
HTE diplomaterv és szakdolgozat pályázat

ALMANACH

2023



Tartalom

Huszty Csaba

HTE diplomaterv és szakdolgozat pályázat, 2023 – Előszó

1

Bencsik Blanka

Efficient Neural Network Pruning Using Model-Based Reinforcement Learning/Mély neurális hálózatok hatékony ritkítása megerősítéses tanulás alkalmazásával

2

Császár Zsófia

DATA MINING IN HEALTHCARE - Clinical decision support based on blood test data of heart transplant patients

3

Békési Gergő Bendegúz

Mérésautomatizálás mesterséges intelligencia segítségével

4

Barva Tamás

IoT alapú árammérő szenzor fejlesztése ipari villamos gépekhez

5

Tibor Attila Gábor

Szteganográfiai szoftver fejlesztése

6

Saska Szilvia

Adaptív fuzzing módszertana autóiipari környezetben

7

Hírközlési és Informatikai Tudományos Egyesület

www.hte.hu

Elnök: Vágújhelyi Ferenc

H-1051 Budapest, Bajcsy-Zsilinszky út 12., 5. em./502.

Tel.: 353-1027 • e-mail: info@hte.hu

HTE diplomaterv és szakdolgozat pályázat, 2023

A Hírközlési és Informatikai Tudományos Egyesület a korábbi évek hagyományai szerint 2023-ban ismét meghirdette a Diplomaterv és Szakdolgozat Pályázatot, amelyre mesterszakos (MSc), alapszakos (BSc) és üzemmérnök alapszakos (BProf) kategóriákban vártuk a pályaműveket.

Ugyancsak kiírásra került ismét az angol nyelvű dolgozatokkal pályázó végzős hallgatók elismerésére az IEEE Communications Society-vel és a Hungarian Joint ComSoc/MTT/AP/ED/EMC Chapter-rel közösen a „HTE – IEEE ComSoc Thesis Award” különdíj is.

A pályázatra 15 pályamű érkezett, ebből 7 az MSc, 6 a BSc, és 2 a BProf kategóriában. A pályázók között 2 felsőoktatási intézmény hallgatói képviseltették magukat, a Budapesti Műszaki és Gazdaságtudományi Egyetem és a Dunaújvárosi Egyetem hallgatói.

A pályázatra beérkezett dolgozatokat a témaválasztás korszerűsége, a kapcsolódó szakirodalom feldolgozása, a saját munka mennyisége, saját munka és színvonala, az elért eredmények, a szerkesztés, és a formai elemek alapján értékelték. A felsorolt szempontok szerint végzett bírálói értékeléseket összesítve a következő eredmény született az egyes kategóriákban:

Bprof kategória díjazottjai:

1. helyezett: Saska Szilvia: Adaptív fuzzing módszertana autópári környezetben (BME, HIT)

Konzulens: Schulcz Róbert, Babud Imre

Dicséretben részesült:

Szabó Kristóf: Mobil banki alkalmazás modern automatizált tesztelési megoldása (BME, TMIT)

Konzulens: Kérdő Attila, Moldován István

BSc kategória díjazottjai:

1. helyezett: Volentér Krisztián Adrián: Detection of network attacks using ensemble learning methods (BME, HIT)

Konzulens: Dr. Mészáros András Gergely

2. helyezett: Barva Tamás: IoT alapú árammérő szenzor fejlesztése ipari villamos gépekhez (BME, TMIT)

Konzulens: Dr. Fehér Gábor

3. helyezett: Tibor Attila Gábor: Szteganográfiai szoftver fejlesztése (Dunaújvárosi Egyetem, Informatika Intézet, Szoftverfejlesztési és Alkalmazási Tanszék)

Konzulens: Dr. Katona József

Dicséretben részesült:

Árvai Zsombor: Egyedi okosöntöző tervezése és fejlesztése (BME, HIT)

Konzulens: Schulcz Róbert

Lőrincz Áron: Millimeter wave 5G hálózatok optimalizálása (BME, TMIT)

Konzulens: Dr. Cinkler Tibor

Váczai Ottó: Dinamikus csatornaváltás modellezése MCO működés vizsgálatához Artery/OMNeT++ keretrendszerben (BME, HIT) Konzulens: Dr. Bokor László

MSc kategória díjazottjai:

1. helyezett: Bencsik Blanka: Efficient Neural Network Pruning Using Model-Based Reinforcement Learning (BME, AUT)

Konzulens: Dr. Szemenyei Márton

2. helyezett: Császár Zsófia: DATA MINING IN HEALTHCARE - Clinical decision support based on blood test data of heart transplant patients (BME, TMIT)

Konzulens: Dr. Alija Pašić, Revisnyei Péter

3. helyezett: Békési Gergő Bendegúz: Mérésautomatizálás mesterséges intelligencia segítségével (BME, AUT)

Konzulens: Dr. Ekler Péter, Urbin Ágnes, Szőke Szilárd

Dicséretben részesült:

Czurkó Szabolcs Dániel: Kooperatív robot navigáció (BME, TMIT)

Konzulens: Dr. Fehér Gábor

Kovács-Hegedűs András Márton: Jelenlét alapú zenelejátszás okosotthon környezetben (BME, HIT)

Konzulens: dr. Szabó Sándor

Márton Botond László: Utófeldolgozási eljárások implementálása kvantum alapú kulcsszétosztó rendszerben (BME, HIT)

Konzulens: dr. Bacszárdi László, dr. Kis Zsolt

Nagy Bence Damján: Kockázatbecslés támogatása automatizált módszerekkel IT/OT rendszerekben (BME, HIT)

Konzulens: Dr. Holczér Tamás

A HTE – IEEE ComSoc Thesis Award különdíjban **Bencsik Blanka** „Efficient Neural Network Pruning Using Model-Based Reinforcement Learning” című dolgozata részesült.

Jelen kiadványunk a 2023-as Diplomaterv és szakdolgozat pályázat díjazott pályaműveiből készült 1 oldalas kivonatait tartalmazza.

Minden díjazottnak szívből gratulálunk, és sok sikert kívánunk további pályafutásukhoz!

A pályázatról további információk a <https://www.hte.hu/hte-diplomatervszakdolgozat-palyazat> weboldalon érhetők el.

Dr. Huszty Csaba
Tudományos területért
felelős elnökségi tag



Efficient Neural Network Pruning Using Model-Based Reinforcement Learning/Mély neurális hálózatok hatékony ritkítása megerősítéses tanulás alkalmazásával

Bencsik Blanka

Budapesti Műszaki és Gazdaságtudományi Egyetem
bencsik.blanka@gmail.com

Konzulens: Dr. Szemenyei Márton

Kulcsszavak: neurális hálózatok, objektumdetektálás, megerősítéses tanítás, neurális háló ritkítás

A mély neurális hálók az elmúlt tíz évben kimagasló eredményt mutattak az objektumdetektálás területén, alkalmazásuknak azonban gátat szab a nagy számításigényük és méretük, mely a hatalmas paraméterszámukkal magyarázható. Különösen jelentős ez a probléma az erőforráskorlátos eszközök esetén, ahol még a betanított modellek tárolása és futtatása is nehézséget okozhat. A probléma megoldására használatos a neurális háló ritkítás, melynek célja egy neurális háló modell paramétereinek lehető legnagyobb mértékű redukálása a pontosság romlásának elkerülése mellett. A keretes részben legyen megadva a szerző emailcíme, illetve a kulcsszavaknál legyen 4-5, a témához illő kulcsszó felsorolva

A probléma megközelíthető megerősítéses tanulás alkalmazásával, melynek során az ágens emberi beavatkozás nélkül igyekszik megtalálni az optimális eltávolítandó paraméterszámot a modell minden rétegéhez. A probléma ezen megközelítése jelenleg is nyitott téma az irodalomban, ám a létező megoldások legnagyobb hátulütője, hogy az ágens számára a két legfontosabb környezeti változót - a ritkaságot és a pontosságromlást - a modell tényleges ritkításával és validálásával határozzák meg futási időben, ami nagymértékben lelassítja a tanítási folyamatot.

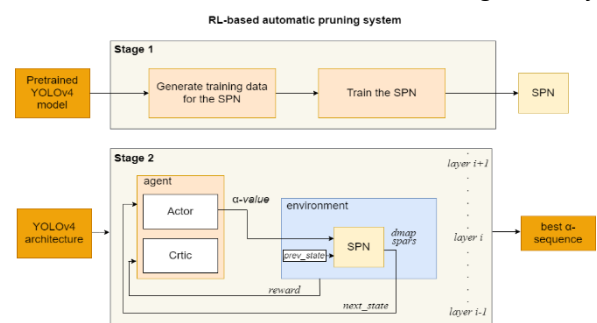
Munkám során egy olyan megerősítéses tanulás alapú rendszert valósítottam meg, mely a YOLOv4 objektumdetektor optimális ritkítását teszi lehetővé a tanítási folyamat idejének csökkentése mellett. Az eddig létező megoldásokhoz képest a rendszert egy olyan neurális hálóval egészíttem ki, mely a ritkítandó háló pontosságváltozását és ritkaságát képes megbecsülni az addig törölt paraméterek mennyiségének és az adott réteghez választott redukáló tényező függvényében. Ezen állapotbecslő háló a környezet állapotának meghatározásához szükséges hosszadalmas műveletek szerepét veszi át, nagyságrendekkel növelve így a tanítás sebességét. Az állapotbecslő hálót önfelügyelt tanítás segítségével lett betanítva, automatikusan generált adatokon.

Az elkészült ritkító rendszer a ritkított YOLOv4 modell teljesítménye és az eredmény eléréséhez szükséges teljes fejlesztési idő alapján került értékelésre. A ritkított modell kimagasló eredményeket produkált; paraméterei 61 %-ának eltávolítása mindössze 6,4 %-os mAP romlást eredményezett. Ezen eredmény felülmúlja a kutatásban vizsgált legjobb kézzel készített ritkító módszert 9 %-kal nagyobb ritkasággal és 3,9 %-kal kisebb pontosságromlással. A teljes fejlesztési időt tekintve az elkészült módszer felülmúlja mind az AMC, mind a PuRL state-of-the-art megerősítéses tanulás-alapú ritkító módszerek becsült teljes fejlesztési idejét. A javasolt ritkító rendszer a

vizsgált problémán 16,72-szer gyorsabbnak bizonyul, mint a PuRL és 12,14-szer gyorsabb, mint az AMC.

A korábbiakban bemutatott neurális háló ritkító rendszer megerősítéses tanulással való ilyen módú megközelítésére a legjobb tudomásom szerint nincs példa az irodalomban. A rendszer fő előnyei között említendő, hogy a megerősítéses tanulási ágens használata nem korlátozza a ritkító stratégiát egy bizonyos szabályra, lényegesen növelve ezzel az optimális megoldás megtalálásának valószínűségét. Az eredményül kapott detektor kisebb méretének következtében alkalmazhatóvá válik beágyazott rendszerekben, mobiltelefonokban és más erőforráskorlátos berendezésekben. Mindemellett, a rendszer felhasználásával a megerősítéses tanulás alapú automatikus ritkítás területén történő fejlesztések elérhetővé válnának olyan kutatók számára is, akik nem rendelkeznek drága, nagyteljesítményű grafikus processzorokkal, hiszen annak egyik része sem igényelne nagy GPU memóriát.

A dolgozat ezen kívül magában foglalja a jövőbeli tervek kezdetleges megvalósítását; az első, kulcsfontosságú fejlesztési lépéseket a ritkító rendszer adatbázisok és neurális háló architektúrák közti általánosíthatóság céljából.



1.ábra: A bemutatott megerősítéses tanulás-alapú neurális háló ritkító rendszer folyamatábrája

A szerzőről



Bencsik Blanka tanulmányait 2017-ben kezdte meg a BME Villamosmérnöki és Informatikai Karának villamosmérnöki képzésén. A BSc diploma megszerzése után a villamosmérnök mesterképzést is elvégezte, MSc diplomáját 2023 nyarán vette át. Az alapképzés utolsó éveiben foglalkozni kezdett a neurális hálózatok kutatásával. Kutatásainak eredményességét a TDK-án szerzett kimagasló helyezések és az OTDK-án elnyert első helyezés is alátámasztják. Jelenleg a BME Informatikai Tudományok Doktori Iskola PhD hallgatója, emellett Machine Learning mérnök pozícióban praktizál az ipari szektorban.

Clinical decision support based on blood test data of heart transplant patients / Klinikai döntés-támogatás szívtranszplantált betegek vérgáz adatai alapján

Császár Zsófia

BME, VIK, Távközlési és Médiainformatikai Tanszék
zsofiacsaszar0@gmail.com

Konzulensek: Dr. Pašić Alija, Revisnyei Péter (BME, VIK, Távközlési és Médiainformatikai Tanszék)

Kulcsszavak: adatbányászat, neurális háló, idősor, vérgáz, szívtranszplantáció

A modern technológiának köszönhetően, manapság már az egészségügyben is lehetséges hatalmas mennyiségű adatot generálni és gyűjteni. Mivel a gépi tanulási módszerek hatékonyan bizonyultak a komplex adatokban rejlő minták és kapcsolatok felismerésében, fontos szerepet játszhatnak a klinikai döntés-támogatásban is.

A szívtranszplantációs műtét utáni túlélés esélyeit számos tényező befolyásolhatja, így fontos lehet a betegek különböző adatai alapján az állapotukra vonatkozó előrejelzéseket tenni. A projekthez rendelkezésre álló orvosi adatszett a betegek különböző időpontokban vett artériás vérgáz paramétereinek méréseit tartalmazta, mind a szívtranszplantáció előtt és után. Munkám célja a vérgáz paraméterek közötti lineáris és nem lineáris kapcsolatok vizsgálata, valamint a mérési értékek előrejelzése a páciensek korábbi időpontokban vett saját, vagy más páciensek mérési adatai alapján.

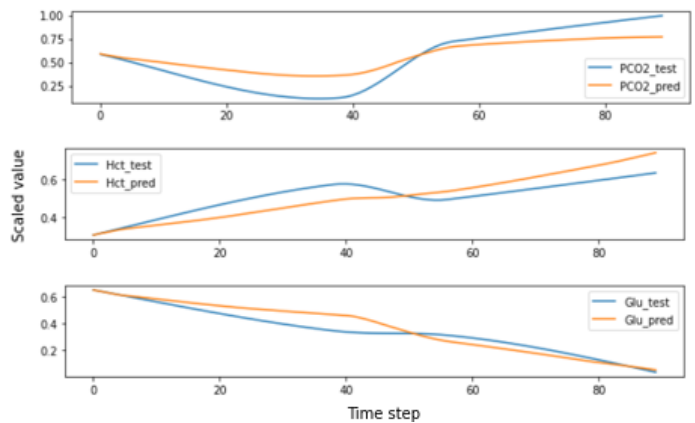
Dolgozatomban a paraméterek idősorain tisztítást és aggregálást végeztem, majd a rendelkezésre álló túlélési adatokat is felhasználva adatbányászati technikákkal elemeztem az adatszettet. Vizsgáltam a mérési értékek különbségeit a túlélő és elhunyt betegek között, a referenciaintervallumon kívül eső értékeket mutató betegek százalékos arányát különböző időpontokban, a vérgáz paraméterek korrelációját, valamint a betegek közötti klaszter tendenciákat.

Az eredmények alapján a legtöbb paraméter változásában szignifikáns különbség figyelhető meg a túlélő és elhunyt páciensek csoportjai között, a vizsgált időszakban. Továbbá, szinte minden paraméter változásában szignifikáns különbség mutatkozik a különböző posztoperatív túlélési idővel rendelkező páciensek között is. Ezen különbségek arra engednek következtetni, hogy a vérgáz mérések idősoros adatai alkalmasak lehetnek a posztoperatív túlélési hossz előrejelzésére is. Kimutatható szignifikáns korreláció több paraméter között, illetve a nem lineáris kapcsolatokról is látszik, hogy minden paraméter esetében van néhány erős prediktor a többi között.

A modellezési folyamat elején automatizált gépi tanulással kerültek kiválasztásra a regressziós modellek. Lineáris regresszió, döntési fa alapú, idősoros és neurális háló alapú modelleket is használtam. A legjobb teljesítményűre értékelt modelleken további fejlesztést, hiperparaméter-optimalizálást és feature importance vizsgálatot végeztem. A számolt átlagos hiba értékek alapján a modellek értékelésre

kerültek a referenciaintervallumok függvényében is. Azért volt fontos ilyen szempontból is értékelni a modelleket, mert a tévesen normálisnak jóslt értékek kritikusabb hibának számíthatnak, mint a tévesen abnormális előrejelzések.

Az alábbi ábrán a valós (kék) és a jóslt (sárga) értékek



összehasonlítása látható három paraméter esetében.

Az értékelések alapján a vérgázparaméterek a legjobban többváltozós többretegű perceptron modellekkel jelezhetők előre egymásból, 0.0015-0.0025 közötti átlagos RMSE és 1% alatti átlagos MAPE mellett.

A paraméterek időben nagyobb távra is előre jelezhetők hasonlóan alacsony átlagos hibákkal. Teljesen ismeretlen betegek esetében, más betegek adatai alapján ugyan kisebb pontossággal, viszont anélkül lehet előrejelzéseket tenni, hogy a jóslt értékek tévesen esnének a normál referencia-intervallumba. A létrehozott előre jelző modellek csökkenthetik az ABG-vizsgálatok gyakoriságát, ezáltal a költségeket is. Az orvosok tájékozódhatnak a várható tendenciákról, valamint észlelhetnék az esetlegesen bekövetkező életveszélyes állapotokat is.

A szerzőről



Császár Zsófia tanulmányait a Budapesti Corvinus Egyetem gazdaságinformatikus alapképzésén kezdte meg, majd a Budapesti Műszaki és Gazdaságtudományi Egyetem gazdaságinformatikus mesterképzésén folytatta. Egyetemi évei alatt több munkahelyen is megfordult, foglalkozott szoftverfejlesztéssel és webanalitikával is. Jelenleg Üzleti Intelligencia elemzőként

dolgozik a Hearsay Systems-nél.

Mérésautomatizálás mesterséges intelligencia segítségével

BÉKÉSI GERGŐ BENDEGÚZ

BME, VIK, Automatizálási és Alkalmazott Informatikai Tanszék
bekesi.gergo@aut.bme.hu

Konzulensek: Dr. Ekler Péter (BME, VIK, AUT), Urbán Ágnes (BME, GPK, MOGI), Szőke Szilárd Zsigmond (Robert Bosch Kft.)

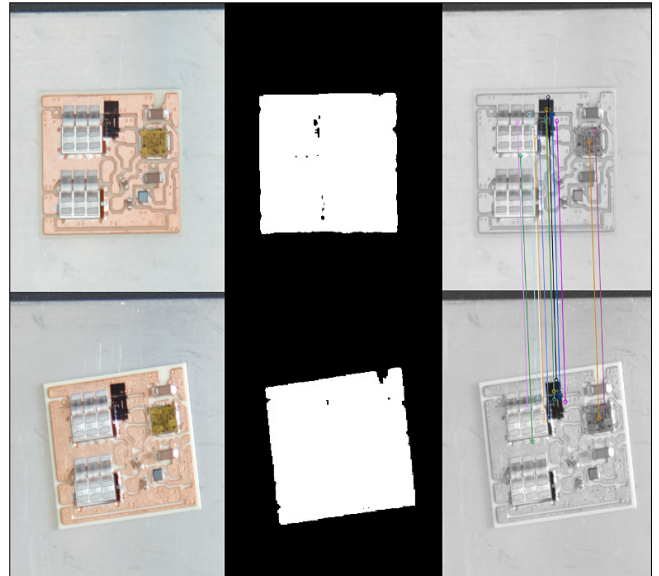
Kulcsszavak: mesterséges intelligencia, mérésautomatizálás, látórendszer, mélytanulás, képfeldolgozás

Napjainkban a növekvő elektrifikáció, az okoseszközök elterjedése, a villamosenergia-fogyasztási igények növekedése, az elektronika és autóelektronika terén végbemenő bővülés, valamint a villamos autók egyre népszerűbbé válása miatt különös hangsúly helyeződik az elektronikai iparra, azon belül is a teljesítménytranszistorok iparágára. Ezen elektronikai eszközöknek a nagyobb leadott villamos teljesítményéhez az egyre kisebb felületükön, egyre nagyobb hőteljesítményt kell leadniuk, ami komoly műszaki kihívást eredményez, hiszen épp a túl magas hőmérséklet a vezető meghibásodási ok esetükben. Így kiemelten fontos a termikus vizsgálatuk, melyet termikus tranziens méréssel, azaz T3Ster méréssel lehet elvégezni.

Ezen mérési folyamat automatizálásában, gyorsításában, gazdaságosabbá tételében vettem részt a Robert Bosch Kft. ThID csapatában, amely termikusmodell-identifikációval foglalkozik. Egy LabVIEW-környezetben vezérelt robothoz fejlesztettem olyan komplex elektronikai eszközt, illetve látórendszert, amely segíteni tudja az automatikusan mérni kívánó robotot a mérendő MOSFET-ek és más elektronikai komponensek megtalálásában, a hozzájuk való navigációban. A látórendszer hardver-és szoftverfejlesztését is én végeztem. Megfelelő szenzorral rendelkező kamerát és hozzá alkalmas optikát választottam. Ezekhez egy egyszerre akár több vezérlő számítógép kiszolgálására is képes szerverplatformot valószínűsítem meg egy Raspberry Pi 4 Model B segítségével. Autodesk Inventor Professional 2022 szoftverben megterveztem a mechanikai integrációt segítő konstrukciót, majd 3D-nyomatóval kinyomtattam.

Munkám leghangsúlyosabb részében mesterséges intelligencia, teljesen konvolúciós neurális hálók, valamint számítógépes látás algoritmusainak segítségével szemantikus szegmentációt és kulcspontkeresést végeztem a robot navigálásához. A teljesen konvolúciós neurális hálókat saját kóddal implementáltam, a tanításhoz szükséges adathalmazt az éles mérés esetében is használt kamerával és optikával készítettem el, és kézzel annotáltam.

A neurális hálókat komplex vizsgálat alá vettem. Automatizált futtatások segítségével 21380 alkalommal tanítottam be és értékeltem ki hálókat, módosítva a mélységet, a csatornaszámokat, a felbontást, és a batch méretet. Ezeket a nyílt forráskódú Python 3 programozási nyelven elsősorban az OpenCV, Pytorch és Torchvision



könyvtárak segítségével végeztem. A mérendő komponensekhez való navigálást robusztusan megvalósító, 100 μm és 1° pontosságú elektronikai rendszert készítettem, amelyhez 94% pontosságú IoU érték társult a szemantikus szegmentáció esetében, amelyet valós, eredeti mérési környezetben teszteltem.

Szakirodalmi vizsgálatom során nem találtam olyan megoldást, amely ilyen pontossággal használt volna szemantikus szegmentációt és helymeghatározást elektronikai komponensekre, így munkám felhasználható további tudományos és ipari újításokhoz, projektekhez. Ezen felül újszerű megoldásnak számít a teljesen konvolúciós neurális hálók és a SIFT-algoritmus együttes használata, amelyekkel ezeket az eredményeket elértem. Ezen megoldásomnak kiterjeszhetőségét is igazoltam azzal, hogy hiperparaméter optimalizációs algoritmus alkalmazásával továbbfejlesztettem és implementáltam közvetlen kötésű réz kerámiahordozók esetén is.

A szerzőről



BÉKÉSI GERGŐ BENDEGÚZ BSc- és MSc-tanulmányait a Budapesti Műszaki és Gazdaságtudományi Egyetemen végezte energetikai mérnöki és villamos-mérnöki szakon. Jelenleg az intézmény Informatikai Tudományok Doktori Iskolájának PhD hallgatója, valamint az i-Cell Mobilsoft Zrt. deep learning mérnöke.

IoT-alapú árammérő szenzor fejlesztése ipari villamos gépekhez

BARVA TAMÁS

BME, VIK, Távközlési és Médiainformatikai Tanszék
barva7tamas@gmail.com

Konzulens: Dr. Fehér Gábor (BME, Távközlési és Médiainformatikai Tanszék)

Kulcsszavak: IIoT, árammérő szenzor, MQTT, Ipar 4.0

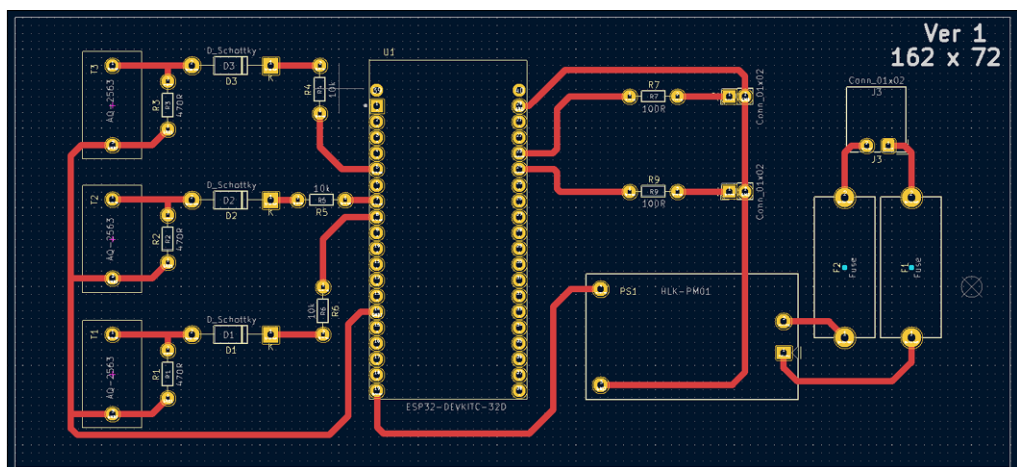
Az emelkedő villamosenergia-árak mellett az iparban is fontossá vált a gépek villamosenergia-fogyasztásának monitorozása. Erre nyújtanak megoldást az „okos” fogyasztásmérő készülékek, amelyek valós időben képesek a fázisáramok, teljesítmény, energiafogyasztás mérésére és az eredmények továbbítására. A gyűjtött adatok alapján a vállalat optimalizálhatja az energiafogyasztását, meg tudja állapítani a gépek kihasználtságát, illetve állapotát. Ezen információk által a cég döntéseket tud hozni abban a kérdésben, hogy a gyártásban az adott feladatot melyik berendezéssel végezze el, ütemezni tudja a berendezések karbantartását. Hiba esetén pedig segítséget nyújthat a probléma forrásának megtalálásában.

A dolgozatomban bemutatom a két legnépszerűbb árammérő szenzor működését, felépítését, elemzem őket erősségeik és gyengeségeik alapján, kiválasztom a feladathoz legjobban illeszkedő megoldást. Továbbá bemutatom még a piacon elérhető két vezeték nélküli IoT-árammérő szenzort.

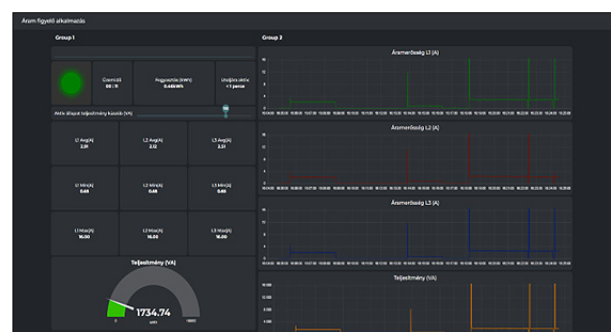
Ezt követően az iparban elérhető vezeték nélküli IoT-technológiákat elemzem tulajdonságaik alapján, majd kiválasztok két technológiát, melyek legjobban illeszkednek az adott feladathoz és részletesen bemutatom ezeket. Ezután az alkalmazásokat kiszolgáló platformokra térek ki, ezek közül kettőt részletesen bemutatok és összehasonlítom őket.

Szakedolgozatomban bemutatom az általam készített vezeték nélküli árammérő szenzor és IoT-szolgáltatás tervezésének folyamatát, melynek során az ipari elvárásokat is szem előtt kellett tartanom. Részletesen bemutatom a kapcsolási rajzom és nyomtatott áramköri tervem elkészítésének folyamatát, az IoT-szolgáltatás topológiáját. Részletezem a tervezés során felmerülő problémákat és az ezekre nyújtott megoldásokat, valamint a vezeték nélküli árammérő szenzor során használt mikrokontroller és IoT-platform programozását és konfigurálását.

Legvégül gyakorlati vizsgálati példák alapján ellenőrzöm az általam épített árammérő szenzor és IoT-szolgáltatás helyes működését. Erre egy-egy régebbi típusú fűró és forgácsoló gépet használtam, amelyekben az



aszinkron motorok voltak a legnagyobb fogyasztók. Mivel ezeket a motorokat nem látták el semmilyen lágy indítással, ezért tesztelés során jól látható a rájuk jellemző nagy indulási áram.



A szerzőről



BARVA TAMÁS tanulmányait a Budapesti Műszaki és Gazdaságtudományi Egyetemen végezte, villamosmérnöki alapszakon, majd az Óbudai Egyetemen folytatta PLC-szakmérnök-képzésen. Jelenleg a Weldmatic Kft.-nél dolgozik tervezőmérőként a hegesztés-automatizálás területén.

Szteganográfiai szoftver fejlesztése

TIBOR ATTILA GÁBOR

Dunaújvárosi Egyetem, Informatikai Intézet
tattigbr@gmail.com

Konzulensek: Dr. Katona József (Dunaújvárosi Egyetem, Informatikai Intézet),
Szarka Péter (CodeCool Kft)

Kulcsszavak: szteganográfia, kriptográfia, kódolás, C#, WPF

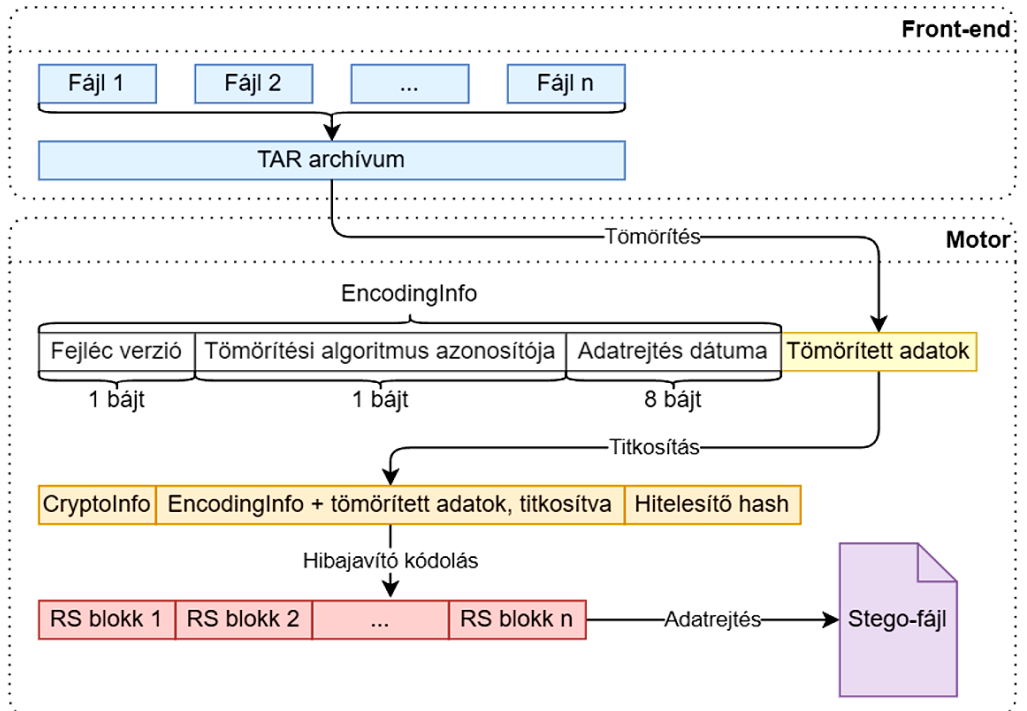
Amikor először találkoztam a szteganográfiával, mint tudományággal, azt tapasztaltam, hogy nem volt olyan ingyenesen elérhető adatrejtő szoftver, amely egy ilyen szoftverrel kapcsolatos elvárásaimat kielégítette volna.

Szakdolgozatom első részében ezzel a problémával foglalkozom. Egy egyszerű értékelési rendszer keretében felmértem számos elérhető szoftvert különféle szempontok szerint, hogy egy általános képet kapjak az elérhető funkcionálisokról, illetve hiányosságokról. Ezt követően az értékelési rendszer szempontjából legjobb szoftvereket közelebbről is megvizsgálom, például információ-biztonsági szempontból is.

A levont tanulságok, illetve az elvárásaim fényében egy biztonságos, rugalmas és felhasználóbarát adatrejtő szoftver elkészítését határozom meg célkitűzésként, amely igyekszik kiküszöbölni a konkurens szoftverekben talált problémákat is. Ennek megfelelően határozom meg az elkészítendő szoftver specifikációját, ahol a követelmények rangsorolása a MoSCoW módszer szerint történik.

Dolgozatom hátralévő részében próbát teszek egy ezen követelményeknek megfelelő szoftver kifejlesztésére, amelynek első lépéseként egy előzetes tervezési fázist részletezek. A tervezés során – az ábrán is látható adatrejtési folyamat lépéseinek megfelelően – rétegekre bontom a program motorját, illetve meghatározom az egyes rétegekben használatos algoritmusokat. Ebben a fejezetben ismertetem a fejlesztés során használt eszközöket és konvenciókat is.

Ezt követően a már megvalósított program, valamint a megvalósítás során meghozott további tervezési döntések kerülnek tárgyalásra. Az elkészült programot a dolgozat első részében használt értékelési rendszerrel



is pontozom, illetve mérlegelem a konkurenciával szemben. A projekt során csak egy egyszerűbb szteganográfiai algoritmus került implementálásra, a Random-LSB, amellyel a program PNG-kiterjesztésű fájllokba képes adatot rejteni. A program hasznosságát jelentősen fokozná, ha képes lenne több fájltypussal működni (legfőképp veszteségesen tömörített fájltypusokkal) – így ez az egyik elsődleges lehetséges továbbfejlesztési iránya.

Úgy érzem a fejlesztés során a legnagyobb kihívást a kriptográfia kutatása és implementációja jelentette, ami jelentős időráfordítást igényelt. Még a dolgozat végleges verziójának leadása után is találtam egy kisebb biztonsági problémát, amit azóta javítottam.

A szerzőről



TIBOR ATTILA GÁBOR tanulmányait 2018-ban a BME VIK mérnök-informatikus alapképzésén kezdte, végül a Dunaújvárosi Egyetem mérnök-informatikus alapképzésén fejezte be, szoftvertechnológia szakirányon. Jelenleg a Thyssenkrupp Components Technology Hungary Kft.-nél dolgozik szoftver-tesztmérnökként.

Adaptív fuzzing módszertana autóiipari környezetben

SASKA SZILVIA

BME, VIK, Hálózati Rendszerek és Szolgáltatások Tanszék
saska.szilvi09@gmail.com

Konzulensek: Schulcz Róbert (BME, Hálózati Rendszerek és Szolgáltatások Tanszék),
Babud Imre (thyssenkrupp Components Technology Hungary Kft.)

Kulcsszavak: kiberbiztonság, autóiipar, tesztelés, fuzzer

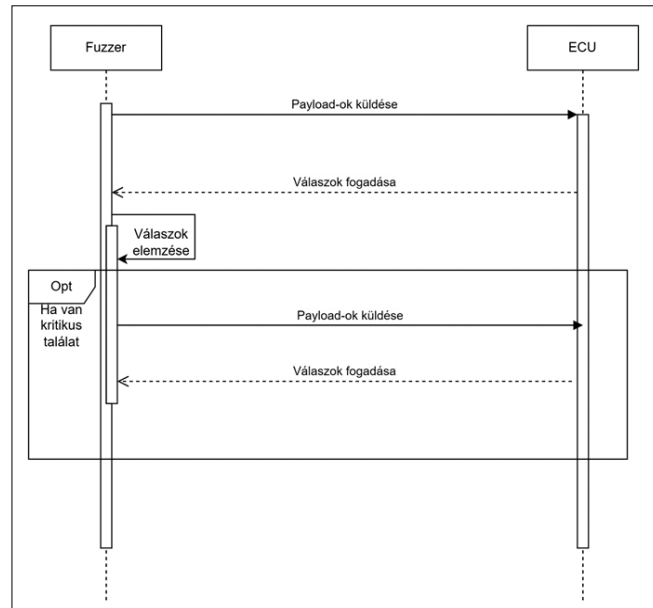
A mai modern járművek egyre összetettebb rendszerekből állnak össze. Ennek a növekvő komplexitásnak megfelelően a támadási és sérülékenységi pontok száma is növekszik. Az új technológiák, például az önvezető járművek és a kommunikációs hálózatok fejlődése új biztonsági kihívásokat vet fel. Ennek eredményeként az autóiipari kiberbiztonságnak alkalmazkodnia kell a változásokhoz, és új módszerekkel kell lépést tartania a nagy kihívásokkal. Az új, hatékonyabb eszközök fejlesztése és alkalmazása révén pedig biztonságosabb rendszerek jöhetnek létre. Az autóiipari szektor szereplőinek alkalmazkodniuk kell a megnövekedett igényekhez, ami új tesztelési eljárások széles skálájának megjelenéséhez és beépítéséhez vezet a termékfejlesztési folyamataikban.

Az autóiiparban egyre elterjedtebbé válik az információs technológiák világából ismert fuzzing módszer alkalmazása, különösen a fenti jelenségek hatására. A fuzzing olyan technika, amelynek során a szoftver vagy a rendszer bemeneteinek véletlenszerűen módosított változatait tesztelik annak érdekében, hogy felfedezzék a hibákat és sérülékenységeket.

Szakdolgozatomban az okos fuzzing módszertanát mutatom be, mely elméleti tesztesetek kidolgozásával is foglalkozik. Ezek a tesztesetek az autóiiparban használt UDS (Unified Diagnostic Services) és CAN (Control Area Network) protokollokra épül.

Munkám első részében az olvasó megismerkedhet a fent említett autóiipari protokollokkal, illetve a különböző tesztelési technikákkal és módszertanokkal. Ezek után dolgozatom fő témájára, az okos, más néven adaptív fuzzing bemutatására kerül sor. A fejezetben belül megtalálható az adaptív és az egyszerű fuzzer általános összehasonlítása és a különböző iparágakban – fő hangsúly az IT és az autóiipar – használatos nyílt és zártforráskódú keretrendszerek is. A következő fejezetben bemutatom a két általam választott UDS szolgáltatás elméleti teszteseteinek felépítését (egy általánosabb és egy összetettebb folyamatot), melyeket adaptív fuzzer segítségével hoztam létre. Ezenfelül ismertetem a Security Access-hoz (egy specifikus UDS-szolgáltatás) való hozzáférés módszerét, valamint kifejtem az NRC- (Negative Response Code) kódokból tanuló adaptív fuzzer szerkezetét is.

A tervezés során az elsődleges célom az volt, hogy olyan eszközt lehessen kifejleszteni, amely képes auto-



matikusan finomhangolni a tesztelési folyamatot a gyűjtött, illetve a kapott adatok alapján. A hatékony adaptív megoldásokhoz egy általam kidolgozott stratégiát is elkészítettem, melynek a fő lépéseit pontokba szedtem.

Munkámban a fuzzer architektúráját legtöbb esetben Python-kód példákkal és szekvenciadiagramokkal mutatom be. Az ábrán a TesterPresent funkcióhoz tartozó válasz elemzést lehet látni, mely a mai modern járművekben alapfunkciónak tekinthető.

Az utolsó részben áttekintem a kutatásom továbbfejlesztési lehetőségeit és következtetéseit annak érdekében, hogy a jövőben hatékony és eredményes felhasználást lehessen biztosítani.

A szerzőről



SASKA SZILVIA tanulmányait a Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Karán végezte üzemmérnök-informatikus szakon, Hálózat és Biztonság specializáción. A jövőben szeretne kiberbiztonsági területen elhelyezkedni.