1, 2013

A. Singh: *Performance Analysis of Spread Spectrum Techniques*, in *Conference on Advances in Communication and Control Systems (CAC2S 2013)*, 2013.

F. Chen: *Application of MATLAB in Teaching of High Frequency Circuits*, in *Advanced Technology in Teaching - Proceedings of the 2009 3rd International Conference on Teaching and Computational Science (WTCS 2009)*, Vol. 116, Y. Wu, Ed., Berlin, Heidelberg, SpringerLink, 2009, pp. 243-250.

R. L. Pickholtz, D. L. Schilling and L. B. Milstein: *Theory of Spread-Spectrum Communications-A Tutorial*, IEEE Transactions on Communications, Vol. 30, No. 5, pp. 855-884, 1982.

J. J. Baeza-Baeza, F. F. Pérez-Pla and M. C. García-Álvarez-Coque: *Teaching Chemical Equilibria Using Open Source Software OCTAVE*, World Journal of Chemical Education, Vol. 3, No. 3, 2015, pp. 127-133.

J. S. Hunter, *The Exponentially Weighted Moving Average*, Journal of Quality Technology 18: 203-210, 1986

J. M. Lucas, M. S. Saccucci, *Exponentially Weighted Moving Average Control Schemes: Properties and Enhancements*, Technometrics 32, 1-29, 1990

Ye et al., *Computer Intrusion Detection through EWMA for Autocorrelated and Uncorrelated Data*, IEEE Transactions on Reliability, Vol. 52, No. 1, 2003

J. M. Westall: *An Introduction to Direct-Sequence Spread-Spectrum,* Aplication Note 1890, 2003, https://people.cs.clemson.edu/~westall/851/spread-spectrum.pdf.

A. Lazarevic, V. Kumar, J. Srivastava: *Managing Cyber Threats: Issues, Approaches and Challenges, Chapter: A survey of Intrusion Detection techniques,* Kluwer Academic Publishers, Boston, 2005

V. Siris, F. Papagalou: *Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks*. IEEE Global Telecommunications Conference, *2004. GLOBECOM '04.*, 2004, pp. 2050-2054 Vol.4, https://doi: 10.1109/GLOCOM.2004.1378372

J. J. Weinman, E. Learned-Miller, A. R. Hanson: *Scene Text Recognition Using Similarity and a Lexicon with Sparse Belief Propagation*. IEEE Transactions on Pattern Analysis and Machine Intelligence. 31(10), pp.1733-1746, 2009, doi:10.1109/TPAMI.2009.

M. Yokobayashi, T. Wakahara: *Binarization and Recognition of Degraded Characters Using a Maximum Separability Axis in Color Space and GAT Correlation*. in Proc. of 18th Int. Conf. on Pattern Recognition (ICPR2006) Vol. 2, 2006, pp. 885-888, doi:10.1109/ICPR.2006.326

B. P. Gerkey, S. Thrun: *Parallel Stochastic Hill-climbing with Small Teams*. in L. E. Parker et al. (eds.) Multi-Robot Systems: From Swarms to Intelligent Automata. Volume III, Springer, 2005, 65-77

T. Le, R. Garcia, P. Casari, P-O. Östberg: *Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey,* ACM Computing Surveys, Vol. 52. No. 5., 2019, pp.1-39. https://doi.org/10.1145/3341145

A. Kizrak: *Comparison of Activation Functions for Deep Neural Networks*, Towards Data Science, 2019, https://towardsdatascience.com/comparison-of-activation-functions-for-deep-neural-networks-706ac4284c8a

L. Hauzenberger, E. Holmberg Ohlsson: *Drone detection using audio analysis*, M.S. thesis, Department of Electrical and Information Technology, Lund University, Sweden, June 2015.

S. Rafiul Hussain, M. Echeverria, O. Chowdhury, N. Li, E. Bertino: *Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information*, Network and Distributed System Security (NDSS) Symposium, San Diego, 2019.

D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler: *A Formal Analysis of 5G Authentication*, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), 2018

N. Rodday: *Hacking a Professional Drone*, Black Hat, Asia 2016, https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf

A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.–P. Seifert: *Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems*, Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS), 2016

Ju, Gin-Fon N., Bork, A., *The Implementation of an Adaptive Test on the Computer*, 5th IEEE International Conference on Advanced Learning Technologies (ICALT'05), Kaohsiung, Taiwan, 2005, pp.822-823, http://doi.ieeecomputersociety.org/10.1109/ICALT.2005.274

M. Takacs, A. Szakál, A., G. Csikós Pajor: *Software Supported Mathematics Teaching*, Proceedings of the 3rd International Conference on Information Technology Based Higher Education and Training, ITHET Conference, July 4-6, 2002, Budapest, Hungary

R. D. Carlson: *Computer-adaptive testing: a shift in the evaluation paradigm*. Journal of Educational Technology Systems, 22(3), 1994, pp. 213-224.

T. Eggen: *Choices in CAT models in the context of educational testing*. In D. J. Weiss (Ed.), Proceedings of the 2007 GMAC Conference on Computerized Adaptive Testing, 2017, pp.1-19, 2007

J. Jacobsen, R. Ackermann, J. Egüez, D. Ganguli, P. Rickard, & L. Taylor : *Design of a computer-adaptive test to measure English literacy and numeracy in the Singapore workforce*: *Considerations, benefits, and implications*. Association of Test Publishers, 12(1), 2011, pp.1-26

W. Kruse, J.G. Heiser: *Computer Forensics: Incident Response Essentials*, Addison-Wesley, 2002

M. Reith, C. Carr, G. Gunsch: *An Examination of Digital Forensic Models*, International Journal of Digital Evidence, Volume 1, Issue 3, 2002

C. Cruz–Neira, M. Fernandez, C. Portales: *Virtual Reality and Games, Multimodal Technologies and Interaction*, 2018

A. Sutcliffe, B. Gault: *Heuristic evaluation of virtual reality applications*, Interacting with Computers 16, 2004, Elsevier, pp. 831–849.

T. Pant, S. Neelakantam: *Learning Web–based Virtual Reality: Build and Deploy Web–based Virtual Reality Technology*, Apress, 2017

V. A tézispontokhoz kapcsolódó tudományos közlemények

1. P. Čisar, S. Maravić Čisar, *A first derivate based algorithm for anomaly detection*, International journal of computers, communications & control, ISSN 1841-9836, E-ISSN 1841-9844, Volume III (2008), Supplementary Issue – Proceedings of ICCCC 2008, pp. 238-242, Oradea, Romania

2. P. Čisar, S. Bošnjak, S. Maravić Čisar, *EWMA algorithm in network practice*, International journal of computers, communications & control, ISSN 1841-9836, E-ISSN 1841-9844, Volume V (2010), No. 2, pp. 156-167.

3. P. Čisar, S. Maravić Čisar, *Skewness and Kurtosis in Function of Selection of Network Traffic Distribution*, Acta Polytechnica Hungarica, Vol.7, No.2, 2010, ISSN 1785-8860, pp. 95-106.

4. P. Čisar, S. Maravić Čisar, *The Framework of Runtime Application Self-Protection Technology*, 17th IEEE International Symposium on Computational Intelligence and Informatics, CINTI 2016, 17–19 November, 2016, Budapest, Hungary – Proceedings, pp. 81-85.

5. P. Čisar, S. Maravić Čisar, *Network Statistics in Function of Statistical Intrusion Detection*, Computational Intelligence and Informatics, Vol. 313, 1st Edition, 2010, ISBN 978-3-642-15219-1, e-ISBN 978-3-642-15220-7, ISSN 1860-949X, DOI 10.1007/978-3-642-15220-7, 2010 Springer-Verlag Berlin Heidelberg, pp. 27-36

6. P. Čisar, P. Odry, S. Maravić Čisar, G. Stankov, *Teaching Spread Spectrum in the Course Telecommunication Systems Using Octave*, Computer Applications in Engineering Education, Wiley Periodicals, Inc., 2020, pp. 1-17.

7. P. Čisar, D. Erlenvajn, S. Maravić Čisar, *Implementation of Software-Defined Networks Using Open-Source Environment*, Technical Gazette, Vol. 25, Suppl. 1, 2018, pp. 222-230.

8. P. Čisar, S. Maravić Čisar, *Security Aspects of 5G Mobile Networks*, Annals of Faculty Engineering Hunedoara – International Journal of Engineering, Tome XVII-Fascicule 4, ISSN 1584–2665, pp. 137-143, 2019.

9. P. Čisar, R. Pinter, S. Maravić Čisar, M. Gligorijević: *Principles of Anti-Drone Defense*, 11th IEEE International Conference on Cognitive Infocommunications (electronic conference), 2020, ISBN 978-1-7281-8213-1, pp. 19-26.

10. P. Čisar, S. Maravić Čisar, *Improvement of Exponential Smoothing Using Simulated Network Environment*, Acta Technica Corviniensis – Bulletin of Engineering, Tome VI (2013), Fascicule 4, ISSN: 2067-3809, pp. 119-122

11. S. Maravic Cisar, P. Cisar, R. Pinter, *Evaluation of Knowledge in Object Oriented Programming Course with Computer Adaptive Tests*, Computers & Education, Volume 92-93, 2016, Elsevier, pp. 142-160.

12. V. Borović, P. Spalević, P. Čisar, D. Rančić, S. Jović, *Supervisory System for Physical Objects Spatial Location Detection*, Physica A: Statistical Mechanics and its Applications, 2019, Elsevier, pp. 781-795.

13. S. Maravić Čisar, D. Radosav, B. Markoski, R. Pinter, P. Čisar, *Computer Adaptive Testing of Student Knowledge*, Acta Polytechnica Hungarica, Vol.7, No.4, 2010, ISSN 1785-8860, pp. 139-152.

14. P. Čisar, S. Maravić Čisar, B. Markoski, *Implementation of Immunological Algorithms in Solving Optimization Problems*, Acta Polytechnica Hungarica, Vol. 11, No. 4, 2014, pp. 225-240.

15. P. Čisar, S. Maravić Čisar, D. Subošić, P. Đikanović, S. Đukanović, *Optimization Algorithms in Function of Binary Character Recognition*, Acta Polytechnica Hungarica, Vol. 12, No. 7, 2015, pp. 77-87.

16. P. Čisar, S. Maravić Čisar, *General Directions of Development in Digital Forensics*, Acta Technica Corviniensis, ISSN 2067-3809, Vol. 5, No. 2, 2012, pp. 87-91

17. P. Čisar, S. Maravić Čisar, *Development Concepts of Virtual Reality Software*, Acta Technica Corviniensis – Bulletin of Engineering, e-ISSN 2067–3809, Tome XIII-Fascicule 3, pp. 23-29, 2020.

18. P. Čisar, S. Maravić Čisar, *Optimization methods of EWMA Statistics*, Acta Polytechnica Hungarica, Vol. 8, No. 5, 2011, pp. 73-87.

19. P. Čisar, S. Maravić Čisar, B. Popović, K. Kuk, I. Vuković, *Application of Artificial Immune Networks in Continuous Function Optimization*, Acta Polytechnica Hungarica, Vol. 19, No. 7, 2022, pp. 153-164.

20. P. Čisar, B. Popović, K. Kuk, S. Maravić Čisar, I. Vuković (2022). *Machine Learning Aspects of Internet Firewall Data*. In: Kovács, T.A., Nyikes, Z., Fürstner, I. (eds) Security-Related Advanced Technologies in Critical Infrastructure Protection. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-2174-3_4

21. P. Čisar, S. Maravić Čisar, *Artificial intelligence and data mining in function of computer infrastructure security*, 10th Alma Mater Europaea Conference, It's About People 2022: Embracing Digital Transformation for a Sustainable and Ethical Future, Maribor, Slovenia, 2022.

22. P. Čisar, S. Maravić Čisar, *EWMA Statistics and Fuzzy Logic in Function of Network Anomaly Detection*, Facta Universitatis, Series: Electronics and Energetics, University of Nis, Vol. 32, No. 2, 2019., pp. 249-265.

VI. További tudományos közlemények

23. Újvidéki Egyetem, Szabadkai Közgazdasági Kar, „Biztonsági szempontok megvalósítása mobilbanki alkalmazásokban”, 2008. - magiszteri dolgozat

24. Újvidéki Egyetem, Szabadkai Közgazdasági Kar, „Módszerek az internetes forgalmi hibák észlelésére az elektronikus üzletben”, 2010. - doktori értekezés