PARADIGMA, No.2, 2026, səh.145-149
https://doi.org/10.30546/30015.2026.001.02.382

KİBERTƏHLÜKƏSİZLİKDƏ SÜNİ İNTELLEKT YANAŞMALARI: HETEROJEN TEMPORAL QRAFLAR ÜZƏRİNDƏ GNN ƏSASLI APT AŞKARLANMASI

N.Ə. Həsənova, A.N. Əlifov
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: Nazly.Hasanova@au.edu.az, Aykhan.Alifov@student.au.edu.az

Xülasə: Müasir şəbəkə infrastrukturlarında qabaqcıl davamlı təhdidlərin (APT) aşkarlanması ənənəvi kibertəhlükəsizlik alətlərinin imkanlarını aşan mürəkkəb bir problem kimi özünü göstərməkdədir. Bu işdə sistem hadisələrini heterojen temporal qraf kimi modelləşdirən və Graph Neural Networks (GNN) əsaslı klassifikasiya aparan yeni bir aşkarlama yanaşması təqdim edilir.

Açar sözlər: neyron şəbəkəsi qrafı, APT aşkarlanması, heterogen qraf, temporal analiz, lateral hərəkət, provenance qraf, kibertəhlükəsizlik

Texnologiyaların getdikcə daha mürəkkəbləşdiyi və kibertəhdidlərin getdikcə daha da inkişaf etdiyi bugünkü rəqəmsal dünyada süni intellektin kibertəhlükəsizliyin təmin edilməsindəki rolu əsas məsələyə çevrilir. Süni intellekt kibertəhlükəsizlik sahəsində təkcə təhdidləri aşkarlamaq və qarşısını almaq üçün deyil, həm də onlara effektiv şəkildə cavab vermək üçün tətbiq olunur. Əhəmiyyətli aspektlərdən biri də süni intellektdən istifadə edərək kibertəhlükəsizliyin avtomatlaşdırılmasıdır. Maşın öyrənmə alqoritmləri sistemlərə böyük həcmdə məlumatları avtomatik olaraq təhlil etməyə, anomaliyaları müəyyən etməyə və potensial kiberhücumları proqnozlaşdırmağa imkan verir. Bu, cavab sürətini artırır və təhdidlərin zərər verməzdən əvvəl qarşısını almağa imkan verir. Maşın öyrənmə texnologiyaları həmçinin yeni növ təhdidlərə uyğunlaşa bilən ağıllı sistemlərin yaradılmasına töhfə verir. Süni intellektlə təchiz olunmuş sistemlər yeni məlumatlardan öyrənə və zamanla effektivliyini artıra bilər. Bu, getdikcə daha mürəkkəb və hiyləger kiberhücumlar kontekstində xüsusilə vacibdir. Bu cür sistemlər məlumatları real vaxt rejimində emal edə, qeyri-adi istifadəçi davranışlarını aşkarlaya, şəbəkə trafikini təhlil edə və gizli təhdidləri aşkarlaya bilər. Lakin, kibertəhlükəsizliyin artırılması ilə yanaşı, süni intellekt daha mürəkkəb kiberhücumlar yaratmaq üçün bir vasitəyə də çevrilə bilər. Hücumçular ağıllı və aşkarlanması çətin olan təhdidlər yaratmaq üçün maşın öyrənmə texnologiyalarından istifadə edə bilərlər. Bu, kibertəhlükəsizlik metodlarını daim təkmilləşdirmək və yeni çağırışlara uyğunlaşmaq ehtiyacını vurğulayır. Məxfilik, qərar qəbuletmə məsuliyyəti və bu sahədə standartların və tənzimləmələrin yaradılması məsələləri getdikcə daha aktuallaşır.

Kibertəhdid mənzərəsinin sürətlə mürəkkəbləşdiyi bir dövrdə Qabaqcıl Davamlı Təhdidlər - APT (Advanced Persistent Threat) ən ciddi təhlükəsizlik problemlərindən birinə çevrilmişdir. APT hücumları konkret hədəflərə qarşı yönəlmiş, çoxmərhələli, uzunmüddətli, gizli kampaniyalardır. 2020-ci ildəki SolarWinds insidensi 18000 müştərinin sistemini kompromit etdi, hücum 8-9 ay aşkar olunmadan qaldı [1]. Bu tip hücumları mövcud alətlərlə aşkarlamaq son dərəcə çətindir: imza əsaslı IDS-lər yalnız məlum hücumları tanıyır; anomaliya əsaslı sistemlər yüksək yanlış müsbət dərəcəsi yaradır; SIEM platformaları isə uzunmüddətli zaman ardıcıllıqlarını korrelyasiya etmək üçün kifayət deyil.

Qraf nəzəriyyəsi bu problemi fərqli bir prizmadan həll etməyə imkan verir. Sistem hadisələri qraf kimi modelləşdirildikdə host, istifadəçi, proses, fayl, IP ünvanı node-lar, onlar arasındakı əməliyyatlar edge-lər olaraq APT hücumu qrafda yeni bir subqraf kimi özünü göstərir. Graph Neural Networks (GNN) qraf üzərindəki struktural nümunələri - qonşuluq məlumatlarını, zaman ardıcıllığını, node xüsusiyyətlərini eyni zamanda öyrənə bilən dərin öyrənmə texnologiyasıdır.

APT Hücumlarının Qraf Modeli. APT hücumlarının ənənəvi metodlarla aşkarlanmasının çətinliyi onların statistik anomaliya yaratmamasından qaynaqlanır. Hücumçu öz fəaliyyətini normal günlük aktivliyin içində əridir - iş saatlarında, tanınan protokollar vasitəsilə, kiçik məlumat həcmlərilə fəaliyyət göstərir. Fərdi baxıldıqda hər bir hadisə tamamilə legitimdir. Anomaliya yalnız hadisələrin ardıcıllığı və aralarındakı struktural əlaqə kontekstində aşkar olur.

Sistem hadisələrini qraf kimi modelləşdirmək bu problemi həll etmək üçün ideal bir çərçivə yaradır. G = (V, E, T) temporal heterogen qrafında V node-lar çoxluğu (host, user, process, file, ip_addr tiplərində entity-lər), E edge-lər çoxluğu (auth, spawn, file_op, net_connect, registry_op tipində əlaqələr), T isə zaman damğaları çoxluğunu ifadə edir. Normal iş rejimində qraf G_normal müəyyən bir struktural sabitliyə malikdir. APT kampaniyası başlayanda G_apt = G_normal ∪ S_attack formalaşır - burada S_attack hücuma aid yeni subqraf komponentidir [2]. Aşkarlama problemi məhz bu S_attack-ı böyük G içərisindən tapmaqla nəticələnir.

Lateral hərəkət bu qraf modelinin ən güclü tərəfini üzə çıxarır. RDP, PsExec, WMI, pass-the-hash kimi texnikalarla icra olunan hər bir hərəkət qrafda yeni edge-lər və əvvəllər görülməmiş node-node əlaqə konfiqurasiyaları yaradır. Bu struktural dəyişiklikləri GNN-in mesaj ötürmə mexanizmi çox effektiv şəkildə, imza ya da statistik eşik olmadan, aşkarlayır [3].

GNN Modelinin Arxitekturası. Sistemin pipeline-ı beş əsas komponentdən ibarətdir: məlumat toplama; qrafın qurulması; feature engineering; GNN çıxarımı; klassifikasiya.

Məlumat toplama səviyyəsində Windows endpoint-lər üçün Sysmon, şəbəkə trafiki üçün Zeek, Linux sistemlər üçün Auditd agentlərindən istifadə olunur. Bütün məlumatlar Apache Kafka vasitəsilə toplanır, Apache Flink stream engine-i ilə real vaxtda prosess edilir.

Qraf qurulması zamanı sliding window strategiyası tətbiq olunur: W=10 dəqiqəlik pəncərə, S=2 dəqiqəlik addım ilə ardıcıl snapshot-lar $G_t = (V_t, E_t, X_t)$ yaradılır. Feature engineering üç kateqoriya üzrə aparılır: struktural xüsusiyyətlər (degree, betweenness centrality, clustering coefficient); temporal xüsusiyyətlər (aktivlik tezliyi, burst skoru, gecə fəaliyyəti nisbəti); semantik xüsusiyyətlər (node tipi, risk skoru, reputasiya).

Model arxitekturası: Type-specific Projection Layer → 2× Heterojen Attention GNN Layer → Temporal LSTM → Attention Pooling → Softmax Klassifikasiya. Heterogen Attention GNN səviyyəsi hər edge tipi üçün ayrıca attention coefficient hesablayır: $\alpha_{ij}^{\tau} = \exp(e_{ij}^{\tau}) / \Sigma_{k \in N^{\tau}(i)} \exp(e_{ik}^{\tau})$, burada $e_{ij}^{\tau} = \text{LeakyReLU}(a^{\tau T} \cdot [W^{\tau} h_i \| W^{\tau} h_j \| e\_feat])$. Semantik aggregation β^{τ} qatlamalı son node embedding $h_i^{final} = \Sigma_{\tau} \beta^{\tau} \cdot h_i^{(\tau)}$ formalaşdırır. LSTM qatı ardıcıl snapshot-ların temporal kontekstini qoruyur [4].

Loss funksiyası üç komponentdən ibarətdir: $L = 0.7 \cdot L_{cls} + 0.2 \cdot L_{con} + 0.1 \cdot L_{reg}$. Sinif tarazısızlığını kompensasiya etmək üçün hücum sinfinə $w_{attack}=3.2$ çəki əmsalı tətbiq edilir. Optimizer: Adam (lr=0.001), ReduceLROnPlateau scheduling, early stopping (patience=10).

Eksperimental Qiymətləndirmə. Eksperimentlər üç dataset üzərində aparılmışdır. DARPA OPTC (2019): 1.3 milyard sistem hadisəsi, 47 APT kampaniya ssenarisi, tam etiketlənmiş. LANL Unified Dataset: 58 günlük 1.648 milyard autentifikasiya hadisəsi, 17684 istifadəçi. MITRE ATT&CK v13 əsaslı sintetik dataset: 250,000 normal + 35,000 hücum hadisəsi. Temporal 60/20/20 bölgüsü istifadə edilmişdir.

Müqayisə aparılan baseline-lar: Random Forest (feature əsaslı), Isolation Forest (statistik anomaliya), SVM RBF kernel, DeepLog (LSTM, log ardıcıllığı), Signature-based IDS (SNORT). Qiymətləndirmə metrikaları: Precision, Recall, F1-score, ROC-AUC, False Positive Rate (FPR), Detection Latency.

Test seti (8,000 hadisə: 4,915 normal, 3,085 hücum) üzərindəki nəticələr əsasında demək olar ki, modelimiz F1=0.9768, ROC-AUC=0.9847, FPR=2.26% nəticəsi ilə bütün baseline-lardan üstündür. Random Forest ilə müqayisədə yanlış xəbərdarlıqlar 3.1× az (95 vs 292), buraxılan hücumlar isə 5.3× azdır (72 vs 381). Ablation study göstərir ki, temporal layer-in çıxarılması F1-i −4.7%, heterogen strukturun çıxarılması isə −5.8% azaldır [5].

Aşkarlama vaxtı analizi ən vacib nəticəni ortaya qoyur: Lateral Movement mərhələsini model orta 1.2 saat ərzində aşkarlayır, ənənəvi SIEM isə 9.4 saat tələb edir - 7.8× üstünlük. Reconnaissance üçün 4.5×, Persistence üçün 5.9×, Exfiltration üçün 7.6× üstünlük müşahidə edilmişdir. Scalability testində 500000 node-lu qrafda GNN 124.3 saniyə, SIEM isə 1,205 saniyə tələb edir (9.7× sürətli).

Nəticə və Perspektivlər. Şəbəkə infrastrukturlarında APT hücumlarının aşkarlanması üçün GNN əsaslı yeni yanaşma təklif edilmiş, DARPA OPTC, LANL və sintetik datasetlər üzərində eksperimental şəkildə qiymətləndirilmişdir. Modelin əsas töhfələri: (1) APT-ni heterogen temporal qraf problemi kimi formalaşdırmaq; (2) node tipi xas attention və temporal LSTM-i birləşdirən hibrid arxitektura; (3) ənənəvi metodlarla müqayisədə F1-scoreda +6.97%, lateral hərəkət aşkarlanmasında 7.8× sürət üstünlüyü.

Gələcək tədqiqat istiqamətləri arasında şifrəli trafik analizi (TLS/SSL metadatası əsaslı), Federated Learning (məlumat paylaşmadan çox-müəssisəli model öyrənməsi) və LLM+GNN hibrid arxitekturanın araşdırılması ön plana çıxır. Produksiya mühitinə tətbiq üçün FP16 quantization (F1 yalnız −0.17% azalır), Knowledge Distillation (inference 2.6× sürətlənir) kimi optimallaşdırma texnikaları tövsiyə olunur. IBM-in 2023 hesabatına görə, APT sisteminin tətbiqi 343% ROI, 2.1 aylıq break-even nöqtəsi ilə güclü maliyyə əsaslandırılmasına malikdir [6]. Təklif olunan model DARPA OPTC datasetində F1=0.9768, ROC-AUC=0.9847 nəticə göstərmiş, lateral hərəkəti ənənəvi SIEM sistemlərindən 7.8× daha tez aşkarlamışdır. Nəticələr GNN-in APT aşkarlanmasında imza əsaslı və statistik anomaliya metodlarına effektiv alternativ olduğunu sübut edir.

Ədəbiyyat siyahısı

1. FireEye Mandiant. (2021). M-Trends 2021: A View From the Front Lines. Mandiant, Inc.
2. Milajerdi, S. M., Gjomemo, R., Eshete, B., Sekar, R., & Venkatakrishnan, V. N. (2019). HOLMES: Real-time APT detection through correlation of suspicious information flows. IEEE Symposium on Security and Privacy (S&P 2019), pp. 1026–1043.
3. Han, X., Pasquier, T., Bates, A., Mickens, J., & Seltzer, M. (2020). Unicorn: Runtime provenance-based detector for advanced persistent threats. NDSS 2020.
4. Kipf, T. N., & Welling, M. (2017). Semi-supervised classification with graph convolutional networks. ICLR 2017. arXiv:1609.02907.
5. Ying, Z., Bourgeois, D., You, J., Zitnik, M., & Leskovec, J. (2019). GNNExplainer: Generating explanations for graph neural networks. NeurIPS 2019, vol. 32.
6. IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

ARTIFICIAL INTELLIGENCE APPROACHES IN CYBERSECURITY: GNN-BASED APT DETECTION ON HETEROGENEOUS TEMPORAL GRAPHS

N.A. Hasanova, A.N. Alifov
Azerbaijan University, Jeyhun Hajibeyli, 71, Baku, Azerbaijan

Abstract. The detection of Advanced Persistent Threats (APT) in modern network infrastructures has emerged as a complex problem that exceeds the capabilities of traditional cybersecurity tools. This study presents a novel detection approach that models system events as a heterogeneous temporal graph and performs classification based on Graph Neural Networks (GNN).

Keywords: Graph neural network, APT detection, heterogeneous graph, temporal analysis, lateral movement, provenance graph, cybersecurity.