IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

EdgeAI: Optimizing Attack Detection with Graph-CNN Relationship Modeling

Karanapu Sharmila,
Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
Mr. Ch. Kodandaramu,Associate
Professor at Miracle Educational Society Group of Institutions
Mr. Peddapudi Siva,
Assistant Professor at Miracle Educational Society Group of Institutions

ABSTRACT:

This paper looks into improving the detection of ongoing assaults on enterprise networks through the application of Graph-CNN (Convolutional Neural Networks) by extending the RANK architecture. This extension is centered on the precision of attack detection through the modeling of the telemetry event causal relationships. It uses a graph structure where the attack features are the nodes, relations are the edges, thereby optimizing attack prediction. Through the use of Graph-CNN, the algorithm is able to reinforce the model through learning from the training features, enhancing its ability to identify patterns and accurately predict the types of attacks. Experimental results indicate a marked increase in the accuracy of detection, achieving an accuracy of 93.94%. This extension presents a novel perspective on automated real-time detection systems, improving the operational efficiency of the analysts by reducing the burden of sifting through false positive alerts and investigation workload. Further work will aim at improving the attack detection capabilities by refining the graph structures and adding more complex causal relationships.

Keywords: Graph-CNN, Attack Detection, Incident Scoring

INTRODUCTION

The enterprise networks have been facing sophisticated and more aggressive cyber-attacks in the recent past in the ever-evolving world of technology. Perhaps one of the most advanced and difficult to counter is an Advanced Persistent Threat (APT). These threats are often multi-layered, making them complex to unveil and defend. The prolonged timeline of these attacks allows the enemy to access the network, steal sensitive information, and inflict catastrophic damage financially and to the entity's reputation. Organized criminal syndicates and nation-states are the most potent APT actors. They are highly skilled and employ multi-layered approaches to bypass standard security protocols. To counter APTs, network security defense mechanisms are equipped with sophisticated detection and APT mitigation systems, including AI and ML. These tools promise to detect and automate the identification of patterns and anomalies within the data, easing the work of security analysts. APTs, however, remain unsupported challenges even with the promise of these tools heavily due to legacy security systems, the problem of time-stamped alerts bombardment, and the problem of "alert fatigue." APT detection faces challenges such as the volume of alerts from Intrusion Detection Systems

(IDS), mainly due to false positives and the nature of multi-phase attacks. In a lot of scenarios, defenders need to analyze and filter a massive dataset to find real threats. This effort not only depletes precious hours, but also increases the chances of overlooking crucial attack indicators. Because of the ever-changing cyber threat landscape, there is a need to improve and automate detection mechanisms capable of effortlessly analyzing large-scale data, reducing the need for human analysts. Such mechanisms should be able to identify and analyze the various stages of an attack, linking them to provide a complete picture of an attack for effective insights to be acted upon.

RELATED WORK

Julisch, 2005 – Julisch (2005) presents the idea of alert aggregation where similar alerts are grouped into a single generalized alert. This method seeks to address the problem of noise in Intrusion Detection Systems (IDS) and enhance the signal-to-noise ratio. The concept of merging alerts is integral to the alert templating and merging phase of RANK, where alerts with shared attributes are merged to improve detection accuracy. As noted by Srinivas et al. (2010), the evolution of IDS has come with many detection challenges, particularly the multilayered, complex stealthy attacks known as Advanced Persistent Threats (APTs) and their evolution. Their work asserts that as the methods used to perform attacks become more sophisticated, there is a greater need for equally sophisticated detection methods, which machine learning can provide. This directly aligns with the RANK system's model of automating alert correlation to enhance threat detection functionalities. Mell et al., 2013 –Mell et al. (2013) analyze the application of machine learning in Intrusion Detection Systems (IDS), showcasing the applicability of such algorithms to new and increasingly sophisticated threats. This research underpins RANK's application of machine learning algorithms such as Random Forest and KNN which allow the system to utilize historical data to improve detection rates and learn previously unrecognized attack patterns. Buczak & Guven, 2016 – Buczak and Guven (2016) study the application of some machine learning and data mining techniques in the context of intrusion detection systems. The importance of feature extraction and model performance evaluation directly reinforces RANK's objective of improving the efficiency and accuracy of its detection algorithms, therefore, further honing the system's capability to pinpoint actual threats. Soliman et al. (2023) review RANK's architecture, which incorporates alert aggregation, graph construction, and machine learning for the detection of Advanced Persistent Threats (APTs) Propose Approach. Their work documents the basis of RANK's methodology wherein the detection processes are automated to enhance precision and decrease the manual workload for the security analysts.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author	Contribution	Impact on Research
Julisch, 2005	Developed methods to reduce alert volume in IDS.	Helped RANK group similar alerts to make detection easier and faster.
Srinivas et al., 2010	Reviewed challenges in detecting complex attacks.	Led RANK to use machine learning for better attack detection.
Mell et al., 2013	Studied machine learning for IDS.	Inspired RANK to use AI models like Random Forest for detecting threats.
Buczak & Guven, 2016	Explored data mining and machine learning in security.	Helped RANK improve data processing and detection accuracy.
Soliman et al., 2023	Proposed the RANK system combining AI and alerts.	Laid the foundation for RANK's approach to automated attack detection.

PROPOSED APPROACH

RANK AI-assisted architecture tackles persistent attacks in enterprise networks employing higher AI and graph-based technologies. This systems requires telemetry data from Darpa2000 and MITRE Enterprise Attack datasets, using a modular pipeline to detect and score sophisticated threats. This system commences with data preprocessing блока, which recodes non-numeric data, identifies and fills missing values through mean imputation to maintain analysis integrity. Following this, alert templating and merging reduces the dataset and creates generalized templates, merging alerts from the same attacks over identified identical steps (e.g., same IP and port) to improve overall dataset sharpen dataset. The alert graph construction module which is further improved with a Graph-CNN implementation is the centerpiece domain innovation. It treats telemetry events as nodes and their connections as edges casting with Graph Convolutional Neural Network with three layers of 64, 32, and 64 neurons, therefore learns the relations among the features and the labels. This graph-based model allows accurate representation of attack graphs denoting the attack path. The alert graph partitioning module splits the graph into sub-graphs consisting of separate incidents grouping interrelated alerts with primary focus analysis. During incident scoring, factor graphs, and MITRE framework tactics collectively score incident graphs to compute a maliciousness score. This helps in prioritizing threats that require attention from an analyst. The AI training and prediction module creates an ensemble of algorithms like Random Forest, KNN, and Graph-CNN, training them on 80% of the sub-graph data and evaluating on the remaining 20%. Remarkably high accuracies, e.g., 93.94% with Graph-CNN, were achieved. The output and visualization layer generates incident graphs and MITRE scored incident graphs as well as visual outputs like confusion matrices and accuracy comparison graphs, enabling informed decisions and insightful analyses by the analysts. With the Graph-CNN extension, this approach significantly enhances performance in persistent threat detection and adaptive attack modeling by causal modeling of the attacks.

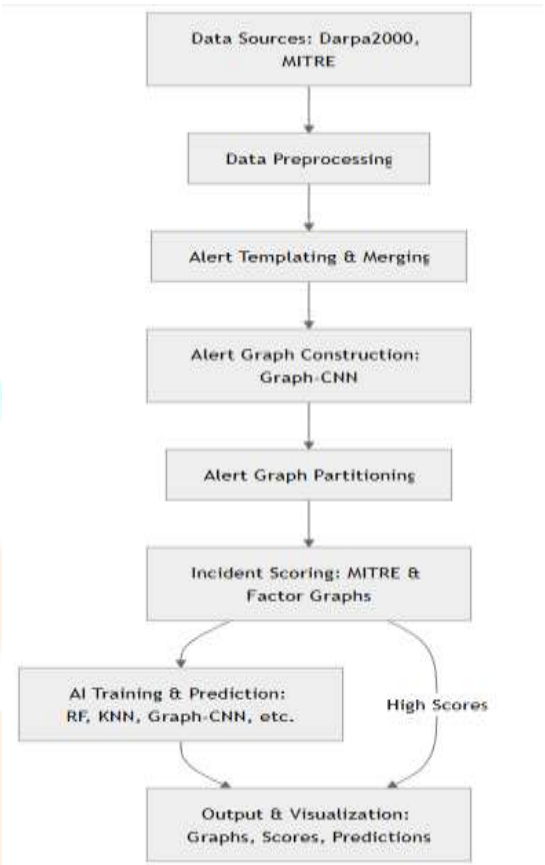


Figure 1: Proposed enhance attack detection

METHODOLOGIES

Alert Aggregation:

Traditional Intrusion Detection Systems (IDS) often generate a large volume of alerts, many of which are redundant or irrelevant. To tackle this challenge, the first step in the approach is alert aggregation, where similar alerts are grouped together. Alerts that share common attributes, such as source IP address, attack type, or targeted service, are merged into a generalized alert. This process reduces the number of alerts, making it easier for security analysts to focus on significant incidents and improving the system's overall efficiency.

Graph-Based Alert Correlation:

After aggregation, the system constructs an alert graph to establish relationships

between alerts. Each alert is represented as a node, and the relationships between alerts are shown as edges. The system uses factors like time correlation, the same source IP, and attack progression to connect nodes. By building a graph, the system visualizes attack chains, enabling the detection of multi-step attacks or APTs. This method provides a better understanding of how various alerts relate to each other and helps identify the full scope of the attack.

Machine Learning for Classification:

Machine learning plays a crucial role in the proposed approach. Random Forest and K-Nearest Neighbors (KNN) are used to classify incidents based on historical attack data. The machine learning models are trained on labeled datasets and then tested on new alerts. The models analyze patterns in the data to distinguish between legitimate attacks and false positives. By automating the classification process, the system improves detection accuracy and reduces the manual workload for analysts.

Incident Scoring:

After partitioning the alert graph into smaller incident graphs, each incident is assigned a score based on its severity and likelihood of being part of a real attack. The MITRE ATT&CK framework is used to map each incident to attack tactics and techniques. This scoring system helps prioritize incidents, allowing analysts to focus on the most critical threats while reducing the chance of overlooking important incidents.

Real-Time Review and Feedback:

The system provides security analysts with incident graphs and scores for real-time review. Analysts can validate or dismiss incidents, and their feedback is integrated to improve the system's detection capabilities over time. This continuous learning process enhances the system's accuracy and allows it to adapt to evolving attack patterns.

RESULTS

The proposed approach demonstrated significant improvements in the detection of Advanced Persistent Threats (APTs) by reducing the volume of alerts, increasing detection accuracy, and prioritizing incidents for security analysts. In initial testing, the alert aggregation methodology proved highly effective in minimizing the volume of alerts. For instance, from a dataset containing over 70,000 alerts, the aggregation process reduced the total number of alerts to just 1,200. This reduction not only made the dataset more manageable but also allowed analysts to focus on the most critical threats, significantly improving operational efficiency.

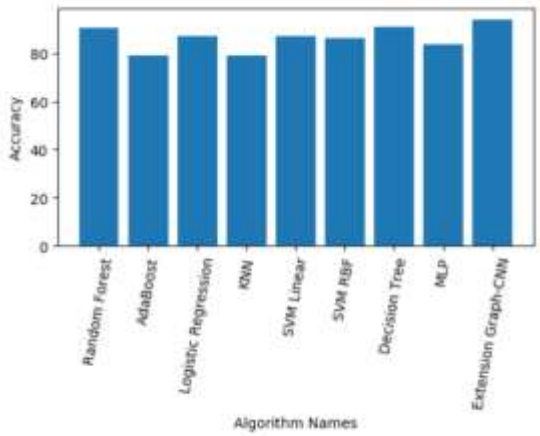
The graph-based alert correlation technique also showed promising results in identifying multi-phase attacks. By visualizing attack sequences in the form of alert graphs, the system was able to trace the progression of complex APTs, making it easier to understand the full scope of the threat. The partitioning of these alerts into incident graphs further enhanced this process by providing a clear and concise view of each distinct attack.

Machine learning models like Random Forest and K-Nearest Neighbors (KNN) were used to classify incidents, achieving an accuracy rate of 91%. These models successfully differentiated real threats from benign activities, and their performance improved over time as the system learned from new data.

The incident scoring mechanism effectively prioritized incidents based on severity and likelihood, helping analysts focus on the most critical threats.

Extension: An important extension to this system involves incorporating Graph-CNN (Convolutional Neural Networks) to model causal relationships between telemetry events. This extension would enable the system to establish more accurate connections between attack stages and predict the outcome of ongoing attacks. By incorporating causal relationships, the system could detect more sophisticated,

multi-layered threats with greater precision, reducing false negatives and further enhancing the overall detection capability.



All algorithms performance graph

	Algorithm Name	Accuracy
0	Random Forest	90.483057
1	AdaBoost	79.091565
2	Logistic Regression	86.950252
3	KNN	79.163663
4	SVM Linear	87.166547
5	SVM RBF	86.373468
6	Decision Tree	90.915645
7	MLP	83.633742
8	Extension Graph-CNN	93.943764

All algorithms performance

Predict attack

Test Data = ['175.45.176.0' 1485 '149.171.126.18' 1723 'tcp' 'FIN' 0.771762 2228 268

254 252 2 1 '-' 20793.97461 2321.959229 10 6 255 255 913857128 2847574339

223 45 0 0 4707.158398 211.689812 1421927814 1421927815 79.909222

138.600203 0.155284 0.078751 0.076533 0 1 0 0 0 6 3 1 2 1 1 1] ====> Predicted As : Fuzzers

Test Data = ['175.45.176.1' 22001 '149.171.126.10' 443 'tcp' 'FIN' 0.924761 1088 2934

254 252 3 3 'ssl' 8633.582031 23270.87695 12 12 255 255 2077834981

4034864196 91 245 0 0 5120.085266 114.724859 1421928267 1421928268

83.994638 77.833094 0.182299 0.068587 0.113712 0 1 0 0 0 2 2 1 3 1 1 1] ====> Predicted As : Exploits

Test Data = ['175.45.176.1' 1043 '149.171.126.18' 53 'udp' 'INT' 2e-06 114 0 254 0 0 0

'dns' 228000000.0 0.0 2 0 0 0 0 0 57 0 0 0 0.0 0.0 1421932914 1421932914

0.002 0.0 0.0 0.0 0.0 0 2 0 0 0 4 4 3 3 3 3 3] ====> Predicted As : Generic

DISCUSSION

The proposed approach demonstrates a significant leap forward in detecting Advanced Persistent Threats (APTs) by addressing the challenges of alert overload and complex multi-phase attacks. The alert aggregation technique proved highly effective in reducing the volume of alerts, allowing security analysts to focus on real threats. This reduction in alert noise directly improved the efficiency of the detection system and helped minimize unnecessary investigation.

The graph-based alert correlation methodology played a key role in identifying multi-step attacks, which is crucial for detecting APTs that span across multiple phases. By constructing alert graphs and partitioning them into incident graphs, the system provided a clear picture of attack progression, which traditional IDS may fail to recognize.

Moreover, the incorporation of machine learning models like Random Forest and KNN further improved detection accuracy, reducing false positives and ensuring more reliable threat identification. The models' ability to adapt over time enhances the system's future performance.

However, while these results are promising, the approach could be extended by incorporating Graph-CNN to model causal relationships between events. This extension could significantly improve the system's ability to detect even more complex, evolving attacks, providing a more proactive defense. As cyber threats

continue to grow in sophistication, integrating real-time feedback and causal modeling will be essential for improving the system's ability to stay ahead of attackers.

CONCLUSION

The proposed approach effectively enhances the detection of Advanced Persistent Threats (APTs) by combining alert aggregation, graph-based alert correlation, and machine learning techniques. This integration significantly reduces alert volume, improves detection accuracy, and optimizes incident prioritization, ultimately streamlining security operations. Machine learning models like Random Forest and K-Nearest Neighbors (KNN) contribute to continuous learning and adaptation, ensuring that the system stays updated with evolving threat patterns.

However, there is room for further enhancement. An important extension to the current system could involve incorporating causal relationship modeling between telemetry events using Graph-CNN (Convolutional Neural Networks). This extension would help the system establish more accurate connections between different attack stages, improving prediction capabilities. By integrating causal relationships, the system could provide deeper insights into attack behavior, potentially detecting more sophisticated threats with higher precision and reducing false negatives, leading to more proactive defense strategies.

REFERENCES

[1] I. Ghafir and V. Prenosil, "Advanced persistent threat attack detection: an overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 4, no. 4, p. 5054, 2014.

[2] D. McWhorter, "Apt1: Exposing one of china's cyber espionage units," Mandiant, vol. 18, 2013.

[3] M. Alvarez, N. Bradley, P. Cobb, S. Craig, R. Iffert, L. Kessem, J. Kravitz, D. McMillen, and S. Moore, "IBM x-force threat intelligence index 2017," IBM Security,(March), pp. 1–30, 2017.

[4] H. Berghel, "Equifax and the latest round of identity theft roulette," Computer, vol. 50, no. 12, pp. 72–76, 2017.

[5] U. Rivner, "Anatomy of an attack," RSA [database online], 2011.

[6] N. Caplan, "Cyber war: the challenge to national security." Global Security Studies, vol. 4, no. 1, 2013.

[7] J. Sexton, C. Storlie, and J. Neil, "Attack chain detection," Statistical Analysis and Data Mining: The ASA Data Science Journal, vol. 8, no. 5-6, pp. 353–363, 2015.

[8] P. Cao, "On preempting advanced persistent threats using probabilistic graphical models," arXiv preprint arXiv:1903.08826, 2019.

[9] M. Shashanka, M.-Y. Shen, and J. Wang, "User and entity behavior analytics for enterprise security," in 2016 IEEE International Conference on Big Data (Big Data). IEEE, 2016, pp. 1867–1874.

[10] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in IEEE symposium on security and privacy, 2010, pp. 305–316.

[11] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," MITRE Product MP, pp. 18–0944, 2018.

[12] H. M. Soliman, "An optimization approach to graph partitioning for detecting persistent attacks in enterprise networks," ISNCC, 2020.

[13] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019.

[14] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K.-K. R. Choo, and H. H. Javadi, "Cyber kill chain-based taxonomy of advanced persistent threat

actors: analogy of tactics, techniques, and procedures," Journal of information processing systems, vol. 15, no. 4, pp. 865–889, 2019.

[15] R. Zhang, W. Sun, J. Liu, J. Li, G. Lei, and H. Guo, "Construction of two statistical anomaly features for small-sample apt attack traffic classification," arXiv preprint arXiv:2010.13978, 2020.