



FEJLETT ÁGENSALAPÚ BEHATOLÁS-ÉRZÉKELŐ RENDSZEREK

SIMÓ ZSUZSA

George Emil Palade Orvosi, Gyógyszerészeti, Tudomány- és Technológiai Egyetem
Marosvásárhely, Románia

zsuzsa.simo@umfst.ro

IANTOVICS LÁSZLÓ BARNÁ

George Emil Palade Orvosi, Gyógyszerészeti, Tudomány- és Technológiai Egyetem
Marosvásárhely, Románia

barna.iantovics@umfst.ro

TOKODY DÁNIEL

Óbudai Egyetem, Budapest

daniel_tokody@ieee.org

Absztrakt: A behatolás-észlelő rendszer (Intrusion Detection System – IDS) a hálózati forgalmat és a felhasználói tevékenységeket figyeli rosszindulatú adatforgalom felderítéséhez osztott környezetben. Jelen tanulmány néhány előzetes eredményt mutat be, az IDS-ek telepítéséhez javasolt ágensalapú biztonsági megközelítéssel kapcsolatban. A decentralizált, ágensalapú IDS feladatokat oszt ki az ágenseknek a fenyegetések felismeréséhez szükséges adatok gyűjtésére, elemzésére és szállítására. Javaslatunk előnyei a következők: nincs egyedi meghibásodási pontja, korlátozza a hálózati terhelést és késést, és megfelelő IDS-modellt jelent nagy hálózati környezetek számára. Ilyen például az egészségügyben szereplő páciensek személyes adatainak védelme, amely gépi tanuláson alapuló predikciós algoritmusokkal kombinálva hatékonyabb védelmet biztosíthatnak.

Kulcsszavak: *intelligens ágens, Ipar 4.0, behatolásérzékelő rendszer, gépi tanulás, egészségügyi predikciók*

1. Bevezetés

A behatolás-észlelő rendszer egy olyan szoftveres alkalmazás, amely a hálózat és/vagy rendszer tevékenységeit figyeli annak érdekében, hogy kiszűrje a rosszindulatú tevé-

kenységeket [1, 2]. A behatolás-észlelő rendszerek legfontosabb feladata a lehetséges incidensek beazonosítása, a róluk szóló információk naplózása és a kérésre behatolási kísérletek jelentése. A behatolás-észlelő rendszerek korlátai általában a következők: a valós támadások száma kevesebb, mint a téves riasztásoké, a szoftverhibák rossz csomagok létrejöttét eredményezhetik, a kiszabadult helyi csomagok téves riasztásokhoz vezethetnek stb.

A kognitív ágensalapú rendszerek [3, 4, 5] ígéretes kutatási irányt jelentenek számos bonyolult probléma megoldásához. A bemutatott eredmények [6, 7], azt bizonyítják, hogy az ágensalapú rendszerek megfelelő megoldást kínálnak a behatolásérzékelés problémáira is.

Jelen tanulmány egy olyan intelligens ágensalapú biztonsági megközelítést javasol, amely az osztott környezetben telepített IDS-eknél alkalmazható. A decentralizált, ágensalapú IDS feladatokat oszt ki az ágenseknek a fenyegetések felismeréséhez szükséges adatok gyűjtésére, elemzésére és szállítására. Ilyen bizalmas adatok védelme főként az egészségügyi területhez tartozó betegek esetén válik fontossá, ahol olyan iparágban szabályozások betartásában alkalmazzák, mint a HIPAA (U.S. Health Insurance Portability and Accountability Act), azaz az egészségbiztosítás hordozhatóságáról és elszámoltathatóságának törvénye [8].

A tanulmányt a továbbiakban a következők szerint tagoltuk: A 2. fejezetben a legújabb IDS-megoldásokat mutatjuk be, míg a 3. fejezet az általunk javasolt IDS-megoldást részletezi. Végül a 4. részben a kutatás eredményeit foglaljuk össze.

2. A legújabb behatolás-észlelő rendszerek

Az IDS-ek két nagy csoportra oszthatók: hálózati behatolás-észlelő rendszerek (lásd [9, 10]) és a hostalapú behatolás-észlelő rendszerek (lásd [11, 12]). A hostalapú behatolás-észlelő rendszer egy ágensből áll, amely a megfigyelő szenzor szerepét tölti be egy olyan hoston, amely a rendszerhívások, alkalmazásnaplók és fájlmodosítások elemzésével felismeri a behatolásokat. A hálózati behatolás-észlelő rendszerek a hálózati forgalom vizsgálatával és több host megfigyelésével képesek felismerni a behatolásokat. A hálózati behatolás-észlelő rendszerben speciális szenzorok figyelik a hálózati forgalmat és elemzik az egyes csomagok tartalmát a rosszindulatú adatforgalom észlelése érdekében.

A Jha és Hassan [13] által javasolt megoldás alapjául a Linux platformra épülő szabályalapú ágensek szolgálnak. A kutatásban ez a megoldás mind megelőző mind pedig reagáló behatolásészlelésként is szolgál. A megelőző megoldás esetében egy hálózatalapú ágens figyeli a hálózatba belépő összes csomagot, és egy előre meghatározott szabály szerint keres egy ismert támadást. A második megoldás egy különálló hostalapú ágensen keresztül valósul meg, amely a meghatározott naplófájlok rutinszerű ellenőrzésére specializálódott annak érdekében, hogy észlelje a sikeres támadások eredményeképpen jelentkező rendszeranomáliákat.

Denning és Dorothy [14] egy olyan IDS-modellt javasol, amely különböző statisztikai számításokat alkalmaz az anomáliák észlelésére. Ez a megoldás számos mai IDS-rendszer, mint például az IDES, alapjául szolgált [15].

Wisdom és Sense (W&S) 1989-ben a Los Alamos National Laboratory-ban [16] fejlesztett ki egy statisztikaalapú anomália-észlelő megoldást. W&S statisztikai elemzések alapján állított fel bizonyos szabályokat, majd alkalmazta azokat az anomáliák észlelésében.

Az IDS-rendszerek közé tartozik még többek között a Multics [17], az Audit Data Analysis and Mining [18], a Bro [19], a Probabilistic Agent-Based Intrusion Detection (valószínűségi ágensalapú behatolás-észlelő) rendszer (PAID) [20], és a CIDS [21]. Az iparágban használt különböző IDS-ek leírását a [22–24] tanulmányok tartalmazzák.

Khan és Pi [25] 2019-ben egy olyan hibrid-többszintes anomália predikciós megközelítést valósítottak meg, amelyek a behatolásészleléshez a felügyeleti, szabályozó és adatgyűjtő rendszer (Supervisory Control and Data Acquisition-rendszerek – SCADA) esetén 97%-os pontosságot értek el, mialatt alacsony számítási kapacitásra van szüksége.

Az egészségügyben számos alkalmazása létezik az IDS-rendszereknek. Hady és Gubaish [26] 2020-ban egy olyan orvosi és hálózati adatokra épülő IDS-rendszert javasolt, amely valós idejű és egy továbbfejlesztett egészségügyi figyelőrendszer. A betegek megfigyelt biometrikus adatait egy távoli szerverre küldték, amely a továbbiakban diagnózist állíthat fel vagy kezelési döntéseket hozhat. Ehhez közbeékeződes kibertámadásokat (man-in-the-middle – MITM) alkalmaztak, amely 16 ezer rekordján gépi tanuló módszereket alkalmaztak és bizonyítottan 7–25%-os teljesítménybeli javulást értek el. Egy hasonló rendszert javasolt 2020-ban Saif és Das [27], akik egy metaheurisztikus algoritmusokon alapuló hibrid intelligens behatolás-érzékelő rendszert javasoltak a mentett egészségügyi adatok biztonsága és védelme érdekében. Az optimalizáláshoz részecske-raj-optimalizációt (PSO) és genetikus algoritmusokat (GA) használtak, illetve felügyelt algoritmusokkal (kNN, döntési fa) választották ki az adathalmaz legjobb jellemzőit, amely felülmúlta a korszerű megközelítéseket.

Bár számos hatékony IDS áll rendelkezésre, a kutatás iránya még mindig adott, tekintve a kibertámadások növekvő számát és változatosságát. Ennek jegyében szeretnénk bemutatni az elméleti hátterét annak az általunk javasolt IDS-nek, amely az összetett kibertámadások széles skáláját képes beazonosítani.

3. A javasolt IDS

A következőkben az osztott környezetben történő IDS-telepítéseknek egy új, decentralizált, ágensalapú biztonsági megközelítését szeretnénk röviden bemutatni. Néhány előzetes eredmény a javasolt rendszer kapcsán már megjelent egy korábbi cikkben [1]. A javasolt kooperatív többágenses rendszert a következőképpen jelöljük:

összeköttetés nélküli szolgáltatást használ a riasztási üzenetekhez, és összeköttetés-alapú szolgáltatást a Gyűjtő által összegyűjtött IDS-specifikus adatokhoz. Az Elemző ágensek több Gyűjtő ágenssel is kapcsolatot létesíthetnek. Ugyanazt az adatot pedig több Elemző ágens is megkaphatja. Ugyanakkor viszont a kritikus feladatokat, mint például a duplikált adatok kezelését az Elemző ágensek együtt oldják meg az IDS hatékony megvalósításának érdekében.

Az Elemző ágens adja át a Cselekvő ágensnek azokat a pontos utasításokat, amelyeket a Cselekvő ágensnek végre kell hajtania. Ezeket az utasításokat a Cselekvő ágens a következő tevékenységek formájában hajtja végre: új tűzfal-szabályok aktiválása, csomagok eldobása, portok és kapcsolatok lezárása, folyamatok befejezése stb. Az adott utasítást küldő Elemző ágens jelentést kap az egyes tevékenységek státuszáról.

Predikció esetében a Gyűjtőnél lévő adatokban az Elemző azonosítja az egyedi mintákat és jellegzetességeket, amelyet a Cselekvőnek továbbítva, elvégzi a predikciót és végrehajtja az így kapott feladatot. Ilyen például egy kórház prediktív karbantartási és adatbiztonsági rendszere, amely az orvosi gépeken levő szenzorok adatait felhasználva, a lehetséges minták által előrejelzi a szükséges karbantartást, mialatt olyan feladatokat hajt végre, amelyek ütemezik a karbantartást vagy épp figyelmeztetik a személyzetet az esetleges beavatkozásokról [28–30].

Az *IDS Problémamegoldó algoritmus* azt írja le, hogy az Ag_h -ként jelölt Elemző ágens hogyan járjon el, amikor egy bonyolult problémával ($Probléma_k$) szembesül (azaz egy olyan bonyolult helyzettel, amely támadásra utalhat). Azt szemlélteti, hogy az Ag_h a többi Elemző ágenssel együttműködve, hogyan tegyen kísérletet a $Probléma_k$ probléma megoldására, és hogyan határozza meg a végrehajtandó tevékenységet (tevékenységeket). A SOL_k jelöli a $Probléma_k$ megoldását.

IDS Problémamegoldó Algoritmus

BE: $Probléma_k$; **KI:** SOL_k

@ Ag_h átveszi $Probléma_k$ -t. Ag_h megbecsüli $Probléma_k$ szükséges feldolgozását.

HA (Ag_h fel tudja dolgozni $Probléma_k$) **akkor**

@ Ag_h feldolgozza $Probléma_k$ -t az eredmény _{h} megszerzésével.

HA (eredmény _{h} a megoldás) **akkor** @ SOL_k = eredmény _{h} ;

Különben @ Ag_h továbbítja az eredmény _{h} bejelentését A_n néhány ágensnek.

Vége Ha

Különben @ Ag_h továbbítja $Probléma_k$ bejelentését A_n néhány ágensnek.

Vége Ha

Ameddig ((a várakozási idő az A_n bejelentéséig nem járt le) **és** (a megoldást nem kapják meg)) **végezd**

@ Ag_h fogadja és értékeli az A_n bejelentésre érkező ajánlatokat.

Vége Ameddig

@ Ag_h odaítéli $Probléma_k$ egy megfelelő ágensnek, Ag_i -nek. Ag_h megkapja a Ps eredményt Ag_i ágenstől. Ha szükséges Ag_h feldolgozhatja a Ps eredményt, és megkapja a SOL_k megoldást.

VégeProblémamegoldás.

A $Probléma_k$ bejelentése, melyet A_n jelöl, a következő paraméterekkel rendelkezik: $A_n = \langle Szerepek_k, InfLista_k, Probléma_k \rangle$. A $Szerepek_k$ egy becsült specializációs listát jelent, amely szükséges a $Probléma_k$ megoldásához. Az $InfLista_k$ pedig az átdott információt jelöli, mint például az alkalmassági (*alkalmassági*) specifikációt, az ajánlat (*ajánlat*) specifikációt és a lejáratí idót.

Egy Ag_i ágensnek az A_n problémabejelentésre adott válasza (Val) az alábbi paraméterekkel rendelkezik: $Val = \langle A_n, Rv_k, Szerepek_k, Ajánlat_k, Képesség_k, Kapacitás_k \rangle$. $Ajánlat_k$ a problémamegoldásra adott ajánlat (amely lehet „elfogadás” vagy „elutasítás”). $Képesség_k$ jelenti az Ag_i ágens képességét. $Kapacitás_k$ pedig a feldolgozási kapacitását. $Szerepek_k$ az ágens által megadott becsült specializációs listát jelenti, amely szükséges az A_n bejelentésben meghatározott probléma megoldásához. Az Rv_k lista értékei megmutatják a specializációs lista pontosságát.

4. Konklúzió

Jelen tanulmány egy intelligens ágensalapú biztonsági megoldást mutat be az IDS-ek osztott környezetben való alkalmazásához. Néhány előzetes eredmény egy korábbi tanulmányban [1] már bemutatásra került. A javasolt megoldásban egy decentralizált, ágensalapú IDS feladatokat oszt ki az ágensek között azoknak az adatoknak a gyűjtésére, elemzésére és szállítására, amelyek szükségesek a fenyegetések felismeréséhez és a hatékony válaszlépések megtételéhez. Ennek a megközelítésnek fő előnyei közé tartozik a skálázhatóság, a hálózati késleltetés és terhelés kezelése, és az egyedi hibapont hiánya. A javasolt megoldás megfelelő IDS-modellként szolgál a nagy, heterogén hálózati környezetek számára. Másik fő alkalmazási területe az iparban, például az Ipar 4.0-ban és az okosgyárakban lehet, amelyek az eszközök széles skáláját használják, és ki vannak téve a kibertámadások veszélyének, illetve az egészségügyi területen is fontos szerepet játszik az intelligens egészségügyi alkalmazásokban és az Orvosi Dolgok Internetében (IoMT), mialatt számos megközelítés hangsúlyozza ki az IDS-rendszerek együttesének fontosságát a gépi tanulásban, a metaheurisztikus algoritmusokban és az anomáliák korai észlelésében az egészségügyi adatok biztonságának érdekében. A kiberfizikai rendszerek legfőbb sérülékenységeit egy korábbi tanulmány [31] mutatja be részletesen.

A továbbiakban fontos kiindulási alap lehet az egészségügyi predikciók fejlesztésére szolgáló IDS-technológiák a valós idejű anomáliák észlelésében, a fenyegetésre alapuló intelligens algoritmusok kidolgozásában az újonnan megjelenő kiberfenyegetésekkel szembeni ellenálló képesség növelésének biztosításában.

Irodalomjegyzék

- [1] Crainicu, B., Iantovics, B. (2011). An agent-based security approach for Intrusion Detection Systems. In: Hluchý, L. et al. (eds.). *7th Int. W. on Grid Computing for Complex Problems, Slovak Academy of Sciences, Bratislava*, pp. 126–134
- [2] Crainicu, B. and Iantovics, B. (2009), “*Cryptanalysis of KSA-like Algorithms*”, in B. Iantovics, et al. (Eds.), *Proc. of the First Int. Conf. on Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing*, IEEE Computer Society Press, pp. 130–148.
<https://doi.org/10.1109/CANS.2008.24>
- [3] Iantovics, B. (2008). *Agent-Based Medical Diagnosis Systems. Computing and Informatics*, Vol. 27, No. 4, pp. 593–625.
- [4] Chandiok, A. and Chaturvedi, D. K. (2018). *CIT: Integrated cognitive computing and cognitive agent technologies based cognitive architecture for human-like functionality in artificial systems. Biologically Inspired Cognitive Architectures*, Vol. 26, pp. 55–79.
<https://doi.org/10.1016/j.bica.2018.07.020>
- [5] Park, H.S., Tran, N. H. (2012). An autonomous manufacturing system based on swarm of cognitive agents. *Journal of Manufacturing Systems*, Vol. 31, Iss. 3, pp. 337–348.
<https://doi.org/10.1016/j.jmsy.2012.05.002>
- [6] Onashoga, A. S., Akinde A. D. and Sodiya A. S. (2009). A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems. *Issues in Informing Science and Inf. Technology*, Vol. 6, pp. 1–14.
- [7] Shamshirband, S. et al. (2013). An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. *Engineering Applications of Artificial Intelligence*, Vol. 26, Iss. 9, pp. 2105–2127.
- [8] Thompson, E. C. (2020). HIPAA Security Rule and Cybersecurity Operations. In: *Designing a HIPAA-Compliant Security Operations*. Apress, Berkeley, CA, pp. 23–36
- [9] Snort. [http://en.wikipedia.org/wiki/Snort_\(software\)](http://en.wikipedia.org/wiki/Snort_(software)) (utolsó letöltés: 2023. 09. 10.).
- [10] Liu, J., Gao, Y., Hu, F. (2021). A Fast Network Intrusion Detection System Using Adaptive Synthetic Oversampling and LightGBM. *Computers & Security*.
<https://doi.org/10.1016/j.cose.2021.102289>
- [11] Ossec. documentation <http://www.ossec.net/doc> (utolsó letöltés: 2023. 09. 10.).
- [12] Ou, C. M. (2012). Host-based intrusion detection systems adapted from agent-based artificial immune systems. *Neurocomputing*, Vol. 88, pp. 78–86.
<https://doi.org/10.1016/j.neucom.2011.07.031>
- [13] Jha, S., Hassan, M. (2002). *Building agents for rule-based intrusion detection system. Computer Communications*, Vol. 25, Iss. 15, pp. 1366–1373.
[https://doi.org/10.1016/S0140-3664\(02\)00038-5](https://doi.org/10.1016/S0140-3664(02)00038-5)
- [14] Denning, D. E. (1986). An Intrusion Detection Model. *Proceedings of the Seventh IEEE Symposium on Security and Privacy*, May, pp. 119–131.

-
- [15] Lunt, T. F. (1990). IDES: An Intelligent System for Detecting Intruders. *Proceedings of the Symposium on Computer Security; Threats, and Countermeasures*, Rome, Italy, November, 22–23, pp. 110–121.
 - [16] Vaccaro, H. S. and Liepins, G. E. (1989). Detection of Anomalous Computer Session Activity. *1989 IEEE Symposium on Security and Privacy*, May, pp. 280–289.
 - [17] Sebring, M. M. et al. (1988). Expert systems in intrusion detection: a case study. *Proc. of the 11th National Computer Security Conf.*, Baltimore, MD, October 1988, pp. 74–81.
 - [18] Barbara, D. et al. (2001). ADAM: Detecting Intrusions by Data Mining. *Proceedings of the IEEE Workshop on Information Assurance and Security United States Military Academy*, West Point, NY, June 5–6, pp. 11–16.
 - [19] Paxson, V. (1998). Bro: A System for Detecting Network Intruders in Real-Time. *Proceedings of The 7th USENIX Security Symposium*, San Antonio, TX.
 - [20] Gowadia V., Farkas C., Valtorta, M. (2005). PAID: A Probabilistic Agent-Based Intrusion Detection system. *Computers & Security*, Vol. 24, Iss. 7, pp. 529–545. <https://doi.org/10.1016/j.cose.2005.06.008>
 - [21] Dasgupta, D., Gonzalez, F. et al. (2005). CIDS: An agent-based intrusion detection system. *Computers & Security*, Vol. 24, Iss. 5, pp. 387–398. <https://doi.org/10.1016/j.cose.2005.01.004>
 - [22] Alem, S., Espes, D. et al. (2019). A Hybrid Intrusion Detection System in Industry 4.0 Based on ISA95 Standard. *2019 IEEE/ACS 16th Int. Conf. on Comp. Syst and Appl. (AICCSA)*, pp. 1–8. <https://doi.org/10.1109/AICCSA47632.2019.9035260>
 - [23] Tuptuk, N., Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, Vol. 47, pp. 93–106. <https://doi.org/10.1016/j.jmsy.2018.04.007>
 - [24] Rubio, J. E., Roman, R. and Lopez, J. (2018). Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection. *The 12th Int. Conf. on Critical Information Infrastructures Security vol. Lecture Notes in Computer Science*, 10707, pp. 119–130. https://doi.org/10.1007/978-3-319-99843-5_11
 - [25] Khan, I. A., Pi, D. et al. (2019). HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems. *IEEE Access*, Vol. 7, pp. 89507–89521
 - [26] Hady, A. A., Ghubaish, A. et al. (2020). IDS for Healthcare Systems Using Medical and Network Data: A Comparison Study. *IEEE Access*, Vol. 8, pp. 106576–106584.
 - [27] Saif, S., Das, P. et al. (2022). HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. *Microprocessors and Microsystems*, p. 104622.
 - [28] Maktoubian, J. & Ansari, K. (2019). An IoT Architecture for Preventive Maintenance of Medical Devices in Healthcare Organizations. *Health and Technology*, Vol. 9, pp. 233–243.

-
- [29] Iantovics, L. B., Crainicu, B. (2014). A Distributed Security Approach for Intelligent Mobile Multiagent Systems. In: Iantovics, L. B., et al. (eds.). *Advanced Intelligent Computational Technologies and Decision Support Systems*. Studies in Comp. Int. (series), pp. 175–189.
 - [30] Crainicu, B., Iantovics, B. (2008). Securing WEP Cryptosystems through A New RC4 Key Scheduling Algorithm. In: Iantovics, L. B. et al. (eds.). *Complexity in Artificial and Natural Systems*. “Petru Maior” University Publishing House, pp. 93–99.
 - [31] Snehi, M., Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. *Computer Science Review*, Vol. 40, p. 100371.
<https://doi.org/10.1016/j.cosrev.2021.100371>