DOI: https://doi.org/10.12700/btsz.2025.7.3.167

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: ANOMALIES IN THE TRACKING (APPLICATION OF MACHINE LEARNING TECHNIQUES TO DETECT NETWORK ANOMALIES)

MESTERSÉGES INTELLIGENCIA A KIBERBIZTONSÁGBAN: ANOMÁLIÁK NYOMÁBAN (GÉPI TANULÁSI TECHNIKÁK ALKALMAZÁSA HÁLÓZATI ANOMÁLIÁK DETEKTÁLÁSÁRA)

OLÁH Róbert[1]

Abstract

With the rise of digitalization, cybersecurity has become one of the most critical areas of our time. The IT infrastructures of corporate and government systems are exposed to various cyber attacks every day, such as DDoS attacks, data leaks, network penetration attempts or even internal unauthorized activities. These events can cause serious damage not only financially but also in terms of reputation. Network models and their operation play an important role in building IT infrastructures. The reliable operation of modern IT systems fundamentally depends on the stability and protection of network infrastructures. With the increase in digital traffic, threats to networks are also becoming increasingly complex and frequent. In the IT network, countless network devices have a role in the operation of the network. Network anomalies are becoming an increasingly challenging issue in network traffic. The aim of the research is to investigate the effectiveness of various machine learning algorithms for detecting network anomalies in the cybersecurity context.

Keywords

anomalies, detecting, cybersecurity, various machine,network traffic

Absztrakt

A digitalizáció térnyerésével a kiberbiztonság napjaink egyik legkritikusabb területévé vált. A vállalati és állami rendszerek informatikai infrastruktúrái nap mint nap ki vannak téve különféle kibertámadásoknak, mint például DDoS támadásoknak, adatszivárgásoknak, hálózati penetrációs próbálkozásoknak vagy akár belső jogosulatlan tevékenységeknek. Ezek az események súlyos károkat okozhatnak nemcsak anyagi, de reputációs szempontból is. A hálózati modellek és annak működése fontos szerepet játszanak az informatikai infrastruktúrák építésében. A modern informatikai rendszerek megbízható működése alapvetően a hálózati infrastruktúrák stabilitásán és védelmén múlik. A digitális forgalom növekedésével a hálózatokat érő fenyegetések is egyre összetettebbé és gyakoribbá válnak. Az informatikai hálózatban számtalan hálózati eszköz működhet, amelynek szerepe van a hálózat működésében. A hálózati forgalomban egyre nagyobb kihívást jelentenek a hálózati anomáliák. A kutatás célja annak vizsgálata, hogy milyen hatékonysággal alkalmazhatók különböző gépi tanulási algoritmusok a hálózati anomáliák detektálására a kiberbiztonság kontextusában.

Kulcsszavak

anomália detektálása, gépi tanulás, hálózati modellek, hálózati forgalom

[1] olah.robert0721@gmail.com | ORCID: 0009-0007-9134-9521 | IT teacher, Center of Erd Education | Informatika oktató, Érdi Tankerületi Központ

BEVEZETÉS - A TÉMA ELMÉLETI BEMUTATÁSA (SZAKIRODALOM-FELDOLGOZÁS)

Háttér és problémafelvetés

A kutatásom témája a mesterséges intelligencia a kiberbiztonságban gépi tanulási technikák alkalmazásával az informatikai hálózati anomáliák detektálására. A témakör fontos szerepet játszhat a hálózat biztonságos működésére tekintve.

A digitalizáció térnyerésével a kiberbiztonság napjaink egyik legkritikusabb területévé vált. A vállalati és állami rendszerek informatikai infrastruktúrái nap mint nap ki vannak téve különféle kibertámadásoknak, [8] mint például DDoS támadásoknak, adatszivárgásoknak, hálózati penetrációs próbálkozásoknak vagy akár belső jogosulatlan tevékenységeknek [13]. Ezek az események súlyos károkat okozhatnak nemcsak anyagi, de reputációs szempontból is. A hálózati modellek és annak működése fontos szerepet játszanak az informatikai infrastuktúrák építésében. A modern informatikai rendszerek megbízható működése alapvetően a hálózati infrastruktúrák stabilitásán és védelmén múlik. A digitális forgalom növekedésével a hálózatokat érő fenyegetések is egyre összetettebbé és gyakoribbá válnak. Az informatikai hálózatban számtalan hálózati eszköz működhet, amelynek szerepe van a hálózat működésében. A hálózati forgalomban egyre nagyobb kihívást jelentenek a hálózati anomáliák. A hálózati anomáliák – mint például az elosztott szolgáltatásmegtagadásos (DDoS) támadások, jogosulatlan behatolások vagy hibás konfigurációk – jelentős kockázatot jelentenek a szolgáltatások folyamatosságára és az adatok biztonságára nézve. [13] A hagyományos, szabályalapú forgalomelemző rendszerek korlátozottan képesek kezelni a dinamikusan változó és ismeretlen támadási mintákat. Ezek az eszközök jellemzően múltbeli minták alapján működnek, így nem alkalmasak előre nem látott fenyegetések azonosítására. Mindez rámutat arra, hogy a hálózati biztonság jövője a prediktív, adaptív technológiák felé mutat, ahol kiemelt szerepet kapnak a mesterséges intelligencián és gépi tanuláson alapuló megközelítések.

A hagyományos, szabályalapú biztonsági rendszerek – például tűzfalak vagy behatolásérzékelő rendszerek (IDS) – egyre kevésbé bizonyulnak hatékonynak a folyamatosan fejlődő fenyegetések ellen. Ezzel párhuzamosan megjelent az igény olyan adaptív, tanulásra képes rendszerek iránt, amelyek képesek ismeretlen támadási minták felismerésére is. A mesterséges intelligencia (MI/AI) és azon belül a gépi tanulás (ML) lehetőséget kínál arra, hogy a hálózati viselkedést folyamatosan monitorozzuk. [20]

Célkitűzés és hipotézis

Jelenlegi kutatásom célja gépi tanuláson alapuló megközelítések bemutatása hálózati forgalmi anomáliák észlelésére, figyelembe véve az algoritmikus hatékonyságot és a hálózati forgalom optimalizálás és AI alapú eszközkonfiguráció. A kutatás során különböző gépi tanulási algoritmusokat kívánok alkalmazni az anomáliadetektálás pontosságának és hatékonyságának javítása érdekében. Azt állítom, hogy a gépi tanulási algoritmusok pozitív hatással lehetnek a hálózati forgalmi anomáliák észlelésére.

Hogyan viszonyul a felügyelt és a felügyelet nélküli tanulás teljesítménye a hálózati adatok elemzésében?

A kutatás hipotézise az, hogy a mélytanulási modellek (pl. autoenkóderek, rekurzív neurális hálózatok) hatékonyabbak az összetett és rejtett anomáliák észlelésében, mint a hagyományos, szabályalapú vagy klasszikus gépi tanulási módszerek (pl. döntési fák,

SVM). A hálózati forgalom folyamatos növekedésével egyre nagyobb kihívást jelent a hálózati anomáliák, például a DDoS-támadások és a nem szándékos hálózati hibák időben történő észlelése. Az ilyen anomáliák veszélyeztethetik az informatikai rendszerek biztonságát és működését is. A hagyományos forgalomelemző rendszerek gyakran nem képesek hatékonyan észlelni a dinamikusan változó, ismeretlen támadásokat, mivel nem használnak adaptív algoritmusokat. Ezért gépi tanulási technikák alkalmazása szükséges a hálózati anomáliák észleléséhez. [4]

MÓDSZERTAN

A kutatás során kvantitatív megközelítést alkalmazok. A kutatás során többféle gépi tanulási algoritmust fogok alkalmazni, beleértve a felügyelt és felügyelet nélküli tanulást, mint például a döntési fákat, k-means klaszterezést, illetve a mély tanulási modelleket, mint az autoencoder-eket és neurális hálózatokat. A hálózati forgalom elemzéséhez nyilvános adatokat fogok használni (például KDD99 vagy NSL-KDD), melyeket előfeldolgozott, hogy megfelelő bemeneteket kapjanak a modellek számára. [16]

A vizsgálathoz nyílt forrású hálózati forgalom-adatbázisokat használunk, például:

- **NSL-KDD** – kiegyensúlyozott hálózati forgalomadatok különféle támadásokkal
- **CICIDS2017** – modern, valósághű hálózati viselkedések és támadások. [16]

USN-NB15-komplex, új típusú hálózati fenyegetések. A felügyelt és felügyelet nélküli tanulást, mint például a döntési fákat, k-means klaszterezést, illetve a mély tanulási modelleket, mint az autóencodereket és neurális hálózatokat. Az NS-KDD az egyik legismertebb behatolásérzékelésre felkészített adatbázis. Több különböző informatikai hálózati forgalom van benne, amely normál és támadó pozíciót felvevő viselkedésre utaló jellemzők vannak.

A CICIDS2017 adatbázis a hálózati forgalomra van specializálva, modern támadási mintákat tartalmaz, ami hatékonyan használható és hálózati felderítésre alkalmazható a biztonsági intézkedések során, amely gyakorlatban is előfordulhatnak. Támadástípusok botnet, port scan, DDDoS, webes támadás, brute force. Több mint 80 attributúmal ad jellemzést az eseményről. Mélytanulásnál kiemeleten jól alkalmazható.

Az UNSW-NB15 az Australian Centre for Cyber Security által létrehozott adatbázis, amely tartalmaz modern támadási módszereket, a normál informatikai hálózati forgalom reprezentációjához alkalmas. 9 különböző támadási mintáét tartalmaz, pl: DoS, backdoor, shelcode. A hálózati esemény több mint 40 jellemzővel bír, az OSI modell alapján a hálózati réteg, csomaginformációk, és hálózati forgalmakat is tekintve kerülnek levonásra. Az adatbázis jól **alkalmazható gépi tanulásra, és alhálózat teljesítmény mérésére.** Azonban jobb választás lehet TON_IoT Datasets adatbázis, ami megfelel a kor szellemének és folyamatosan frissítik. Az adatbázis az MI-re van készítve hálózat támadások ellen. Többnyire logok és hálózati forgalom van benne. Támadástípusok amire alkalmas az adatbázis rendszerbeli alkalmazásra (injection,scanning, DoS, DDoS, ransomware). A modell alkalmas mélytanulásra.

CSE-CIC-IDS2021

Ez az adatbázis heterogén forgalomra is alkalmas, megfelel a modern támadási típusoknak pl. brute-force, SQL injection. Ennek segítségével valós hálózati környezetet tudunk szimulálni. Többdimenziós adattal rendelkezik, amit betanításra fel tudunk használni, mélytanulásra alkalmas az adatbázis. Számos helyen alkalmazzák. A következő támadástípusokat ismerjük: Brute-force (SSH, FTP), Web alapú támadások (XSS, SQL injection),Malware / RansomwareBotnet / Command and Control (C&C), Denial of Service (DoS, DDoS),Infiltration / Backdoor Phishing,Man-in-the-Middle (MITM), VPN-alapú elrejtett forgalmakat is kezel. Célunk, hogy az adatbázis segítségével alkalmazzuk a rendszerben a lehetséges adatbázis minták segítségével a hálózati sérülékenység és a támadás lehetőségét. Az NSL-KDD különféle hálózati forgalmakat tartalmaz, amelyeket normál és támadó viselkedésekre osztanak

ALGORITMUSOK

Az algoritmusok fontos szerepe van a programok létrehozása során. Az alábbi táblázat tartalmazza azokat az algoritmus típusokat, amelyek felderíthetik az informatikai hálózat anomáliákat, amelynek jelentős hatása van a hálózat biztonságos működésében. Az alábbi 6 szempontot vizsgáltam meg, előnyök és hátrányokat is figyelembe véve, amely alapján besoroltam osztályzási szintet is. A táblázat jól összefoglalja melyik algoritmus milyen szempontokat helyez előtérbe, és annak alkalmazásának lehetőségét.

	Algoritmus / módszer	Miért hasznos egy működő hálózat hibakezelésében?
1	Bayes-hálók (Bayesian Networks)	Hibák okainak valószínűségi modellezése (pl. router, kapcsolat, eszközhiba). Diagnózisban kiváló.
2	Reinforcement Learning (megerősítéses tanulás)	A rendszer tanul, hogyan javítsa ki önmagát – például útvonalváltás vagy újrakonfigurálás automatikusan.
3	Root Cause Analysis + Decision Trees	Hibák okainak automatikus feltérképezése szabály-alapú vagy tanuló döntési fákkal.
4	Autoencoder + hibajelzések monitorozása	Ismeretlen hibák és viselkedések feltárása automatikusan a hálózati viselkedésből.
5	LSTM (idősoros hálózati log elemzéshez)	Hálózati eseménysorokból időben felismeri, ha hibába fut a rendszer – megelőző figyelmeztetés/javítás.
6.	Graph Neural Networks (GNN)	A hálózat mint gráf modelle zése. Képes lokalizálni, hogy a topológia mely pontján lép fel hiba.
7.	Runbook Automation Anomaly Detection +	Pl. egy szabály-alapú motor (pl. Runbook Automation) az észlelt anomáliák automatikus orvoslására.
8.	Predictive Maintenance modellek (ML alapú)	Előrejelzi, mikor és hol lesz esedékes egy hiba (pl. router túlterhelés, sávszélesség telítődés).
9.	Configuration Drift Detection (pl. diff modellek)	Gépi tanulással figyeli, ha a konfiguráció eltér az optimálistól, és visszaállítja.
10.	AI-Ops rendszerek (pl. IBM Watson, Moogsoft, Dynatrace)	Gépi tanulással figyelik, diagnosztizálják és javítják az IT infrastruktúra problémáit, valós időben.

1. táblázat Ajánlott algoritmusok és módszerek önjavító hálózati rendszerekhez, saját szerkesztés

A fenti táblázatot az alábbi szempontok szerint osztályoztam vizsgálva a hatékonyságot is. A hálózati anomáliák felderítésében fontos, hogy a feladat specifikációjához mérten válaszunk algoritmust. Az alábbi táblázat jól összefoglalja az előnyöket és hátrányokat is, amely kutatásom egyik fő szempontja.

	Algoritmus	Előnyök	Hátrányok
1.	*Bayes-hálók*	*- Képes valószínűségi hibadiagnózisra - Jól modellezi az ok-okozati kapcsolatokat*	*- Szükség van részletes hálózati modellezésre - Nehéz karbantartani komplex rendszernél*
2.	*Reinforcement Learning (RL)*	*Jól alkalmazható dinamikus hálózatokra - Képes tanulni javító lépéseket*	*- Nehéz visszavonni hibás „döntéseket” - Lassú tanulás, sok próbálkozás kell*
3.	*Decision Tree / Root Cause Analysis*	*-Hatékony ismert hibák felismerésére -egyszerű logikai struktúra*	*- Nehezen skálázható - Új típusú hibák esetén nem működik jól*
4.	*Autoencoder (deep learning)*	*-Ismeretlen hibákat is felismer -Nem igényel címkézett adatot*	*-Csak azonosít, nem javít*
5.	*LSTM (idősoros elemzéshez)*	*Előrejelezhetőek a hibák Felismeri időbeli mintázatokat*	*Nehéz értelmezni és tréningezni Sok adat kell*
6.	*Graph Neural Network (GNN)*	*Lokalizálja a hibapontokat A hálózat topológiáját természetesen modellezi*	*Nagy számítási igény Fejlett implementáció szükséges*
7.	Anomaly Detection + Runbook Automation	Szabályokkal jól kezelhető visszatérő hibák Gyors beavatkozás	- Kézzel kell karbantartani a szabályokat - Korlátozott rugalmasság
8.	Predictive Maintenance (ML)	Csökkenti a leállásokat Előre jelzi a hibákat	Pontos előrejelzéshez sok jó adat kell - Csak ismétlődő, trendalapú hibáknál hasznos
9.	Configuration Drift Detection	Könnyen automatizálható - Megőrzi a hálózati állapot stabilitását	- Manuális beavatkozás szükséges lehet - Nem minden hiba konfigurációs
10.	AI-Ops rendszerek (pl. Moogsoft, Dynatrace, Watson)	Több technológiát integrál - Komplett megoldás valós idejű és automatikus beavatkozással	-komplex bevezetés

2. táblázat Algoritmusok előnyök és hátrányok, saját szerkesztés

Hálózati algoritmusok értékelése kutatási elemzés alapján

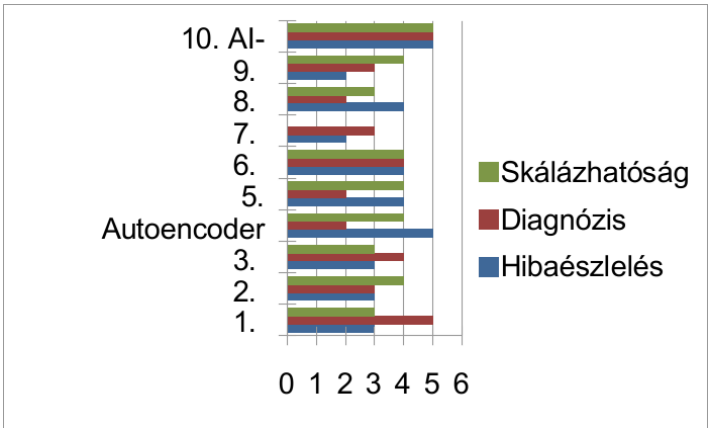
- Hibaészlelés pontossága, Diagnosztikai képesség (hiba okának azonosítása)
- Automatikus javítás lehetősége, Skálázhatóság (nagy hálózatokon való használhatóság)

Magyarázhatóság (mennyire érthető az eredmény) 1 = gyenge / nem jellemző, 5 = kiváló / erős képesség

Algoritmus / Módszer	*Hibaészlelés*	*Diagnózis*	*Skálázhatóság*
1. Bayes-hálók	*3*	*5*	*3*
2. Reinforcement Learning	*3*	*3*	*4*
3. Decision Tree	*3*	*4*	*3*
4. Autoencoder	*5*	*2*	*4*
5. LSTM (idősor)	*4*	*2*	*4*
6. Graph Neural Network	*4*	*4*	*4*
7. Runbook Automation	*2*	*3*	*3*
8. Predictive Maintenance	*4*	*2*	*3*
9. Config Drift Detection	*2*	*3*	*4*
10. AI-Ops rendszerek	*5*	*5*	*5*

2. táblázat (algoritmusok osztályzás) saját szerkesztés

Grafikonon ábrázolva:



1. grafikon algoritmusok kiértékelése, saját szerkesztés

HÁLÓZATI FORGALOM OPTIMALIZÁLÁS

AI-algoritmusok képesek folyamatosan monitorozni a hálózati forgalmat, és automatikusan módosítani az adatátviteli irányokat, hogy csökkentsék a torlódásokat vagy op-

timalizálják a késleltetést. Ilyen algoritmusok például a gépi tanulás (ML) alapú forgalomelőrejelzés, amely segíthet a dinamikus útvonalválasztásban. A hálózati forgalom optimalizálására vizsgálat alá venném az alábbi algoritmusokat.

- **Reinforcement Learning (DRL, Q-learning)**,
- **LSTM**,
- **GNN**,

Képesek optimalizálni a hálózati forgalmat, **csökkenteni a torlódást**, **javítani a válaszidőt**, és **önálló döntéseket hozni** az adatútvonalakról – még **valós időben is**.

Q -learning algoritmus

Ez táblázatban tárolja az **állapot–akció értékeket (Q-értékeket).** Q(s, a) – megtanulja, hogy egy adott **állapotban (s)** melyik **akció (a)** a legjobb. Csak **kis mértékű problémákra** alkalmas, ahol az állapot- és akciótér nem túl nagy (pl. hálózat max. 10 csomópont).

Reinforcement Learning (DRL, Q-learning),

A **Reinforcement Learning** egy gépi tanulási paradigma, amelyben egy **ügynök (agent)** tanul interakciók során, hogy maximális jutalmat (reward) szerezzen. Az ügynök nem rendelkezik előre meghatározott címkékkel vagy adatokkal, hanem **próbálgatásos alapú tanulással** javítja döntéseit. [11]

Állapotok:

- **Állapot (State, S)**: Az ügynök aktuális helyzete a környezetében. Minden környezet egy állapotot reprezentál (pl. egy robot helyzete egy szobában).
- **Cselekvés (Action, A)**: Az ügynök által választott döntés vagy művelet az adott állapotban.
- **Jutalom (Reward, R)**: A cselekvés eredményeként kapott visszajelzés. Az ügynök a cselekvését úgy választja meg, hogy a jutalmat maximalizálja.**Politika (Policy, π)**: Egy függvény, amely meghatározza, hogy egy adott állapotban az ügynök milyen cselekvést végezzen. A politika lehet determinisztikus vagy valószínűségi.

Q-learning

Q-learning célja, hogy megtanulja az ügynök számára optimális politikát anélkül, hogy tudnia kellene a környezet dinamikáját.

A Q-learning algoritmus egy **Q-táblát** épít fel, amely az egyes állapot-cselekvés párosokhoz rendelt **Q-értékeket** tartalmaz. Ezek a Q-értékek azt mérik, hogy az adott állapotban végrehajtott cselekvés milyen várható jutalmat eredményez a jövőben.

A **Q-érték** (Q(s, a)) az alábbi képlettel frissíthető:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left(R_{t+1} + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t) \right)$$

- **s_t**: Az aktuális állapot.
- **a_t**: Az aktuális cselekvés.
- **R_{t+1}**: A cselekvés által kapott jutalom.
- **α\alphaα**: A tanulási sebesség, amely meghatározza, hogy mennyire veszi figyelembe az új információkat.

- **γ\gammaγ**: A diszkontálási tényező, amely az **új jutalmak** és a **jövőbeli jutalmak** közötti súlyt szabályozza [19]

LSTM(Long Short-Term Memory) [17]

Az LTMS egy idősor alapú algoritmus, ami alkalmas arra, hogy a hálózati forgalmat előre jelezze. Segítségével a hálózati forgalmi mintázatokat alapján előrejelzést kaphatunk a várható forgalomról, sávszélesség, és késleltetésről. Vizsgálva az algoritmust az időbeli összefüggéseket jól fel lehet ismerni, és jó teljesítményt mutat nemlineáris mintázatok esetében és hatékonyan alkalmazható a hálózati forgalom torlódás előrejelzés, és csomagkésés jóslására. [12]

Előnyök:

- Stabil tanulási folyamatot képvisel
- Képesség a hosszú mintázatok felismerésére.
- Időbeli adatok kezelése

Hátrány

- Számítási erőforrás
- Skálázási nehézségek
- Nagy adatmennyiség szükséges a tanuláshoz.

KÉPESSÉG A HÁLÓZATI ESZKÖZÖK ÖNÁLLÓ KONFIGURÁLÁSÁRA

Az AI képes önállóan beállítani a hálózati eszközöket, figyelembe véve a legfrissebb biztonsági szabványokat és az iparági legjobb gyakorlatokat, ezzel csökkentve az emberi hiba lehetőségét. A hálózati eszközöket kézzel előre megtervezett informatikai struktúra alapján konfiguráluk. Használhatunk hozzá különböző hálózat tervező programokat amelyek segítségével lemodellezhetjük a hálózat működését is. Azonban azt a lehetőség t vizsgálom hogyan lehetne gépi tanulási módszerekkel vizsgálni a hálózati biztonságot, felderíteni a behatolást és gépi tanulási módszerekkel védelmet is adni a hálózatnak.

OPTIMALIZÁLT ERŐFORRÁS KEZELÉS

A modern számítógépes hálózatok, a felhőalapú rendszerek, mobilhálózatok, növekvő kihívás elé állnak a hatékonyság terén is. Az informatikai infrastruktúrában a felhasználók száma dinamikusan nőhet, és a hagyományos hálózati menedzsmentben lehet olyan eset amikor nem képes kielégíteni az elvárt teljesítményt, rugalmasságot és legfőbbképpen a minőséget. A kor vívmányait követve, alkalmazhatjuk az AI technológiát, azon belül a gépi tanulást, megerősítéses tanulást. Reinforcement Learning – RL) és a tartós memóriával rendelkező LSTM [17] és a neurális hálózatot is. Az optimális erőforráskezelés célja az, hogy jelen esetben egy infrastrukturális és adott hálózati topológiájú hálózatban az erőforrások leghatékonyabb leosztása, amely segíthet a szolgáltatás működésének minőségében. Ha az MI megközelítést nézzük akkor, a forgalmi mintázatok alapján képes előre jelezni a hálózati túlterheltséget, és a döntéseket képes létrehozni majd beavatkozni a hálózat működésében, míg a hagyományos hálózat működésében kézzel manuálisan avatkozunk be és javítjuk ki a hálózati hibát, míg az MI alkalmazása egy előrelátó működést , tanult minták alapján döntést hoz és javít a hálózatban. A másik út a megerősítéses tanulás amely egy

ügynök segítségével tanulja alhálózati forgalomirányítást minimális késleltetés, és veszteség mellett, de figyel a megfelelő sávszélességre, amelyben a lehető legnagyobbat veszi alapul. A hálózatban dinamikus újra leosztását az LSTM hálózatok segítségével tehetjük meg, amely lehetővé teszi a hálózati forgalom előrejelzését, a várható hálózati terhelést, és a késleltetés egy becslésé**t.** [17] A harmadik szempont a gráfalapú neurális hálózatok, amely képes lemodellezni az adott hálózat topológiáját, támogatást adva a hálózatban a döntéshozatalra. A gyakorlati szempontot az AI alapra helyezzük, amely egy hálózati menedzsmentrendszer feltételez, szükség van egy hálózat monitorozó modulra, amely gyűjti az információkat a hálózatról, (pl.: késleltetés, hálózati terheltség. Jump) amit a (LSTM) fog feldolgozni, a megerősítéses tanulási rendszer komponense DQN pedig döntéseket hozhat, és segíthet a hálózati anomáliák csökkentésében a döntések és végrehajtási események alapján pl: új forgalomirányitás, ACL, szabályok javaslata vagy végrehajtása során a hálózatban. [21] Az rendszer képes lehet a teljesítményen javítani, amely hatékonyságot mutathat hosszú távon. Az optimális hálózati kezelés kulcsszerepet játszik az MI által vezérelt hálózatokban, amely képes lehet különböző hálózati állapotok alapján reagálni és javítani és tanulni is, a múltbéli eseményekből. Az AI képes a hálózati erőforrások (például memória, CPU, sávszélesség) automatikus felosztására és optimalizálására annak érdekében, hogy a hálózat minden egyes eleme a legjobb teljesítményt nyújtsa. [17]

KONKLÚZIÓ

A gépi tanulás alkalmazása a hálózati forgalomelemzésben ígéretes megoldás a dinamikusan változó támadások és anomáliák felismerésére, amelynek segítségével hatékonyabban beazonosítható az informatikai hálózati korábbról ismert vagy még nem ismert de érzékelhető hálózati fenyegetettség. Az algoritmusok segítségével és az MI is alkalmazva kiberbiztonsági szempontból védettebb informatikai rendszerhez juthatunk. A fenti táblázatokban felsorolt algoritmusok figyelembe véve az egyes előnyöket és hátrányokat is, egy jól összehangolt, és hatékony teljesítményű hálózatot is létre tudunk hozni. Attól függően, hogy mi a specifikáció, mi az, amit szeretnék megvalósítani kombinálhatjuk az algoritmusokat. Az osztályzás jól mutatja, hogy az előnyök és hátrányok alapján kimondható, hogy hatékonyságot érhetünk el a statikus algoritmusokhoz képest és figyelembe véve az emberi reakcióidőt is. A hálózati anomáliák jogosulatlan behatolások vagy hibás konfigurációk jelentős kockázatot jelentenek a szolgáltatások folyamatosságára és az adatok biztonságára nézve. Ha az emberi konfigurációt nézzük, a hálózat védelmét tűzfal konfigurációk, acl szabályok segítségével védik, itt azonban a kutatás arra irányul, hogy milyen módszerek és lehetőségeket lehetne használni a modern kor vívmányai alkalmazásával.

ÖSSZEFOGLALÁS

A digitalizáció és a hálózati technológiák rohamos fejlődése új kihívásokat állít a kiberbiztonság elé. A hagyományos, szabályalapú védelmi rendszerek nem képesek hatékonyan reagálni a dinamikusan változó, előre nem ismert fenyegetésekre. A tanulmány célja annak bemutatása, hogy a mesterséges intelligencia, különösen a gépi tanulási algoritmusok miként alkalmazhatók hatékonyan a hálózati anomáliák észlelésére, előrejelzésére és megelőzésére. A kutatás során különböző gépi tanulási modelleket, köztük autoencodereket, döntési fákat, megerősítéses tanulást és gráfalapú neurális hálózatokat vizsgáltunk, azok

előnyeivel, hátrányaival és alkalmazhatóságukkal együtt. A tanulmány részletesen bemutatja az egyes algoritmusok diagnosztikai képességeit, skálázhatóságát, valamint azt, hogy mennyire képesek támogatni az automatizált hibajavítást. A dolgozatban bemutatásra kerültek nyílt forráskódú adatbázisok (NSL-KDD, CICIDS2017, UNSW-NB15) alapján végzett elemzések, amelyek igazolják, hogy az AI-alapú rendszerek jelentősen javíthatják a hálózati biztonságot. Emellett kiemelésre került az AI szerepe a forgalom optimalizálásában, az önálló eszközkonfigurációban és az erőforrások hatékony kezelésében is. A kutatás megállapításai szerint a gépi tanulási technikák alkalmazása nemcsak a biztonsági fenyegetések pontosabb azonosítását teszi lehetővé, hanem a hálózatok proaktív, önjavító működésének alapját is képezheti. Ezáltal hozzájárulnak a megbízhatóbb, rugalmasabb és jövőállóbb informatikai rendszerek kialakításához.

FELHASZNÁLT IRODALOM

[1] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, 108–116. https://doi.org/10.5220/0006639801080116

[2] Ring, M., Wunderlich, S., Scheel, C., Landes, D., & Hotho, A. (2019). A Survey of Network-based Intrusion Detection Data Sets. *Computers & Security*, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.008

[3] Canadian Institute for Cybersecurity. (2021). CSE-CIC-IDS2021 Dataset. *University of New Brunswick*. https://www.unb.ca/cic/datasets/ids-2021.html

[4] Moustafa, N., Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). *Military Communications and Information Systems Conference (MilCIS)*. https://doi.org/10.1109/MilCIS.2015.7348942

[5] Ferrag, M. A., Maglaras, L., Derhab, A., Mukherjee, M., & Janicke, H. (2020). Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials*, 22(1), 196–248. https://doi.org/10.1109/COMST.2019.2951818

[6] Umer, M. F., Sher, M., Bi, Y., & Debar, H. (2022). Evaluating Deep Learning for Network Intrusion Detection: Benchmarks, Datasets, and Metrics. *Applied Sciences*, 12(3), 1458.

[7] Diro, A. A., & Chilamkurti, N. (2018). Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768.

[8] Krasznay Csaba, Bencsáth Boldizsár, Kiberbiztonság alapjai, Hálózati támadások, megelőzés, behatolás-észlelés, incidenskezelés, Nemzeti Közszolgálati Egyetem, 2021

[9] Gál Zsolt, Kriptográfia, hálózati biztonság, kockázatelemzés, Typotex, 2017

[10] Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning MIT Press 2016

[11] Richard S. Sutton, Andrew G. Barto, Reinforcement Learning: An Introduction, MIT Press (2018)

[12] François Chollet , Deep Learning with Python, Manning Publications 2017 Using LSTMs to Predict the Next Word 6. chapter 185.
[13] William Stallings, Network Security Essentials, Pearson, 2009
[14] Aiko Pras, Paul C. van Oorschot , DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Mitigation 2014
[15] Ivan Nikolaev, Hands-On Network Security with Python: Implementing Real-Time Network Traffic Analysis and Intrusion Detection, Packt Publishing, 2020
[16] Stefan A. W. S. V. G. Gattaca, Machine Learning and Data Science in Cybersecurity: A Practical Guide to Real-World Solutions, Wiley, 2023
[17] Ian Goodfellow, Yoshua Bengio, Aaron Courville , Deep Learning, MIT Press, 2016
[18] S. Chakrabarti, S. N. Balakrishnan, R. Krishna , Deep Learning for Graphs, Springer, 2020
[19] Richard S. Sutton, Andrew G. Barto, Reinforcement Learning: An Introduction, MIT Press, 2018 second press
[20] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley(2011)
[21] Maxim Lapan , Deep Reinforcement Learning Hands-On, Packt Publishing 2018