مدل :MAGNET رویکردی ترکیبی مبتنی بر یادگیری عمیق برای تشخیص بدافزار اندروید با استفاده از ویژگی‌های چندگانه

علیرضا ایرانمنش* **دکتر حمید میروزیری†**

۲ تیر ۱۴۰۴

چکیده

چکیده

زمینه و هدف: با گسترش روزافزون استفاده از دستگاه‌های اندرویدی و افزایش حجم تهدیدات سایبری، تشخیص دقیق و به‌موقع بدافزارها به یکی از چالش‌های حیاتی امنیت اطلاعات تبدیل شده است. روش‌های سنتی تشخیص بدافزار که عمدتاً بر تحلیل تک‌وجهی متکی‌اند، در مواجهه با بدافزارهای پیچیده و تکنیک‌های مبهم‌سازی پیشرفته کارایی محدودی نشان می‌دهند. **روش:** این پژوهش مدل نوین چندوجهی MAGNET (Multi-modal Analysis for Graph-based NEtwork Threats) را معرفی می‌کند که با ترکیب هوشمندانه سه نوع داده—جدولی (ویژگی‌های ایستا)، گرافی (گراف‌های فراخوانی توابع)، و ترتیبی (توالی‌های فراخوانی API)—و بهره‌گیری از معماری‌های پیشرفته یادگیری عمیق شامل ترنسفورمرها و شبکه‌های عصبی گراف، دقت تشخیص بدافزار را بهبود می‌بخشد. مدل پیشنهادی شامل سه ماژول تخصصی EnhancedTabTransformer، GraphTransformer، و SequenceTransformer به همراه مکانیزم توجه پویا و لایه ادغام چندوجهی است. **یافته‌ها:** ارزیابی‌های تجربی بر روی مجموعه داده استاندارد DREBIN شامل 6,092 نمونه (4,641 برای آموزش و 1,451 برای تست) نشان می‌دهد که مدل MAGNET با دقت 0.65±97.24% معیار F1-Score برابر 0.0042±0.9823، و AUC برابر 0.0035±0.9932، عملکردی برتر نسبت به روش‌های مرجع از جمله SVM (90.6%)، Random Forest (93.5%)، XGBoost (94.8%)، و ANN (96.2%) ارائه می‌دهد. مطالعه ablation نشان می‌دهد که حذف هر یک از اجزای مدل منجر به کاهش قابل‌توجه عملکرد می‌شود. **نتیجه‌گیری:** نتایج تأیید می‌کند که رویکرد چندوجهی و استفاده از معماری‌های نوین یادگیری عمیق، پتانسیل قابل‌توجهی در مقابله با تهدیدات پیچیده و نوظهور اندرویدی دارد و می‌تواند به عنوان راه‌حلی مؤثر در سیستم‌های امنیتی عملیاتی مورد استفاده قرار گیرد.

واژگان کلیدی: تشخیص بدافزار اندروید، یادگیری چندوجهی، شبکه‌های عصبی گراف، ترنسفورمر، تحلیل امنیتی، DREBIN، MAGNET

*دانشگاه شهید باهنر، دانشکده مهندسی کامپیوتر، کرمان، ایران. ایمیل: alirezairanmanesh78@gmail.com
†دانشگاه شهید باهنر، دانشکده مهندسی کامپیوتر، باهنر، ایران. ایمیل: h.mirvaziri@gmail.com

MAGNET: A Hybrid Deep Learning Approach for Android Malware Detection Using Multi-feature Analysis

Abstract

Background: With the increasing prevalence of Android devices and cybersecurity threats, accurate malware detection has become crucial. Traditional single-modal approaches show limitations against sophisticated malware. Method: This research introduces MAGNET (Multi-modal Analysis for Graph-based NEtwork Threats), integrating three data modalities—tabular (static features), graph (function call graphs), and sequential (API sequences)—through specialized neural architectures (EnhancedTabTransformer, GraphTransformer, and SequenceTransformer) with dynamic attention and multimodal fusion. Results: Evaluation on the DREBIN dataset (6,092 samples) shows MAGNET achieves 97.24±0.65% accuracy, 0.9823±0.0042 F1-Score, and 0.9932±0.0035 AUC, outperforming baselines (SVM: 90.6%, Random Forest: 93.5%, XGBoost: 94.8%, ANN: 96.2%). Ablation studies confirm each component's significance. Conclusion: The multi-modal approach demonstrates strong potential for operational security systems against emerging Android threats.

Keywords: Android malware detection, Multimodal deep learning, Graph neural networks, Transformer architecture, Security analysis, DREBIN dataset, MAGNET

۱ مقدمه

سیستم‌عامل اندروید با بیش از 70% سهم بازار جهانی دستگاه‌های هوشمند، به بزرگ‌ترین پلتفرم موبایل جهان تبدیل شده است. این محبوبیت گسترده، همراه با معماری باز و انعطاف‌پذیر اندروید، آن را به هدف اصلی حملات سایبری تبدیل کرده است. گزارش‌های امنیتی نشان می‌دهند که تعداد بدافزارهای شناسایی‌شده برای پلتفرم اندروید از 3.2 میلیون نمونه در سال 2020 به بیش از 5.8 میلیون نمونه در سال 2023 افزایش یافته است [۱].

روش‌های سنتی تشخیص بدافزار که عمدتاً بر امضاهای ایستا و تحلیل تک‌بعدی متکی هستند، در مواجهه با تکنیک‌های پیچیده مبهم‌سازی، رمزگذاری، و پیکربندی پویای کد دچار محدودیت‌های جدی می‌شوند [۲]. علاوه بر این، ظهور بدافزارهای تولیدشده با هوش مصنوعی و تکنیک‌های تطبیقی، چالش‌های جدیدی را برای سیستم‌های امنیتی ایجاد کرده است.

این پژوهش با هدف مقابله با این چالش‌ها، مدل نوآورانه MAGNET (Multi-modal Analysis for Graph-based NEt-work Threats) را معرفی می‌کند. این مدل با بهره‌گیری از رویکرد چندوجهی، سه نوع داده مختلف شامل ویژگی‌های جدولی (مجوزها، اجزای برنامه)، ساختارهای گرافی (گراف‌های فراخوانی توابع)، و توالی‌های زمانی (API کال‌ها) را به‌صورت هم‌زمان تحلیل می‌کند.

نوآوری‌های کلیدی این پژوهش عبارتند از:

- طراحی معماری چندوجهی یکپارچه با سه ماژول تخصصی
- توسعه مکانیزم توجه پویا برای ادغام بهینه اطلاعات چندوجهی
- پیاده‌سازی الگوریتم بهینه‌سازی PIRATES برای تنظیم خودکار پارامترها
- ارزیابی جامع بر روی مجموعه داده استاندارد DREBIN

۲ کارهای مرتبط

۱.۲ تکامل روش‌های تشخیص بدافزار اندروید

تحقیقات اولیه در زمینه تشخیص بدافزار اندروید عمدتاً بر تحلیل ایستا متمرکز بودند. Arp و همکاران [۳] با معرفی سیستم DREBIN، یکی از تأثیرگذارترین کارهای این حوزه را ارائه دادند. آن‌ها از ویژگی‌هایی نظیر مجوزها، فراخوانی‌های API، اجزای برنامه، و فیلترهای Intent استفاده کردند و با بهره‌گیری از الگوریتم SVM، دقت 94% در تشخیص بدافزار حاصل کردند.

Schmidt و همکاران [۴] چارچوبی جامع برای تحلیل ایستا برنامه‌های اندرویدی طراحی کردند که شامل استخراج اطلاعات از فایل AndroidManifest.xml، تحلیل کد DEX، و بررسی منابع برنامه بود. این چارچوب قابلیت تشخیص 87.3% از بدافزارهای مجموعه‌آزمایش را داشت اما در مواجهه با تکنیک‌های مبهم‌سازی کارایی چندانی نداشت.

۲.۲ رویکردهای مبتنی بر یادگیری عمیق

با پیشرفت‌های اخیر در یادگیری عمیق، محققان شروع به استفاده از شبکه‌های عصبی پیچیده برای تشخیص بدافزار کردند. Kim و همکاران [۵] اولین کار مهم در استفاده از Deep Belief Networks (DBN) برای تحلیل بدافزار اندروید را ارائه دادند. آن‌ها با استفاده از ویژگی‌های API و دستیابی به دقت 96.5%، کارایی بالای روش‌های یادگیری عمیق را نشان دادند.

Wang و همکاران [۶] سیستم DroidDeepLearner را توسعه دادند که از Deep Belief Networks برای تحلیل ویژگی‌های ایستا و پویا استفاده می‌کرد. این سیستم توانست دقت 97.8% در تشخیص بدافزارهای خانواده‌های مختلف کسب کند.

۳.۲ تحلیل چندوجهی

Alzaylaee و همکاران [۷] یکی از اولین تلاش‌های جامع برای استفاده از داده‌های چندوجهی در تشخیص بدافزار اندروید را ارائه دادند. آن‌ها از ترکیب ویژگی‌های ایستا، پویا، و متنی استفاده کردند و با بهره‌گیری از روش‌های ادغام مختلف، دقت 98.2% حاصل کردند.

Chen و همکاران [۸] رویکرد جدیدی مبتنی بر تحلیل گراف چندوجهی ارائه دادند که از Graph Neural Networks (GNN) برای یادگیری نمایش‌های پیچیده از ساختار برنامه‌ها استفاده می‌کرد. این روش با دقت 96.7% نتایج امیدوارکننده‌ای نشان داد.

۳ روش پیشنهادی

۱.۳ معماری کلی مدل MAGNET

مدل MAGNET یک معماری چندوجهی یکپارچه است که از سه جریان داده مجزا برای پردازش انواع مختلف اطلاعات استفاده می‌کند. هر جریان توسط یک ماژول تخصصی پردازش می‌شود و در نهایت، خروجی‌ها از طریق یک مکانیزم توجه پویا ادغام می‌شوند.

ماژول ویژگی‌های جدولی - EnhancedTabTrans former): این ماژول برای پردازش ویژگی‌های ایستا طراحی شده است. ویژگی‌های ورودی شامل:

- مجوزهای درخواست‌شده توسط برنامه (128 ویژگی)
- اجزای برنامه مانند Activities، Services، و Receivers
- فراخوانی‌های API ایستا
- اطلاعات AndroidManifest.xml

ماژول ساختار گراف (GraphTransformer): این ماژول برای تحلیل گراف‌های فراخوانی توابع طراحی شده است. گراف‌های ورودی دارای مشخصات زیر هستند:

- میانگین 1,245 گره و 3,872 یال در هر نمونه
- ویژگی‌های گره: نوع تابع، فراوانی فراخوانی (64 بعد)
- ویژگی‌های یال: فراوانی و نوع فراخوانی (32 بعد)

ماژول توالی‌های API (SequenceTransformer): این ماژول برای تحلیل توالی‌های فراخوانی API طراحی شده است:

- میانگین طول 87 فراخوانی API در هر نمونه
- رمزگذاری توالی‌ها با استفاده از Word2Vec
- حفظ اطلاعات ترتیب زمانی فراخوانی‌ها

۲.۳ جزئیات پیاده‌سازی

مکانیزم توجه پویا: برای ادغام اطلاعات سه ماژول، مکانیزم توجه پویای زیر طراحی شده است:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (۱)$$

که در آن Q، K، و V به ترتیب ماتریس‌های Query، Key، و Value هستند.

لایه ادغام چندوجهی: خروجی نهایی از طریق ترکیب وزنی خروجی‌های سه ماژول محاسبه می‌شود:

$$\text{Output} = \alpha \cdot h_{\text{tab}} + \beta \cdot h_{\text{graph}} + \gamma \cdot h_{\text{seq}} \quad (۲)$$

که وزن‌های α، β، و γ به صورت تطبیقی یاد گرفته می‌شوند.

۴ پیاده‌سازی و ارزیابی

۱.۴ مجموعه داده

برای ارزیابی مدل MAGNET از مجموعه داده استاندارد DREBIN [۹] استفاده شد که شامل 6,092 نمونه است:

- **lu آموزش:** 4,641 نمونه
- **تست:** 1,451 نمونه (327 نمونه سالم، 1,124 نمونه بدافزار)
- **دوره زمانی:** 2010-2014
- **خانواده‌های بدافزار:** شامل انواع مختلف بدافزار

۲.۴ تنظیمات آزمایش

سخت‌افزار:

- CPU: Intel Core i7-8700K
- GPU: NVIDIA RTX 3080 (۱۰GB VRAM)
- RAM: 32GB DDR4-3200
- Storage: 256GB NVMe SSD

نرم‌افزار:

- Python 3.8.10
- PyTorch 1.12.0
- PyTorch Geometric 2.1.0
- CUDA 11.6

بهینه‌سازی پارامترها: بهینه‌سازی ابرپارامترها با دو روش انجام شد:

- **بهینه‌سازی دستی:** الگوریتم PIRATES با 476 آزمایش
- **بهینه‌سازی Optuna:** 13 آزمایش هدفمند

۵ نتایج

۱.۵ عملکرد کلی

مدل MAGNET در ارزیابی بر روی مجموعه تست شامل 1,451 نمونه به نتایج زیر دست یافت:

- **دقت:** 97.24%
- **F1-Score:** 0.9823
- **Precision:** 0.9796
- **Recall:** 0.9849
- **AUC:** 0.9932

۲.۵ نتایج اعتبارسنجی متقاطع

در اعتبارسنجی متقاطع 5ـتایی، میانگین معیارها به صورت زیر به‌دست آمد:

۳.۵ مقایسه با روش‌های مرجع

۴.۵ تحلیل عملکرد ماژول‌ها

عملکرد تک‌تک ماژول‌های مدل MAGNET بر اساس نتایج پایان‌نامه:

- F1-Score = 0.945 EnhancedTabTransformer
- ۸۹۴.۰ = F1-Score GraphTransformer
- ۹۰۷.۰ = F1-Score SequenceTransformer
- **مدل ترکیبی:** F1-Score = 0.982

۵.۵ مطالعه حذف اجزا (Ablation Study)

بر اساس مطالعه حذف اجزا انجام‌شده در پایان‌نامه:

- **بدون مکانیزم توجه پویا:** F1-Score = 0.954
- **بدون لایه ادغام چندوجهی:** F1-Score = 0.967
- **مدل کامل MAGNET** F1-Score = 0.982

۶.۵ ماتریس درهم‌ریختگی

نتایج تست نهایی بر روی 1,451 نمونه تست:

- **درست منفی (TN):** 304 نمونه
- **نادرست مثبت (FP):** 23 نمونه
- **نادرست منفی (FN):** 17 نمونه
- **درست مثبت (TP):** 1,107 نمونه

۷.۵ مقایسه با روش‌های پیشرفته

۶ بحث و تحلیل

۱.۶ تحلیل نتایج

نتایج به‌دست آمده نشان می‌دهد که مدل MAGNET با دقت 97.24% و F1-Score برابر 0.9823 عملکرد برتری نسبت به روش‌های مرجع و حتی بسیاری از روش‌های پیشرفته دارد. این بهبود عملکرد را می‌توان به عوامل زیر نسبت داد: **تنوع اطلاعات:** استفاده از سه نوع داده مختلف (جدولی، گرافی، ترتیبی) اطلاعات جامع‌تری از ساختار و رفتار برنامه‌ها فراهم می‌کند. **معماری پیشرفته:** استفاده از ترنسفورمرهای تخصصی امکان استخراج

جدول ۱: نتایج اعتبارسنجی متقاطع 5ـتایی مدل MAGNET

معیار	مقدار
دقت	0.9722 ± 0.0065
Precision	0.9810 ± 0.0102
Recall	0.9828 ± 0.0072
F1-Score	0.9818 ± 0.0042
AUC	0.9932 ± 0.0035

جدول ۲: مقایسه عملکرد مدل MAGNET با روش‌های مرجع

روش	دقت	F1-Priceision	Recall	F1-Score	AUC
SVM	0.906	0.915	0.892	0.903	0.945
Random Forest	0.935	0.942	0.928	0.935	0.967
XGBoost	0.948	0.953	0.943	0.948	0.978
ANN	0.962	0.965	0.959	0.962	0.985
MAGNET	0.972	**۹۸۰۰**	0.985	0.982	0.993

جدول ۳: مقایسه با روش‌های پیشرفته

روش	دقت (%)	F1-Score	AUC	یادداشت
MAGNET	97.24	0.9823	0.9932	بهترین عملکرد، DREBIN
(SVM) DREBIN	92.3	0.933	0.955	رویکرد ایستا
PIKADROID	96.8	0.974	0.988	تحلیل API، DREBIN
CrossMalDroid	95.2	0.952	0.976	انتخاب ویژگی، Malgenome
DroidAPIMiner	89.7	0.891	0.927	فرکانس API، DREBIN
DeepImageDroid	96.0	0.960	0.982	ترنسفورمر بصری و CNN
BERT-Graph	95.5	0.950	0.975	BERT و گراف API

الگوهای پیچیده را فراهم می‌کند. **مکانیزم توجه پویا:** این مکانیزم امکان تمرکز بر اطلاعات مهم و نادیده گرفتن اطلاعات نامربوط را فراهم می‌کند.

۲.۶ مقایسه با کارهای پیشین

در مقایسه با کارهای پیشین:

- DREBIN **اصلی:** دقت 94% - بهبود 3.24%
- **روش‌های چندوجهی قبلی:** دقت حدود 96-89% - بهبود قابل‌توجه
- **روش‌های مبتنی بر** GNN**:** دقت حدود 97-95% - رقابتی یا بهتر

۳.۶ محدودیت‌ها

علی‌رغم نتایج مثبت، مدل MAGNET دارای محدودیت‌هایی است: **پیچیدگی محاسباتی:** پردازش سه نوع داده مختلف نیازمند منابع قابل‌توجه است. **وابستگی به کیفیت داده:** عملکرد مدل به کیفیت استخراج ویژگی و پیش‌پردازش داده‌ها وابسته است. **تعمیم‌پذیری:** آموزش بر روی مجموعه داده DREBIN که مربوط به سال‌های 2014-2010 است، ممکن است تعمیم‌پذیری مدل را محدود کند.

۷ نتیجه‌گیری

این پژوهش مدل نوآورانه MAGNET را برای تشخیص بدافزار اندروید معرفی کرد که از رویکرد چندوجهی و معماری‌های پیشرفته استفاده می‌کند. نتایج ارزیابی بر روی مجموعه داده DREBIN نشان می‌دهد که با دقت 97.24% و F1-Score برابر 0.9823 عملکرد برتری نسبت به روش‌ها دارد.

دستاوردهای کلیدی عبارتند از:

- طراحی معماری چندوجهی یکپارچه با سه ماژول تخصصی شامل EnhancedTabTransformer، GraphTransformer، و SequenceTransformer
- توسعه مکانیزم توجه پویا برای ادغام بهینه اطلاعات با وزن‌های تطبیقی
- نشان دادن اهمیت استفاده از اطلاعات متنوع شامل ویژگی‌های جدولی، گرافی و ترتیبی
- ارائه راه‌حلی عملی برای سیستم‌های امنیتی با دقت بالا و نرخ خطای پایین
- استفاده موثر از از الگوریتم بهینه‌سازی PIRATES برای تنظیم خودکار

مطالعه حذف اجزا تأیید کرد که هر ماژول نقش مهمی دارد و حذف آن‌ها منجر به کاهش دقت می‌شود. ماتریس درهم‌ریختگی نشان داد توانایی در تفکیک صحیح نمونه‌های مخرب و سالم دارد.

۸ پیشنهادات آتی

۱.۸ بهبودهای فنی

- ارزیابی مدل بر روی مجموعه داده‌های جدیدتر و متنوع‌تر شامل بدافزارهای سال‌های اخیر
- بهینه‌سازی معماری برای کاهش پیچیدگی محاسباتی و افزایش سرعت پردازش
- توسعه تکنیک‌های فشرده‌سازی مدل برای اجرا بر روی دستگاه‌های با منابع محدود
- پیاده‌سازی یادگیری انتقالی برای تطبیق سریع با انواع جدید بدافزار

۲.۸ کاربردهای عملی

- بررسی قابلیت اعمال مدل در محیط‌های عملیاتی و سیستم‌های تولیدی
- توسعه رابط کاربری برای استفاده آسان توسط متخصصان امنیت
- ادغام مدل با سیستم‌های موجود آنتی‌ویروس و امنیتی

- بررسی عملکرد مدل در تشخیص *real-time* بدافزارها

۳.۸ تحقیقات آینده

- توسعه روش‌های تفسیرپذیری برای درک بهتر فرآیند تصمیم‌گیری مدل
- بررسی مقاومت مدل در برابر حملات تضاد و تکنیک‌های فرار پیشرفته
- توسعه مدل‌های تطبیقی که بتوانند با تکامل بدافزارها به‌روزرسانی شوند
- بررسی کاربرد مدل برای تشخیص انواع دیگر نرم‌افزارهای مخرب در پلتفرم‌های مختلف

مراجع

[1] AV-TEST. “Mobile Malware Report 2023”. In: AV-TEST Security Report (2023). URL: https://www.av-test.org/en/statistics/malware/.

[2] Wei Li et al. “Limitations of Signature-Based Anti-Malware Systems”. In: Communications of the ACM 58.7 (2015), pp. 70–77. DOI: 10.1145/2757269.

[3] Daniel Arp et al. “Drebin: Efficient and Explainable Detection of Android Malware in Your Pocket”. In: Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS). 2014. DOI: 10.14722/ndss.2014.23247.

[4] Andreas-Dirk Schmidt et al. “Static Analysis Framework for Android Applications”. In: Information Security Technical Report 14.2 (2009), pp. 100–104. DOI: 10.1016/j.istr.2009.06.003.

[5] Taeguen Kim et al. “Deep Learning for Android Malware Detection”. In: Expert Systems with Applications 89 (2017), pp. 328–344. DOI: 10.1016/j.eswa.2017.07.046.

[6] Wei Wang et al. “DroidDeepLearner: Identifying Android Malware Using Deep Learning”. In: Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (2017), pp. 160–169. DOI: 10.1109/ICDCS.2017.211.

[7] Mohammed K. Alzaylaee, Suleiman Y. Yerima, and Sakir Sezer. “Multimodal Deep Learning for Android Malware Detection”. In: Journal of Information Security and Applications 40 (2018), pp. 61–75. DOI: 10.1016/j.jisa.2018.03.003.

[8] Li Chen et al. “Multi-modal Graph Learning for Android Malware Detection”. In: Computers & Security 106 (2021), p. 102283. DOI: 10.1016/j.cose.2021.102283.

[9] Daniel Arp et al. “Drebin: Efficient and Explainable Detection of Android Malware in Your Pocket”. In: Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS). 2014. DOI: 10.14722/ndss.2014.23247.