Anomaly Detection in Cybersecurity with Graph-Based Approaches

Md Shariar Sozol[1], Golam Mostafa Saki[2], Md Mostafizur Rahman[3]

[1] *Master of Cybersecurity (Extension) & University of Technology Sydney (UTS), Australia*
[2] *Msc in Engineering Management & University of South Wales, United Kingdom (UK)*
[3] *Master of Engineering (Extension) & University of Technology Sydney (UTS), Australia*

---***---

Abstract - The field of cybersecurity is changing dramatically in this dynamic age of digital revolution. This work on Anomaly Detection in Cybersecurity using Graph-Based Approaches represents a ground- breaking project that uses Graph Neural Networks' (GNNs'), Graph-Based Behavioural Anomaly Detection (GBBAD), Behavioural Identification Graph (BIG) and Graph-Based Botnet Detection (GBBD) capabilities to revolutionize the way we defend our digital borders. The discovery signifies a noteworthy progress in uncovering abnormalities. The precision and flexibility of this system has been emphasized by the ability to identify minute anomalies within intricate network interactions. Graph based techniques locating nodes or edges diverging from the normal behaviour of a graph carry out anomaly detection on graphs. There are several cyber security threats including fraud, malware incursions and network attacks that can be detected using graph-based anomaly detection methods. However, there are still some areas that need more attention. For instance, one possibility is to utilize the graph-based algorithms for pre-filtering alerts from firewalls and other cybersecurity systems. Such development would significantly reduce the workload for security analysts as well as improve overall security posture. In this research work an overview of current methods of detecting anomalies on cyber security using graphs has been presented.

Key Words: Graph-Based Anomaly Detection (GBAD), Graph Neural Networks (GNNs), Graph-Based Behavioural Anomaly Detection (GBBAD), Graph-Based Botnet Detection (GBBD), Types of Anomalies, Availabilities of Data Levels.

1. INTRODUCTION

Anomaly detection systems can detect abnormal behavior and are essential in order to counteract cyber-attacks. Historically, these systems have relied on signature-based approaches which are good for identifying known threats but have not been effective at handling the ever-changing space of unknowns including zero-day attacks. Graph-based techniques find themselves having caught the interest of cyber security professionals as well as researchers.

Early anomaly detection methods were primarily aimed at locating statistical anomalies within data. In terms of graph-based anomaly detection in cybersecurity Dorothy Denning's work during the 1980s is one such pioneer [1]. The adoption of graph-based approaches for intrusion detection systems also began gaining popularity from 1990s onwards [2]. Researchers set out to identify statistical outliers in early methods for detecting anomalies [3]. However, these methods often failed they could not identify cyber threats because cyber attackers became cleverer and better at avoiding typical detection techniques [4].

Anomalies detection is the study of unusual behavior patterns that reveal an inconsistency or error in a data set. The concept has been there for many years, but only recently graph-based approaches have gained importance as alternatives to traditional methods. These algorithms are able to detect anomalies which would have been difficult using conventional techniques [5]. Such algorithms exist today but they can be both expensive and hard to translate into larger data sets [6]. Graph-based anomaly detection techniques take advantage of relationships between points on graphs and can raise alarms to alert the system. When it comes to intricate datasets such as cybersecurity databases, this significantly enhances the capability of graph-based approaches to identifying anomalies in them; therefore these advanced techniques become an important part of the cyber-crime prevention measures [2]. More research needs to be directed toward developing scalable and more effective new algorithms with superior detection abilities.

2. Anomaly Detection Strategies

The process of locating odd or unexpected data points is known as anomaly detection. This process requires that if an anomaly happens, then an investigation should be launched whether it is false positive or real concerns. If the former proves to be true order must be given for its prevention such as stopping fraudulent transactions or repairing broken machines.

2.1. Types of Anomalies:

Types of anomalies can be divided into three categories, including [7]:

1. Point/Rare Anomaly: Individual data points whose values fall outside the predicted value range are known as point anomalies. They are often easy to spot since they are isolated from the bulk of the dataset. This might be seen when high amounts get splashed on a single purchase within different people's shopping lists.
2. Contextual Anomaly: Points that are anomalous with respect to the rest of their environment are referred to as contextual anomalies. In this case it could happen that a particular reading happens to be way above other readings from one sensor at specific time periods.

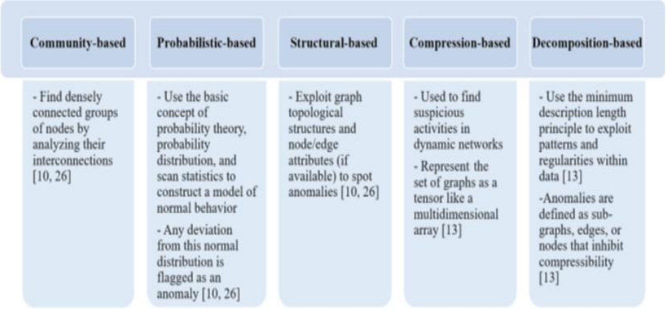
3. Collective Anomaly: These refer to groups of extraordinarily related points besides those mentioned above. For example, in a network traffic database cluster headers with similar features but receiving excessive amounts like never before on one server happened to stand out as collective anomaly.

To resolve, various methodologies for GBAD have been devised to differentiate between various types of irregularities. These techniques detect anomalies on different networks such as attributed or non-attributed dynamic or static graphs through anomaly logging [8] –

- **Nodes:** Anomalous nodes are those nodes wherein distinctive characteristics are present that aren't found in other nodes in the network.
- **Edges:** Similarly to anomalous nodes, each edge within the anomalous edges subset has at least one value that is higher than a certain threshold, hence making it deviate from what's termed as normal.
- **Subgraphs:** The initial step is always identifying subgraphs via community detection methods after which within-graph comparison terms give anomaly score(s) respective to each of them.
- **Events:** This particular category of anomaly is meant for identifying a precise duration of time only within dynamic networks.

2.2. Graph Methods

The important part of this research is the analysis of the terms of graph theory and its application to cyber defense. This refers to awareness about graph algorithms, graph-based anomaly detection methods as well as the representation networks using graphs. It is this understanding that forms the basis for further analysis to follow –



Community-based	Probabilistic-based	Structural-based	Compression-based	Decomposition-based
- Find densely connected groups of nodes by analyzing their interconnections [10, 26]	- Use the basic concept of probability theory, probability distribution, and scan statistics to construct a model of normal behavior - Any deviation from this normal distribution is flagged as an anomaly [10, 26]	- Exploit graph topological structures and node/edge attributes (if available) to spot anomalies [10, 26]	- Used to find suspicious activities in dynamic networks - Represent the set of graphs as a tensor like a multidimensional array [13]	- Use the minimum description length principle to exploit patterns and regularities within data [13] -Anomalies are defined as sub-graphs, edges, or nodes that inhibit compressibility [13]

FIGURE 2.2(a): Five Different Types of Graph-Based Anomaly Detection (GBAD) [8].

Graph methods use machine learning algorithms or algorithms used in networks for identifying diverse types of anomalies. Earlier works have recorded diverse abnormality types through five strategies based on input network parameters, various types of anomalies found in networks and the available data labels.
Determined by the data labels as well as the character of input network, five different GBAD techniques were used in capturing different kinds of anomalies happening within the network in 39 papers reviewed. Community-based approaches were the most popular (35.9%) followed by probabilistic ones second in rank (25.6%). Structural-based techniques were utilized in approximately 17.9% of the papers, compression-based in 10.3% of these studies while decomposition-based methods had least usage at 10.3% [8].

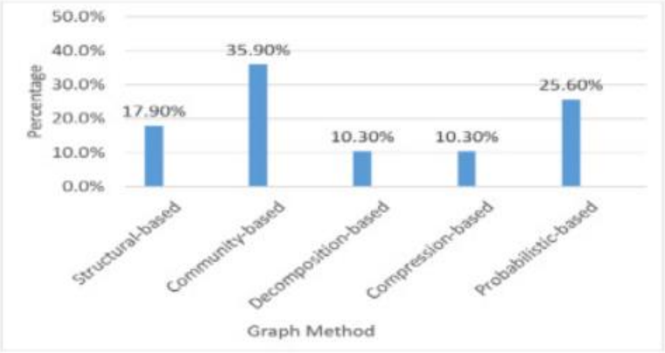


FIGURE 2.2(b): Spread of different GBAD methods in the papers reviewed [8].

2.3. Availability of Data Levels

Data accessibility is a fundamental aspect in determining the efficacy of anomaly detection. When there is more data, the comprehension of normal operations of a suggested system and the recognition of unusual events become improved [8]. Consequently, there are several classes of anomaly detection methods based on present availability of labeled data [8]:

(i) Supervised Anomaly Detection Technique,
(ii) Unsupervised Anomaly Detection Technique, and
(iii) Semi-Supervised Anomaly Detection Technique.

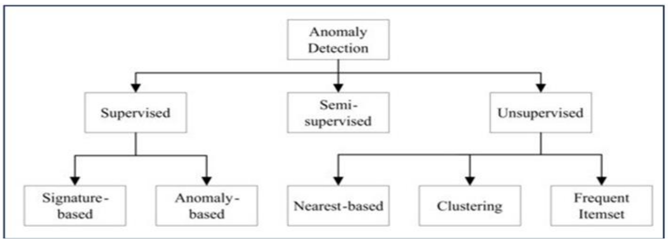


FIGURE 2.3: A taxonomy of Anomaly Detection Approach [9].

2.4. System Overview

In this research paper, we propose a unique graph-based anomaly detection system designed for application in cybersecurity. The framework is designed to be durable, egalitarian, and intelligible in nature. Graph theory provides a solution through using graph-based techniques. Therein, the nodes represent entities while edges or links resemble the interactions among those said entities.

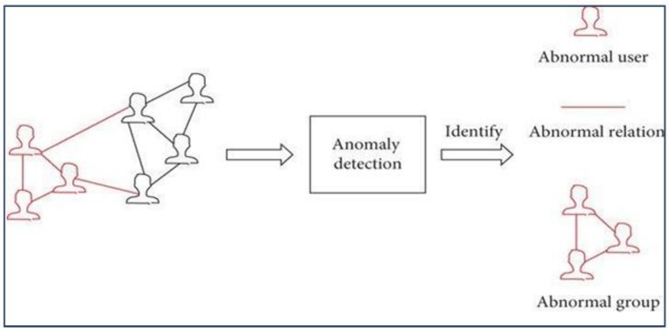


FIGURE 2.4: Schematic Diagram of Graph-Based Anomaly Detection [10].

The quality and relevance of the dataset greatly affect anomaly detection efficiency. We develop an extensive dataset containing diverse forms of interactions taking place within a digital ecosystem by employing genuine network traffic information. Importantly, our anomaly detection system is guaranteed of being well-rounded as well as contextually conscious by first converting unstructured data into structured graphs for its further assessment [10]. To allow continuous monitoring network activity, our technology also integrates real time data streaming capabilities. The main focus while developing our system was Integration and Scalability. To study very large networks in real time, our technology ensures scalability by utilizing parallel processing and distributed computing frameworks [11]. Furthermore, smooth interaction with existing cybersecurity infrastructures leads to timely sharing of threat intelligence and defense mechanisms.

3. Methodology and Modeling

Collecting relevant and diverse data is without a doubt an important step in any research project, especially for graph-based approaches to cybersecurity anomalies detection. The methodology section of our study considers and shall discuss several forms of data collection methods that follow:

3.1. Graph Neural Networks (GNNs)

Graph Neural Networks (GNNs) are one particular machine learning approach that can be taught to represent the relationships between nodes in a graph. There have been several applications where GNNs have proven quite effective, such as in cybersecurity anomaly detection. GNGs distribute information all over the graph. Each node at each layer of the GNG changes its representation depending on what the other nearby nodes are represented as.

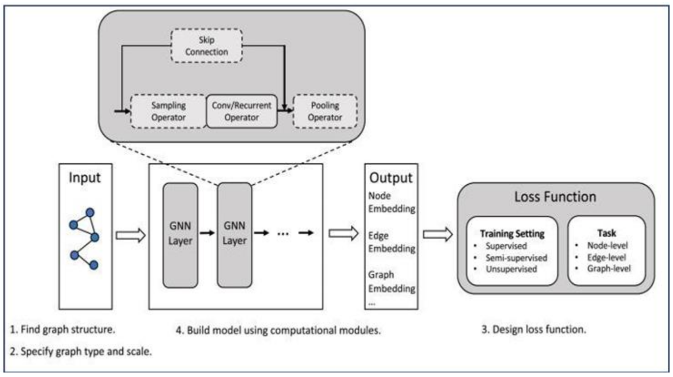


FIGURE 3.1: General Pipeline Design of GNN Model [12].

Once the GNG has learned to depict the connections among the nodes of a certain graph, it can be employed to detect abnormalities within such a structure. There would be some noticeable dissimilarity between any given node's representation and that of other nodes within that particular graph.

3.2. Path Based Method

Shortest paths inspection between nodes reveal anomalies. Unusual lengths or short paths that nodes utilize could indicate a misconfigured network or possible attacks.

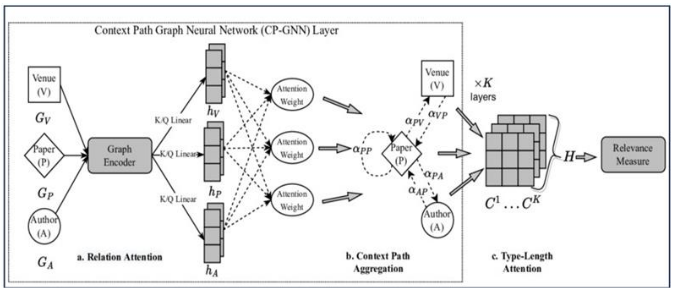


FIGURE 3.2: Overall Framework of Context Path Network (CP-GNN) Layer [13].

Random walks may help find anomalies on graphs. Hovering might also indicate extreme visiting patterns or more frequent visits than normal points which point at odd network behavior thereby showing some potential dangers.

3.3. Graph Clustering Techniques

Using K-means clustering, nodes are grouped according to their relationships or attributes. Anomalies are nodes that do not fit into any cluster or create singleton clusters that indicate possible outliers [13]. Unusual or dubious networks may contain nodes that are isolated or do not belong to any dense cluster, which may indicate anomalies.

3.4. Deep Learning Model

Graph Convolutional Networks (GCNs) allow nodes to learn from nearby areas through transforming neural networks in graph-structured data. Such major differences with its neighbors' embeddings may represent an anomaly or an incorrectly configured entity for a node [13].

4. Architecture of GNNs

In general terms, the GNN topology consists of several different levels, where each level is responsible for providing new node representations through combining information from adjacent nodes. GNN's output layer assigns each node an anomaly score which indicates how abnormal the respective node may probably be. For example, GNNs can be applied to identify nodes having peculiar edge or node features. Furthermore, it is possible to use GNNs in order to identify nodes with unique temporal patterns or those that are part of unusual subgraphs.

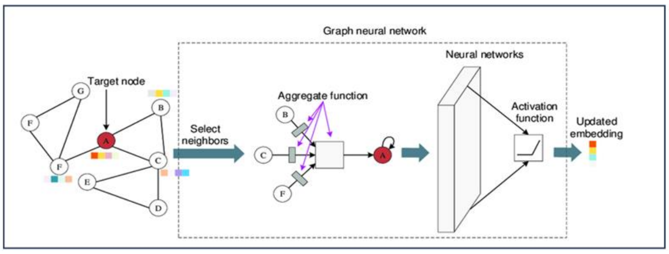


FIGURE 4: Graph Neural Network (GNN) Architecture [16].

To develop an effective graph neural network architecture for anomaly detection in cybersecurity, one needs to be well-versed in the intricacies of network behaviors, as well as the latest techniques for detecting minute anomalies. This is a detailed framework for the design of a GNN architecture specifically tailored to the purpose of cybersecurity anomaly detection.

4.1. Graph Convolution Network (GCN)

The incorporation of Graph Convolutional Networks (GCN) into the overall paradigm of Graph Neural Networks (GNN) has revolutionized anomaly detection in cyber security. GCNs are created specifically for graph-structured data types. They have an exceptional ability to interpret complex connections and patterns within networks topologies.

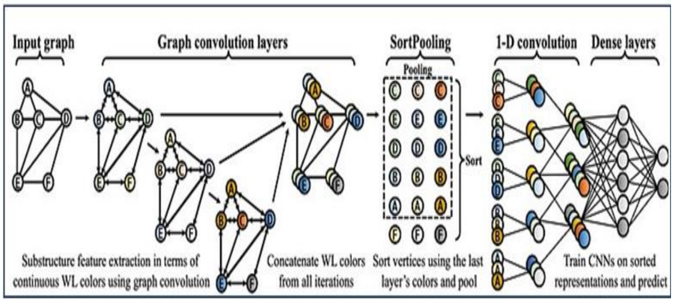

Input graph
Graph convolution layers
SortPooling
Pooling
1-D convolution
Dense layers
Sort
Substructure feature extraction in terms of continuous WL colors using graph convolution
Concatenate WL colors from all iterations
Sort vertices using the last layer's colors and pool
Train CNNs on sorted representations and predict

FIGURE 4.1: Graph Convolutional Networks (GCN) Layers [14].

This feature is extremely significant in cyber security because sometimes it's essential to distinguish from abnormal network behavior [13]. Using various stacked layers and integrating skip connections, GCNs encapsulate all the complexities associated with interconnected devices, individuals, and applications.

4.2. Graph Attention Network (GAT)

The incorporation of Graph Attention Networks (GAT) into the larger Graph Neural Network (GNN) architecture is a groundbreaking development in the field of cybersecurity. Through the use of their self-attention mechanism, GATs have completely changed how complicated network architectures are examined in order to identify anomalies [14]. Proactive threat mitigation is made possible by the accuracy and effectiveness of GATs in cybersecurity anomaly detection, which guarantees that the digital ecosystem will continue to be strong and resilient in the face of changing security threats [15].

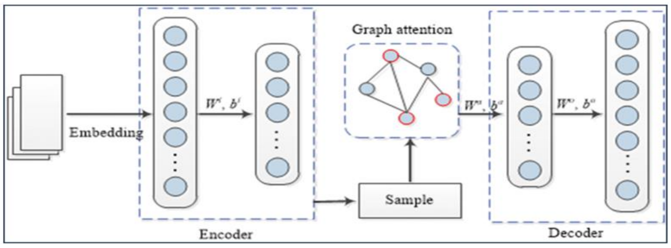


FIGURE 4.2: Graph Attention Neural Networks Architecture [15].

In summary, there is no way to compare the advantages derived from combining Graph Attention Networks with Graph Neural Networks, because it's like trying to measure how high a bird can fly or what color is the sky. Indeed, this novel approach allows GATs to make use of complex features inherent in different classes of communication lines such as Ethernet cables for instance making it easy for experts dealing with data breaches alone without any addition into their mix such as not being able to notice even minute imperfections.

4.3. Graph Representation

Understanding network connections is very important for cybersecurity. Graph Representation, which transforms the intricacy of interrelated entities into a systematic graph, is a fundamental part of the architecture of Graph Neural Networks (GNNs). Nodes are used to symbolize persons, machines or software applications with its own set of attributes. The edges between them represent their interactions or give an overview of a complete network. This complex graph can be traversed by GNNs because they encode these features as well as the interactions that facilitate accurate anomaly detection. The dynamic and complicated nature of cyber threats has made Graph Convolutional Layers the basis for innovative anomaly detection techniques.

This has resulted in cyber security innovations such as Graph Convolutional Networks (GCNs), which take advantage of connected data to transform cyber security designs. By extracting complicated relationships from graphs, these specialized layers enable networks to learn from data topology [14]. Such structures thus enhance anomaly detection through interpreting complex networks and identifying minute relationships thereby shielding virtual environments against ever-evolving internet risks.

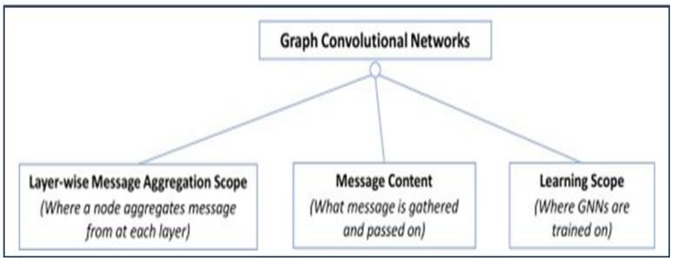

Graph Convolutional Networks
Layer-wise Message Aggregation Scope
(Where a node aggregates message from at each layer)
Message Content
(What message is gathered and passed on)
Learning Scope
(Where GNNs are trained on)

FIGURE 4.3.1: Taxonomy of Graph Convolutional Networks from Structural Perspectives [17].

An important stage in GNN function for anomaly searching is the aggregation of Graph Convolutional layers. After the first convolutional operations, data from neighboring nodes is combined in order to enhance node representations [11]. The aggregated layers improve a model's ability to understand complex intra-network relationships, which aids in detecting abnormalities and fortifying the cyber security framework.

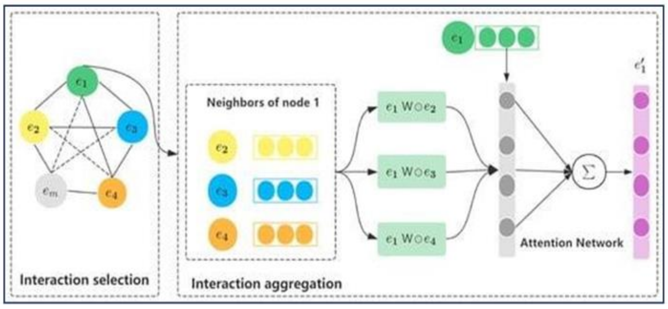


FIGURE 4.3.2: GNN Feature Interaction Layer [18].

Using activation allows the complicated patterns to be picked up by the network so as to identify important features in terms of identifying anomalies [14]. Applying activations permits GNNs to identify subtle differences in the data hence increasing the model's ability to detect bizarre activities in large and complex cyber security databases.

4.4. Layout of GNN in Cyber-Security for Anomaly Detection

For cybersecurity anomaly detection using GNN architecture, the output layer forms the last threshold of knowledge-intensive complexity. Anomaly scores measure how much an observed behavior deviates from the norm, thus giving an indication of its likelihood. In order to compute such scores, complicated algorithms come into play which analyze GNN learned features, often making use of machine learning or probability models. In terms of cyber-security, an enhanced anomaly scoring signifies potential dangers hence promoting a prompt reaction.

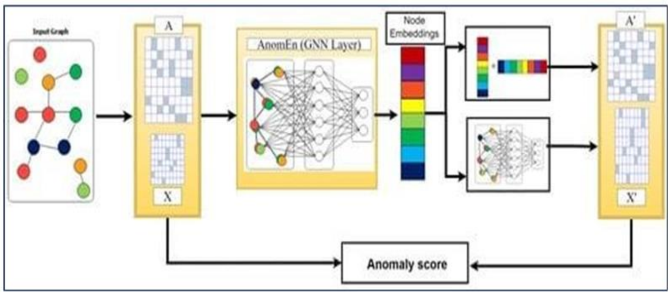


FIGURE 4.4.1: Node Anomaly Detection [16].

First, data preparation is initiated in which unprocessed network data are transformed to an organized graph format. In this case nodes represent hardware, individuals and software, whereas edges signify relationships among them. Well-thought-out node and edge attributes incorporate essential information like IP addresses, actions, timestamps etc., as well as communication trends.

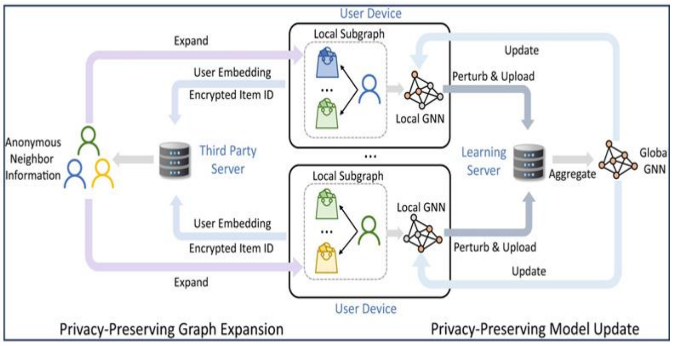


FIGURE 4.4.2: Overall Framework of GNN [19].

The fundamental component of the implementation is the GNN architecture. GNN layers contain graph convolutional layers that perform feature aggregation and transformation, using various libraries. Attention mechanisms such as graph convolutional LSTM layers or graph attention networks (GAT) can be integrated so as to capture complex linkages and temporal correlations [15]. Activation functions, dropout layers deployed strategically, and proper initialization of node embeddings ensure network stability.

In the deployment phase, the trained GNN can receive batches of or real-time streaming data for continuous monitoring. The use of GNNs has rendered them an essential tool for identifying cybersecurity issues before they arise [14, 16].

Apply the trained GNN to derive anomaly ratings for every entity in the network. These scores indicate how likely it is that a particular entity is anomalous. Anomaly detection system based on GNN should be inbuilt in cybersecurity infrastructure for real-time monitoring of attacks. Set automatic responses and alerts for any identified anomalies. Regularly update and retrain the GNN model to keep pace with evolving threats posed by cyber criminals [11, 20]. To maintain effective anomaly detection systems, always cautious monitoring with feedback loops is needed.

5. Architecture of GBBAD

Graph-Based Behavioral Anomaly Detection (GBBAD) is an innovative framework developed to combat the ever-evolving nature of cyber security. Some researchers are trying to come up with more effective behavioral models by using interaction information between behavioral events, such as sequential information about behaviors, so as to extract more useful information from behavior data.

5.1. Approach

When an individual or object tries to perform unlawful acts, they will do their utmost to pretend that their behavior is consistent with that which is legal. Recent statistics reveal that

fraud is costing companies 6% of their income while almost 60% of all fraud cases originate from employees [21].
Anomalies can be categorized into three main classes: insertions, modifications and deletions. Insertions refer to unexpected presence of vertices or edges, deletions denote unexpected absence of vertices or edges while modifications involve unexpectedly labeling vertices or edges [21].

5.2. Behavioral Identification Graph (BIG)

The detailed connections between characteristics forming behavior occurrences provide ripe intelligence and become the basis for high-performance behavior models. To better illustrate these connections, our BIG uses an event space representing behavior occurrences in one low dimensional vector space and a property graph revealing tiny links among them, so as to losslessly reconstruct behavioral events. Node/event representations learned through the event-property composite model are laden with deep association information. The property space (inter associations between properties) and event space (intra associations between events) are the inputs for the event-property composite model. This is how we have integrated two behavioral connections into a singular area with our BIG.

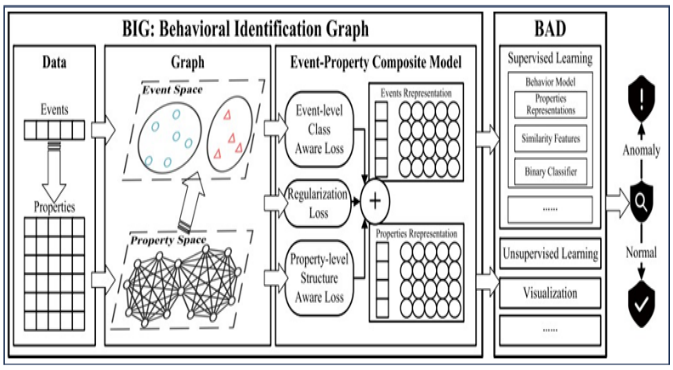


FIGURE 5.1: Workflow of BAD and BIG for anomaly detection [13].

For the purpose of enhancing behavioral modeling for anomaly detection, BIG's approach involves merging intra- (property level) and inter- (event level) associations of behaviors into a unified graph and dimensionality space [22]. This paper makes the following main technical contributions:

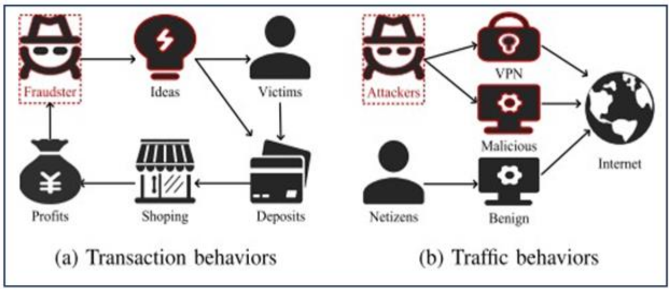


FIGURE 5.2: Illustrations of two different scenarios [13].

By making use of property graphs and understanding event-property composite models, BIG is able to obtain optimal feature representations from behavior events made up of multiple properties. According to these learned representations, BAD converts every behavior event into either an event representation matrix or property representation matrices respectively. Then it utilizes various types of detection models such as supervised or unsupervised in order to identify anomalous behavioral events [22].

6. Overview of GBBD

A BOTNET is an exposed computer network that is managed by a "botmaster". Botnets are regularly used in click fraud, spam mails, and DDoS attacks. By flooding the victim with packets and requests from various bots, DDoS attacks effectively consume scarce resources and deny access to authorized users. The botnet based attacks are rampant. As per a recent survey, 65% of DDoS attacks result in financial loss of up to $10,000 per hour, which affected 300 out of 1000 surveyed organizations [17]. Moreover, since bots are dynamically changing and becoming increasingly advanced, its graph-based detection might produce false positives or negatives or assist them to escape [23].

6.1. Botnet Discovery

The botnet detection technique can be applied when there is sufficient presence of anomalies. Firstly, we define interaction records in order to integrate the outputs of the two methods [17]. For example, Zhao was the first to propose a new framework for cyber threat discovery based on multi-granular attention and the extraction of Indicators of Compromises (IOCs) in cybersecurity; he converted this case study into a semi-supervised classification problem using GCN method [24].

6.2. Botnet Detection Approach

We will discuss two approaches to anomaly detection. Discrete Random Variables are the observations that are made by quantizing flows in the first approach. It uses netflow files as input. In contrast, the second method takes packet files as input, aggregates packets into graphs and uses LDP to find out the degree distribution of the graph obtained from inputted pcap files [23].

6.2. Flow Based Approach

Stability and similarity of C-flow as detection metrics. C-flows are allocated a stability score based on packet length distribution within a C-flow, while similarities between C-flows [24] are measured and assigned using k-means.

The following attributes represent a flow [17]:
1. The source port number,
2. The destination port number,
3. The cluster label of the source IP address, and
4. The cluster label of the destination IP address;
5. The duration of the flow;
6. The bytes of data sent from the source to the destination; and
7. The bytes of data sent from the destination to the source.

6.3. Graph Based Approach

A method for processing data packets at the packet level using graphs. Each packet is seen as a record of the interactions between its source and destination. We first classify packets using timestamps into windows. For all k, we will denote by Wk the set of packets in the window k [17].
In graph-based traffic analysis, three types of graph-based features are extracted: number of nodes, edges and weights in an egonet. More specifically we compute an anomaly score that describes how their neighborhoods change over time using Local Outlier Factor (LOF) and Least-Square method. By merging results based on similarity, stability and anomaly scores BotMark does automated botnet detection through combined flow-based and graph-based traffic analysis [25].

6.4. Comparison between Graph Based Approach and Flow Based Approach

In a real computing environment, Mirai, Black Energy, Zeus, Athena and Ares have recently proliferated into five botnets and a considerable amount of network traffic is gathered [25]. Many experiments have shown that BotMark is very effective. It achieves 99.49% accuracy with flow-based detector, while a graph-based detector has 91.66% detection rate. By using a hybrid of both detectors, BotMark surpasses the performance of each individual detector with a 99.94% detection accuracy. However the graph-based approach makes up for what the C-flow based detector cannot detect by finding certain Zeus bots which are not detected by it. Clearly through hybrid analysis of traffic behaviors based on graphs and flows, identifying botnets becomes both essential and vital [25].

7. Limitation of the Research

Although this research demonstrates significant strides in regard to cybersecurity, one should never ignore its constraints. Among other things, limiting applicability outside more general infrastructure because many of its conclusions are based solely on specific network topologies is just an example. In addition, some techniques used for detecting cyber threats may eventually lose their relevance since they do not keep up with changes in those threats; hence these disadvantages underline why ongoing research is required so that we can secure ourselves against continuous evolving online insecurities by having adaptive and robust defense mechanisms.

8. CONCLUSIONS

In the end, this research is a big leap towards securing digital spaces against constantly evolving cyber threats. The integration of graph-based methods, especially Graph Neural Networks (GNN), provides anomaly detection with unprecedented accuracy and adaptability. Notwithstanding its shortcomings, the research had far-reaching effects. This study combats constraints and takes note of ethical dilemmas thus paving ways for a safer digital tomorrow. Thus, it goes beyond challenging existing beliefs about cybersecurity but also emphasizes persistent innovation, vigilance in ethics and versatility as necessary ingredients for safeguarding our cyber borders.

ACKNOWLEDGEMENT

We gratefully acknowledge the International Journal of Scientific Research in Engineering and Management (IJSREM) for publishing our research paper on "Anomaly Detection in Cybersecurity with Graph-Based Approaches.

REFERENCES

1. Hodge, V.J., Austin, J.: A Survey of Outlier Detection Methodologies. Artificial Intelligence Review 22, 85–126 (2004). https://doi.org/10.1007/s10462-004-4304-y
2. Hofmeyr, S., Forrest, S., Somayaji, A.: Intrusion Detection Using Sequences of System Calls. Journal of Computer Security 6, 151–180 (1999). https://doi.org/10.3233/JCS-980109
3. Barnett, V., Lewis, T.: Outliers in Statistical Data, 3rd edn. J. Wiley & Sons, XVII, 582 (1994). https://doi.org/10.1002/bimj.4710370219
4. Chandola, V., Banerjee, A., Kumar, V.: Anomaly Detection: A Survey. ACM Computing Surveys 41, 1–58 (2009). https://doi.org/10.1145/1541880.1541882
5. Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q.Z., Xiong, H., Akoglu, L.: A Comprehensive Survey on Graph Anomaly Detection with Deep Learning. Journal of LaTeX Class Files, 1–1 (2021). https://arxiv.org/pdf/2106.07178.pdf
6. Chen, X., Wang, S., He, C., Li, Y., Liu, X.: Robust Graph-Based Anomaly Detection for Cybersecurity. arXiv (2023). https://doi.org/10.48550/arXiv.2302.00058
7. Rashid, A.N.M.B., Ahmed, M., Pathan, A.-S.K.: Infrequent Pattern Detection for Reliable Network Traffic Analysis Using Robust Evolutionary Computation. Sensors (Basel) 21(9), 3005 (2021). https://doi.org/10.3390/s21093005
8. Pourhabibi, T., Ong, K.-L., Kam, B.H., Boo, Y.L.: Fraud Detection: A Systematic Literature Review of Graph-Based Anomaly Detection Approaches. Decision Support Systems 133, 113303 (2020). https://doi.org/10.1016/j.dss.2020.113303
9. Pazho, A.D., Noghre, G.A., Purkayastha, A.A., Vempati, J., Martin, O., Tabkhi, H.: A Survey of Graph-based Deep Learning for Anomaly Detection in Distributed Systems. IEEE Transactions on Knowledge and Data Engineering (2023). https://doi.org/10.1109/TKDE.2023.3282898
10. Du, H., Li, D., Wang, W.: Abnormal User Detection via Multiview Graph Clustering in the Mobile e-Commerce Network. Wireless Communications and Mobile Computing 2022, 1–17 (2022). https://doi.org/10.1155/2022/3766810
11. Daniel, G.V., Chandrasekaran, K., Meenakshi, V., Paneer, P.: Robust Graph Neural-Network-Based Encoder for Node and Edge Deep Anomaly Detection on Attributed Networks. Electronics 12, 1501 (2023). https://doi.org/10.3390/electronics12061501
12. Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C., Sun, M.: Graph Neural Networks: A Review of Methods and Applications. AI Open 1, 57–81 (2020). https://doi.org/10.1016/j.aiopen.2021.01.001
13. Luo, L., Fang, Y., Lu, M., Cao, X., Zhang, X., Zhang, W. (2022). GSim: A Graph Neural Network based Relevance Measure for Heterogeneous Graphs. arXiv. https://doi.org/10.48550/arXiv.2208.06144
14. Hui, J. (2021). *Graph Convolutional Networks (GCN) & Pooling.* Medium. Retrieved February 24, 2021, from https://jonathan-hui.medium.com/graph-convolutional-networks-gcn-pooling-839184205692
15. Wekesa, J., Meng, J., Luan, Y. (2020). A deep learning model for plant lncRNA-protein interaction prediction with graph attention. Molecular Genetics and Genomics, 295, 1091-1102. https://doi.org/10.1007/s00438-020-01682-w

16. Zeng, Y., Tang, J. (2021). RLC-GNN: An Improved Deep Architecture for Spatial-Based Graph Neural Network with Application to Fraud Detection. Applied Sciences, 11(5656). https://doi.org/10.3390/app11125656
17. Wang, J., Paschalidis, I. C. (2017). Botnet Detection Based on Anomaly and Community Detection. IEEE Transactions on Control of Network Systems, 4(2), 392-404. https://doi.org/10.1109/TCNS.2016.2532804
18. Zhang, W., Kang, Z., Song, L., Qu, K. (2022). *Graph Attention Interaction Aggregation Network for Click-Through Rate Prediction*. Sensors, 22, 9691. https://doi.org/10.3390/s22249691
19. Wu, C., Wu, F., Lyu, L., et al. (2022). *A federated graph neural network framework for privacy-preserving personalization.* Nature Communications, 13, 3091. https://doi.org/10.1038/s41467-022-30714-9
20. Pourhabibi, T., Ong, K.-L., Kam, B. H., Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decision Support Systems, 133, 113303. https://doi.org/10.1016/j.dss.2020.113303
21. Eberle, W., Graves, J., Holder, L. (2010). Insider Threat Detection Using a Graph-Based Approach. Journal of Applied Security Research, 6(1), 32-81. https://doi.org/10.1080/19361610.2011.529413
22. Wang, C., Zhu, H. (2022). Wrongdoing Monitor: A Graph-Based Behavioral Anomaly Detection in Cyber Security. IEEE Transactions on Information Forensics and Security, 17(11), 2703-2718. https://doi.org/10.1109/TIFS.2022.3191493
23. Wang, W., Shang, Y., He, Y., Li, Y., Liu, J. (2020). BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors. Information Sciences, 511, 284-296. https://doi.org/10.1016/j.ins.2019.09.02
24. Zola, F., Segurola-Gil, L., Bruse, J. L., Galar, M., Orduna-Urrutia, R. (2022). Network traffic analysis through node behaviour classification: A graph-based approach with temporal dissection and data-level preprocessing. Computers & Security, 115, 102632. https://doi.org/10.1016/j.cose.2022.102632
25. Wang, W., Shang, Y., He, Y., Li, Y., Liu, J. (2020). BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors. Information Sciences, 511, 284-296. https://doi.org/10.1016/j.ins.2019.09.024

BIOGRAPHIES

Md Shariar Sozol is currently pursuing a Master of Cybersecurity (Extension) and he has got over a years' professional experience in the cybersecurity industry. He specializes in cryptography and blockchain.

Golam Mostafa Saki has completed his Msc in Engineering Management at University of South Wales, UK.

Md Mostafizur Rahman is currently pursuing a Master of Engineering (Extension) at University of Technology Sydney, Australia.