EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

An Integrated Cybersecurity Defense Framework for Attack Intelligence Analysis, Counteraction, and Traceability in Complex Network Architectures

Hushuang Zeng, Xiangyu Lei*

Guangxi Power Grid Co.Ltd, Nanning, Guangxi province 530000, China

Abstract

INTRODUCTION: In response to the increasingly severe and complex cybersecurity threats posed by advanced persistent threats (APTs) and other sophisticated attacks, this paper proposes an integrated security defense framework for attack intelligence analysis, counteraction, and traceability in complex network architectures. Consolidating threat intelligence from multiple sources that provide different types of intelligence is a major obstacle for the cyber security defense community, particularly when serious challenges arise from complex advanced persistent threats (APTs) involving multiple entities. Inconsistent data formats and methods of structuring data further complicate analyzing the intelligence and creating improved strategies for defense from an all-source intelligence model.

OBJECTIVES: The proposed approach leverages both internal and external threat intelligence sources, standardizes and integrates them into a heterogeneous threat intelligence knowledge graph, and transforms it into a homogeneous representation to facilitate analysis. Here introduces a framework that allows integration of a heterogeneous threat intelligence knowledge graph, Bayesian game theoretic modeling, and a Graph Attention Network (GAT). It is a method that converts multi-source intelligence into a single, homogeneous graph that allows for more informative analysis and a greater adaptive decision-making capacity.

METHODS: To model the strategic interaction between attackers and defenders under incomplete information and resource constraints, we construct a Network Attack-Defense Game Model (NADGM) based on Bayesian game theory and derive the equilibrium strategies using linear programming and Harsanyi transformation.

RESULTS: Furthermore, a graph attention network (GAT) is applied to perform node classification on the threat intelligence reports, exploiting the semantic relations between entities to enhance the accuracy of organization-level attribution. The framework is validated through experiments using real-world APT reports and a case study on ransomware attack-defense scenarios. Experimental results demonstrate that the proposed method achieves superior classification performance, effective strategy optimization, and reasonable attack-defense situation evolution compared to baseline models such as GCN and GraphSAGE. Integrating heterogeneous threat intelligence from diverse sources is a significant challenge in cybersecurity, especially when dealing with complex, advanced persistent threats (APTs). The variation in data formats and structures complicates analysis and defense strategy optimization.

Key Contributions

This paper introduces a framework that integrates a heterogeneous threat intelligence knowledge graph with Bayesian game-theoretic modeling and a Graph Attention Network (GAT). It standardizes multi-source intelligence into a homogeneous graph for improved analysis and adaptive decision-making.

Results

Experimental results show that the proposed framework outperforms traditional models, achieving a classification accuracy of 0.81 for threat intelligence reports. This leads to enhanced detection performance and optimized strategic defense decisions.

CONCLUSION: The findings suggest that integrating threat intelligence, game-theoretic modeling, and graph-based learning can significantly improve the efficiency of threat detection, response, and decision-making in large-scale, complex network environments. The novelty is to integrate a mixed threat intelligence knowledge graph with the application of Bayesian game-theoretic modeling and classifier based on Graph Attention Network (GAT). The classifier leads to a single structured representation of different threat data, recommends defenses that are best and at the same time, enhances the overall detection accuracy across multiple datasets.

Keywords: Threat Intelligence; Advanced Persistent Threat; Bayesian Game Theory; Graph Attention Network; Ransomware; Cybersecurity Defense.

Received on 22 July 2025, accepted on 19 November 2025, published on 03 December 2025

doi: 10.4108/eetsis.9770

*Corresponding author Email: xiangyu_lei25@outlook.com

1. Introduction

With the rapid development of informatization, digitization and intelligence, the cyberspace security situation is becoming increasingly severe. The information system under the complex network architecture has become an important target of all kinds of cyberattacks, and the cyberattacks present the characteristics of persistence, concealment and diversification, especially the attacks represented by Advanced Persistent Threat (APT), which has shifted from the traditional short-term damage to the long-term lurking, continuous infiltration and multi-dimensional strikes [1]. APT attacks are usually highly organized, targeted, and strategic, posing serious threats to the confidentiality, integrity, and availability of information systems and greatly increasing the difficulty of network defense. Therefore, how to quickly and accurately discover, counteract and trace network attacks based on limited defense resources, and build a dynamic and efficient network security protection system has become an important topic in current network security research [2,3]. Among many security protection technologies, Threat Intelligence (TI) has become a key component of situational awareness and proactive defense as an important basis for supporting security decisions. According to Gartner definition, Threat Intelligence is evidential knowledge about existing or potential threats to IT and information assets, including context, mechanisms, identifiers, implications, and actionable recommendations [4]. It covers multi-dimensional information such as attack sources, exploited vulnerabilities, attack targets, attack tactics, techniques and processes (TTPs), etc., which helps security managers to keep abreast of the attack dynamics, optimize the defense strategy, and improve the response capability. Threat intelligence sources mainly include external commercial or open-source threat intelligence and data accumulated by the organization itself, which are complementary to each other and are applied in a synergistic manner. Currently, in order to achieve the standardization, efficient sharing and circulation of threat intelligence, academia and industry have proposed a variety of format standards, such as STIX, CyboX, TAXII, MAEC, CAPEC, OpenIOC, etc., which are used for the description of threat behaviors, computer observable objects, automated exchanges, malware characterization, classification of attack modes, and IOC sharing, etc. [5]. These standards lay a technical foundation for multi-party collaborative defense, effectively enhancing the usability and practicality of threat intelligence.

Although threat intelligence plays an important role in enhancing security protection, it still faces a number of challenges in a complex network environment. First, the long-term and covert nature of APT attacks leads to the lag and incompleteness in the acquisition, updating and utilization of threat intelligence; second, the heterogeneity and redundancy of threat intelligence affects its readability and executability; in addition, there are large differences in the willingness and ability of different organizations to share threat intelligence, which further restricts the effectiveness of its application. Therefore, only relying on threat intelligence itself is not enough to support the global optimal defense strategy, which needs to be combined with game theory and intelligent algorithms to achieve dynamic attack and defense game analysis, strategy optimization and behavioral traceability [6,7].

To address the above problems, in recent years, researchers have tried to introduce game theory into network attack and defense modeling, and proposed a variety of attack and defense game models to portray the strategy choices and evolution laws of attackers and defenders under resource-limited conditions. Models such as non-cooperative static game, dynamic game, Stackelberg game, and evolutionary game are widely used in cyber security scenarios [8]. Among them, the Bayesian game model based on incomplete information (NADGM) can effectively deal with the strategy game under the environment of unknown types of attackers and defenders and incomplete information, and has been proved to be suitable for complex threat scenarios such as APT [9]. However, most of the existing game models stay at the level of theoretical analysis and lack integration with real threat intelligence data; they rely on static assumptions in the quantification of gains, making it difficult to dynamically reflect changes in attack and defense dynamics; and they also lack support for attack behavior traceability and inter-node relationship modeling, which restricts their utility and scalability in large-scale complex network environments [10].

In recent years, Graph Neural Network (GNN) has made significant progress in the fields of social networks, recommender systems, knowledge graphs, etc., providing an effective tool for portraying node relationships and structural information in complex networks. In particular, the GAT model based on the attention mechanism can dynamically calculate the weights among nodes, distinguish the importance of different neighbors, and improve the accuracy and robustness of node feature learning [11]. Some work has been done to apply GNN to the field of network security for tasks such as traffic categorization, malicious domain name detection, intrusion detection, etc., and achieved good results [12]. However, most of the existing researches target isomorphic or single threat scenarios, lack of unified modeling and classification capabilities for heterogeneous threat intelligence networks, and do not fully combine game theory to achieve the organic combination of attack and defense behavior analysis and traceability[13][14].

The novelty of the study is with the integration of a heterogeneous threat intelligence knowledge graph, Bayesian game theory, and a GAT-based deep learning model for threat analysis and defense optimization. In contrast to existing models that only model either detection or representation but not both, our method allows for standardization of multi-source intelligence for a homogeneous graph representation, where adaptive defense strategies are modeled using Bayesian Nash Equilibrium. This then improves decision-making, reduces heterogeneity across threat intelligence, and enhances classification performance against sophisticated cyberattacks. To this end, this paper proposes an integrated network security protection system for attack intelligence analysis, attack behavior countermeasure and traceability for complex network architecture.

The experimental results show that the method in this paper is better than the existing methods in terms of heterogeneous processing of threat intelligence, accuracy of node classification, balance of gaming strategies and rationality of posture evolution, and can effectively improve the threat detection, response and protection capabilities in complex network environments. The research in this paper provides a feasible theoretical framework and engineering realization path for the construction of complex network security protection system, which is of great theoretical significance and application value for improving the security level of cyberspace and coping with persistent advanced threats [15].

The primary contributions of this research are highlighted as follows. We develop a combined security defense architecture for complete attack intelligence analysis, response and traceability across complex network topologies. The proposed architecture also normalizes and feeds external and internal threat intelligence into a multi-layered threat intelligence knowledge graph, and subsequently converts the graph into a more uniform representation that supports improved interoperability and analysis. Additionally, a Bayesian game-theoretic model is proposed to engage dynamic attacks with the aim of extracting the best response strategies, leading to a level of responses by equilibrium. We present Graph Attention Network (GAT) methods for node representation and improved threat categorization. The proposed method presents and resolves how we have demonstrated it significance and utility during stringent and comparitive experimental analysis in experimentation against other state-of-the art methods, and within comparative evaluation of several datasets, in addition to ransomware datasets. The framework is technically robust, using a Bayesian game theory model for attack-defence interactions, deriving computable optimal strategies through Bayesian Nash Equilibrium. Thus, rational defensive decision-making occurs in an uncertain world, reflecting a realistic representation of opponent/model condition. The ability to combine these two apparatus of game-theoretic analysis, and a knowledge graph representation provides theoretical strength, alongside potentially reasonable defensive capacity, of the mechanism of defense we have proposed.

The unique contribution of this research lies in its combination of heterogeneous threat intelligence, Bayesian game-theoretic defense modeling, and graph neural networks learning into one framework. The inclusion of heterogeneous threat intelligence data in a homogeneous knowledge graph addresses data inconsistencies and ameliorates interoperability among heterogeneous data sources. Other modeling approaches, Bayesian games, allow for a more strategic flexibility that enables defenders to change their defensive measures during the defense. Empirical studies over various threat datasets show that the proposed framework generates higher detection accuracy and strategic robustness than comparably.

2. Related Works

A method based on Convolutional Neural Networks (CNNs) has been proposed for the detection of previously unseen attacks in IoT networks at the edge. The data presented supports the idea that automated feature extraction from network traffic is a requirement for effective detection of threats [16]. Using clustering in combination with sequence learning allowed for a more effective intrusion detection method with a reduction in false positives. This demonstrates the effectiveness of combining diverse types of data analysis for threat intelligence [17].

A knowledge graph can illustrate vulnerabilities and aid in risk assessment, and a case example showed that threat was modeled in a structure and therefore allows for automated analysis and decisions to be made by the analyst [18]. In addition, BiLSTM type networks are valuable for modeling temporal behavioral patterns for insider threat detection. This illustrates the importance of well processed and structured data in order to support types of solutions based on analytics [19]. Recent progress in threat intelligence integration and cybersecurity defensive models have reinforced the requirement for improved models and frameworks in cybersecurity. A review of AI-assisted methods for bolstering spear-phishing defense indicates a growth in the implementation of machine learning models within cybersecurity defenses [20]. A digital forensic framework for preserving data privacies during investigative processes reflects secure data manipulations and considerations of privacy in threat intelligence contexts [21].

On the other hand, a framework for the dynamic risk assessment and analysis of large-scale cyber-physical systems parallels our approach in the application of advanced frameworks to risk assessment and mitigation in cybersecurity [22]. Each study pointed to the need for new advanced models and frameworks (i.e., AI and risk assessment frameworks) to be layered into models and frameworks for cybersecurity.

Leveraging artificial intelligence to improve advanced threat detection approaches, the cited work adds to cloud security. In this instance, the AI method was applied in an overall cybersecurity defense framework, developed resiliently through machine learning and threat intelligence analysis, to present proactive responses and traceability. This allows for more consistent methods of proactive and reactive threat detection and increases effectiveness in responding to threats, which improves the security posture of a complex network architecture [23].

3. Threat Intelligence

3.1 Overview of Threat Intelligence

Threat intelligence is evidence-based information to assist organizations to identify, understand, or respond to cyber threats that are real and/or a potential threat. Gartner describes threat intelligence as contextual information, mechanisms, indicators, implications and actionable advice, that can assist in decision-making and technical response to cyber threats [24,25]. In general, threat intelligence includes information which illustrates profiles of attackers, systems or software vulnerabilities, assets affected, and tactics, techniques, and procedures (TTPs) used to conduct the attack [26,27]. This information is valuable in developing a robust cybersecurity situational awareness program, supporting the organizations' ability to be proactive in detecting, anticipating, and responding to complex threat activity.

Threat intelligence consists of internal threat intelligence or external threat intelligence, depending on the source of information. Internal threat intelligence is information created by the organization, which consists of logs, alerts from security events, and the analysis of behavior and systems to determine whether there is risk internally in the infrastructure. External threat intelligence is obtained from the larger security community, various information-sharing organizations, or third-party vendors. Thus, external threat intelligence shares intelligence about attack patterns, APT group behaviors, vulnerabilities currently being exploited, etc., across their industry. Figure 1 shows the way threat intelligence is classified.

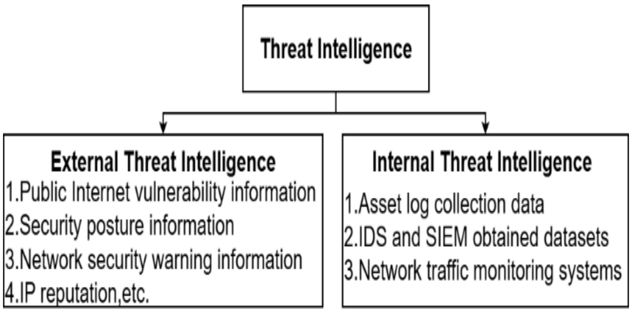
Threat Intelligence
External Threat Intelligence
1.Public Internet vulnerability information
2.Security posture information
3.Network security warning information
4.IP reputation,etc.
Internal Threat Intelligence
1.Asset log collection data
2.IDS and SIEM obtained datasets
3.Network traffic monitoring systems

Figure 1. Sources of Threat Intelligence

3.2 Threat Intelligence Standardization

The use of threat intelligence in cybersecurity frameworks and applications is primarily based upon its ability to be shared and understood among systems and organizations. The method of sharing and automatically processing threat intelligence exists in a shared or standard format and communication protocols. To date, several open standards have been widely accepted within industry-level organizations to provide a standard format to share and analyze threat intelligence [28].

STIX (Structured Threat Information Expression) is a standardized language that is widely accepted for the description of cyber threat information. It is a comprehensive data model that accounts for core components in cyber threat modeling including threat actors, attack techniques, exploited vulnerabilities, malware properties, paths of intrusion, and other key considerations. STIX can be represented in both XML and JSON, so there is semantic interoperability across various platforms.

CyboX (Cyber Observable Expression) defines observable behaviors within networks and systems. Some accessible examples include file access, registry changes, and network communications [29]. CyboX specifies technical accuracy for forensic analysis, log inspection, or event reconstruction. TAXII (Trusted Automated eXchange of Indicator Information) is the standard protocol for the sharing of STIX data [30]. It is built on HTTPS, and supports secure peer-to-peer information sharing exchanges, through pull, push, and subscriptions, thus making it more suitable for organizations to share information with greater frequency.

MAEC (Malware Attribute Enumeration and Characterization) allows for a standardized language to communicate malware characteristics and behavior, lessening reliance on traditional signature-based methods [31]. CAPEC (Common Attack Pattern Enumeration and Classification) provides a structured repository of known attack patterns, facilitating defender understandings of attacker behaviors and situational analysis of possible mitigations. OpenIOC increases machine-readability and efficiency to recall indicators of compromise with logically arrange groups of indicators.

As the existence of advanced persistent threats (APTs) increases and as APTs are concealed, preferable, and enduring, threat intelligence systems must prove capable of versatility. Different from those of other threats, an APT campaign will behave similarly overtime when it is targeting specific industries. And eventually, aggregated intelligence data can create multidimensional threat profiles just as would a consideration of time or evidence or anything else, of course, to present dynamic relationships of threat intelligence in service of detection models or rapid real-time updates.

Thus, the standardization of those threat intelligence systems enables not only immediate incident response but a greater understanding of complex attack movies. It can be said that by creating structured and effective distributed intelligence to share incidental information by industry, we can improve coordinated defense capabilities among organizations and platforms. Again, it is critical understand unified and standardized threat intelligence protocols will create intelligent, precise and resilient defenses in cybersecurity systems [32,33].

4. Modeling Network Attack and Defense Games and Solving Equilibrium

4.1 Construction of the Network Attack-Defense Game Model

In order to effectively represent panning interaction between Attacker and Defender in cyberspace, it is necessary to develop a credible game-theoretic model. In actual network security situations, both adversaries have constraints on factors such as available resources, technical capabilities, and risk preference. Therefore, to maximize their respective payoffs, the adversaries will select strategies that best suit their preferences or capabilities of attack or defence. As a result, the adversarial interaction can be represented as a static non-cooperative Bayesian game informed of some prior incomplete information.

Definition: A Network Attack-Defense Game Model (NADGM) is formally defined as a 7-tuple:

$$\text{NADGM} = (N, S, \Theta, P, T, x(t), U) \qquad (1)$$

Where: N={A,D}: The set of players, including the attacker A and defender D; $S = S_A \times S_D$: The strategy space, where $S_A$and $S_D$are the respective strategy sets for the attacker and defender; $\Theta = \{\theta_A, \theta_D\}$: The type space representing incomplete information; P(θ): The prior probability distribution over types; T: The system transition function that describes state changes under given strategies; x(t): The system state at time t; $U = (U_A, U_D)$: The utility functions for the attacker and defender.

The utility functions for both players can be expressed as:

$$U_D(s_A, s_D) = R_D(s_A, s_D) - C_D(s_D) \qquad (2)$$

Where $R_A$and $R_D$are the payoffs for the attacker and defender under a given strategy combination, andC_A, $C_D$represent the associated costs of executing their strategies.

To find the optimal strategy combination, the Bayesian Nash Equilibrium (BNE) is introduced. At equilibrium, neither player has an incentive to unilaterally deviate from their strategy. The strategy pair (s_A^*, s_D^*) satisfies:

$$U_A(s_A^*, s_D^*) \geq U_A(s_A, s_D^*), \forall s_A \in S_A U_D(s_A^*, s_D^*) \geq U_D(s_A^*, s_D), \forall s_D \in S_D \quad (3)$$

At this stage, both sides attain strategic stability despite having asymmetric information.

Thus, the framework is technically accurate because it uses a Bayesian game theory model to analyze attack-defend interactions and determine the best strategies through a Bayesian Nash Equilibrium. In short, defensive decision-making follows a rational basis under uncertainty, so this reflects real adversarial conditions. The alignment of game-theoretic analysis and knowledge graph representation yields theoretical strength and potentially reasonable defensive capacity for the proposed defense mechanism.

The transformation of a homogeneous knowledge graph from a heterogeneous knowledge graph entails the relationship mapping of distinct entities, such as malware, IP addresses, and methods of attack. The parameters to generate direct connections between nodes are using factors such as semantic proximity (relatedness of nodes), commonality of entities (such as shared techniques used for attack or IPs), and threshold values for edge creation. The resulting homogeneous graph reduces the complexity of threat intelligence and makes the analysis of this intelligence more effective.

4.1.1 Game-Theoretic Modeling

Game theory provides a mathematical framework for studying a particular class of strategic interactions where the outcomes depend on the actions of multiple agents. In cybersecurity, the interaction between an attacker and defender is one of many examples of a game-theoretic scenario. In this situation, each player chooses a strategy based on the information available to them and the strategies they believe will be selected by the other player(s).

The Bayesian Nash Equilibrium (BNE) is a solution in which each player selects the best strategy for themselves given the strategy of the other player taking into account that neither player has complete information regarding the type or behavior of the other. In this context, both the attacker and defender will select a baseline action to implement their respective strategies according to their subjective perception of the opponent's type and actions. The Bayesian Nash Equilibrium guarantees that given the potential actions of the other player, neither player can change his action unilaterally and increase his payoff.

4.2 Game Equilibrium Solving

In cyber-attack and defense modeling, benefit In modeling cyber-attack and defense games, the quantification of benefits forms the basis for solving the game equilibrium. In order to determine the optimal strategies, it is necessary to build models that efficiently quantify the expected payoffs for both attackers and defenders when different combinations of strategy options are taken into account. In recent years, many researchers have adopted quantitative methods to define the payoffs in cybersecurity games. One widely used framework is based on the approach proposed in [34], which systematically classifies payoff factors.

The commonly used payoff indicators include:

- **System Loss Cost (SLC):** This represents the total damage suffered by the target system when an attack succeeds and the defense fails. It is denoted asSLC(D_i, A_j), where $D_i$and $A_j$are the strategies selected by the defender and the attacker, respectively.
- **Attack Gain (AG):** Typically equivalent to the damage caused by a successful attack, i.e.,$AG = SLC$.
- **Defense Gain (DG):** Refers to the avoided loss due to successful defense, representing the benefit of preventing an attack.
- **Attack Cost (C_a)** and **Defense Cost (C_d):** These reflect the resource expenditures associated with each strategy, including computation, manpower, or other overhead costs.

Since attackers and defenders incur different costs and achieve different gains when strategies are executed, the cyber-attack-defense game model falls into the category of non-zero-sum games. To capture the net payoffs for each party under every strategy pair, the following utility functions are defined:

$$U_A(A_j, D_i) = \mathrm{AG}(A_j, D_i) - C_a(A_j) \qquad (4)$$

Defender's Net Payoff:

$$U_D(D_i, A_j) = \mathrm{DG}(D_i, A_j) - C_d(D_i) \qquad (5)$$

By solving for a strategy pair (A_j^*, D_i^*) that satisfies the Nash Equilibrium condition, one can identify an optimal solution where neither side has an incentive to unilaterally change their strategy.

This method captures the dynamic nature of adversarial interactions in real-world network environments and provides a quantitative foundation for designing intelligent defense strategies.

4.3 Transformation and Equilibrium Solution of Incomplete Information Static Game

In order to solve the equilibrium of a static game with incomplete information, the Harsanyi transformation is employed. This technique introduces a fictitious player—Nature—to probabilistically assign types to players before the game begins. By doing so, the original incomplete information game is transformed into a Bayesian game with complete but imperfect information, making it tractable for equilibrium analysis using standard game-theoretic methods.

Assume that the defender can be of three possible types, denoted by $\theta_D^{(1)}, \theta_D^{(2)}, \theta_D^{(3)}$Each reflects different defensive capabilities or strategic preferences. These types are selected by Nature with probabilities:

$$P\left(\theta_D^{(1)}\right) = p_1, \quad P\left(\theta_D^{(2)}\right) = p_2,$$
$$P(\theta_D^{(3)})p_3, \quad \text{where } p_1 + p_2 + p_3 = 1 \qquad (6)$$

Each defender type $\theta_D^{(i)}$ is associated with a specific strategy set $S_D^{(i)} \subseteq S_D$, and may differ in cost, effectiveness, or risk tolerance.

For a given strategy profile$(s_A, s_D^{(i)})$, the expected utility for the attacker is computed as:

$$\mathbb{E}_{\theta_D}[U_A(s_A, s_D)] = \Sigma_{i=1}^{3} \quad p_i \cdot U_A(s_A, s_D^{(i)}) \qquad (7)$$

Similarly, the defender of type $\theta_D^{(i)}$ selects a strategy $s_D^{(i)}$ to maximize its own utility function:

$$U_D^{(i)}(s_A, s_D^{(i)}) = R_D^{(i)}(s_A, s_D^{(i)}) - C_D^{(i)}(s_D^{(i)}) \qquad (8)$$

The solution concept is a Bayesian Nash Equilibrium (BNE), defined as a strategy profile:

$$(s_A^*, s_D^{*(1)}, s_D^{*(2)}, s_D^{*(3)}) \qquad (9)$$

such that:

$$s_A^* \in \arg\max_{s_A \in S_A} \mathrm{E}_{\theta_D}[U_A(s_A, s_D^*)]$$
$$1{,}2{,}3 s_D^{*(i)} \in argmax \quad _{s_D \in S_D^{(i)}} U_D^{(i)}(s_A^*, s_D) \qquad (10)$$

This framework ensures that each player—while not knowing the exact type of the opponent—selects a strategy that maximizes their expected payoff, taking into account the probabilistic distribution of types assigned by Nature.

5. Node Classification Based on Graph Attention Mechanism

This study focuses on shallow representation learning using a graph attention mechanism on a constructed heterogeneous threat intelligence graph in order to classify the nodes of the threat intelligence reports by organization. Recently, with the emergence of graph neural networks (GNNs), which have shown significant advances in heterogeneous graph modeling, there have been many heterogeneous GNN models. However, differences in data preprocessing and evaluation methods has often led to the unfair underestimation of many classical homogeneous models, such as G N N [35].

Prior research has shown that properly structured input features can allow classic traditional models to outperform some of the more complicated heterogeneous models. Consequently, in this study, we use a homogeneous standard graph attention (GAT) mechanism because of its simplicity and effectiveness. The GAT model assigns different attention weights dynamically to different neighboring nodes to increase accuracy of node representation in threat intelligence networks that include rich attributes associated with nodes data and require a complex heterogeneous structure.

By framing the node classification task as a supervised learning task on the graph, we train the attention based model to discern structural dependencies and semantic relationships among organizational threat intelligence nodes to classify nodes that the model has yet seen.

5.1 Mapping Heterogeneous Networks to Homogeneous Networks

After the construction of the threat intelligence knowledge graph, rather than ending up with a heterogeneous information network that has nine different entity types (the nodes), counting the semantic relationship (the edges), each edge is a semantic relationship and each node is a specific element to threat intelligence. Among them, the threat intelligence report nodes are designated as the classification targets in this study.

In order to utilize homogeneous graph-based models (e.g., GAT), the heterogeneous network needs to be transformed to a homogeneous version. This is achieved by projecting indirect relationships between report nodes into direct links. In particular, when two threat intelligence report nodes are connected, either directly or through intermediate nodes (e.g., vulnerabilities, IP addresses, malware samples), to the same threat-related entity, an edge is added between both of those report nodes. This process preserves semantic proximity and threat-relevance [36].

As shown in Figure 2, the original heterogeneous threat graph (left) has multiple node types shown in different colors, and the blue nodes indicate the report nodes that we would like to classify. Through a mapping process, the network is then converted to a homogeneous graph (right) that retains only the report nodes that are now directly connected due to relationships with threat-related elements. This conversion facilitates the application of homogeneous graph neural networks for downstream classification tasks while preserving key structural and semantic information.

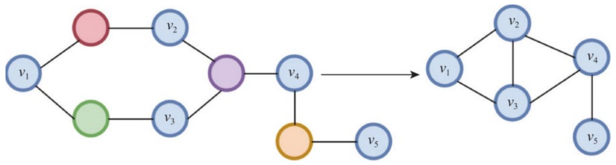

Figure 2. Mapped to homogenous networks are heterogeneous threat intelligence networks.

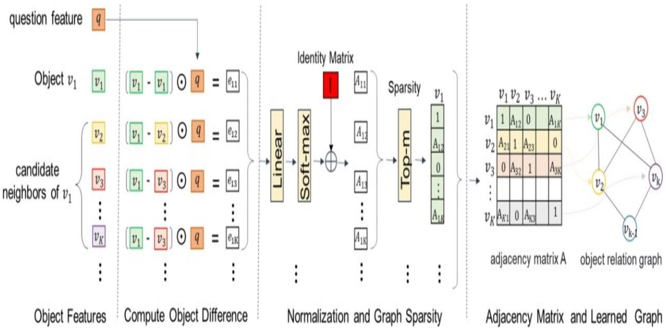
question feature
q
Object v_1
candidate neighbors of v_1
$(v_1 - v_1) \odot q = e_{11}$
$(v_1 - v_2) \odot q = e_{12}$
$(v_1 - v_3) \odot q = e_{13}$
$(v_1 - v_3) \odot q = e_{1K}$
Identity Matrix
Linear
Soft-max
A_{11}
A_{12}
A_{13}
A_{1K}
Sparsity
Top-m
v_1
1
A_{12}
0
A_{1K}
v_1 v_2 v_3 ... v_K
adjacency matrix A
object relation graph
Object Features
Compute Object Difference
Normalization and Graph Sparsity
Adjacency Matrix and Learned Graph

Figure 3. Question-Guided Sparse Object Relation Graph Construction

Figure 3 illustrates the process of constructing a sparse object-relationship graph based on the problem feature q and object features$\{v_1, v_2, \ldots, v_K\}$. First, for the target object $v_1$and its candidate neighbors$\{v_2, v_3, \ldots, v_K\}$, the object differences are computed and interacted with the problem features to obtain the edge-weighted representations$e_{1j} = (v_1 - v_j) \odot qe_{1j}$, where $\odot$denotes the element-by-element product. Subsequently, $e_{1j}$is linearly transformed and the unit matrix II is added, and the weights $A_{1j} = \text{Softmax}(We_{1j} + I)$ are obtained by softmax normalization. In order to ensure the sparsity of the graph, only the neighbors with the top mm of connection weights of each node are retained, and the rest of the weights are set to zero. By repeating the above operation for all nodes, the final adjacency matrix A is formed, where each element A_{ij}denotes the relationship weight between node $v_i$and nodev_j. The corresponding sparse graph structure of this adjacency matrix is the learned object-relationship graph, which is used to model the semantic association between nodes.

5.2 Node Vector Initialization

Once the threat intelligence report nodes are embedded within a homogeneous network structure, the next step is to assign each node an initial feature representation that can be utilized in subsequent attention-based learning. This initialization process involves encoding each node's attributes into a numerical vector form.

Assume the threat intelligence report nodes are denoted as$V = \{v_1, v_2, \dots, v_n\}$, where n is the total number of report nodes. Each node v_i is associated with a set of attributes A_i , such as report timestamp, threat source, severity level, associated malware, etc.

These attributes are embedded into a fixed-dimensional feature space using one-hot encoding for categorical features and normalization for continuous features. The resulting feature vector for node v_i is denoted as:

$$\boldsymbol{h}_i^{(0)} = \mathrm{Embed}(A_i) \in \mathbb{R}^d \qquad (11)$$

where d is the dimension of the input feature space and $\boldsymbol{h}_i^{(0)}$ is the initial representation of node v_i.

When attribute fields are absent or limited, it may be beneficial to either zero-pad to equalize dimensionality or use masked attention while keeping dimensionality consistent across inputs. The feature matrix H^((0)) for the entire graph is represented as:

$$H^{(0)} = [\boldsymbol{h}_1^{(0)}, \boldsymbol{h}_2^{(0)}, \dots, \boldsymbol{h}_n^{(0)}]^T \in \mathbb{R}^{n \times d} \qquad (12)$$

$H^{(0)}$ serves as the matrix input via the graph attention, which allows nodes to learn rich representations by capturing structural and contextual similarity values in the threat intelligence graph. When building the threat intelligence knowledge graph, some entity nodes, such as IP addresses, hash values, etc., do not have an intrinsic degree of semantic meaning and are often made up of solely numbers and symbols, so their initial vectors are mostly random, which limits the representation capabilities of the model altogether. To improve the semantic quality of node representation, the focus of this research to use several feature enrichment strategies from external sources, based on attributes contextually derived from entities (e.g. malware sample, ip address, domain name, etc.). For example, if a domain (e.g. maliciousdns.com) is tagged as a phishing or remote-access malicious artifact, then that meaning can be depicted within the contextual label(s) attributes in the node’s vector representation. For malware samples, behavioral attributes values (e.g. ransomware, remote-access tool, etc.) contextually depicted via malware analysis would exhibit a behavioral trait in order to contextualize the malware entity node's behavioral attribute(s).

In the construction of vector representations for threat intelligence report nodes, this study explicitly incorporates semantic vectors of five high-value entity types (attacks tools, malware, IP addresses, domain names, and tactics/techniques) to the feature aggregation process. This approach effectively adds semantics to structurally defined entities and also significantly increases the discriminative power and semantic breadth of the nodes' representations, providing a solid base for downstream classification and analysis tasks.

5.3 Node Classification Using Homogeneous Graph Attention Mechanism

The Graph Attention Network (GAT) is used to better incorporate the algorithms latent semantic features of nodes performed in the classification of the threat intelligence report nodes. The idea is to simply augment the message passing process and incorporate attention weights; in other words, some neighbors contain more relevant information to represent the target node than others, and thus the overall embedding of the node improves [37].

The steps included in the GAT, are as follows: given a target node, the neighbors impart not only structural context but additionally, multi-dimensional semantic information. The attention mechanism will learn the strength of association between the target node and neighboring nodes dynamically, quantifying these influences in attention coefficients. Each attention coefficient is applied in a weighted sum of neighbor features to refine message passing and aggregation of features.

Refer to the illustration in figure 4, where the red node is the specific target node to be classified, and the blue nodes are neighboring nodes. The graph attention model provides an augmented level of precision in the node embedding, and therefore, in the threat intelligence report node classification. The GAT is particularly efficient in terms of adaptability and scalability when working with complex graph connectivity and heterogeneous attributes..

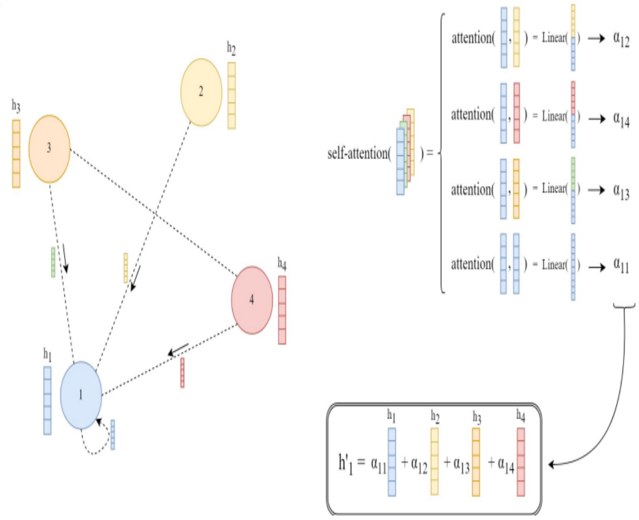
h2
h3
2
3
4
h4
h1
1
self-attention( )=
attention(,) = Linear( ) → α12
attention(,) = Linear( ) → α14
attention(,) = Linear( ) → α13
attention(,) = Linear( ) → α11
h1 h2 h3 h4
h'1 = α11 + α12 + α13 + α14

Figure 4. Graph attention mechanism message aggregation schematic diagram

In a GAT, to enhance the representation capability of a target node, the input features are first linearly transformed and projected into a higher-dimensional feature space. Let the input feature of node ii be$\boldsymbol{h}_i \in \mathbb{R}^F$; it is transformed using a weight matrix $\boldsymbol{W} \in \mathbb{R}^{F' \times F}$as follows:

$$\boldsymbol{h}_i' = \boldsymbol{W}\boldsymbol{h}_i \tag{13}$$

Next, to reflect the varying importance of neighboring nodes in determining the target node's representation, an attention mechanism is introduced. For the target node ii and its neighbor j, the unnormalized attention coefficient is computed as:

$$e_{ij} = \text{LeakyReLU}(\mathbf{a}^T[\boldsymbol{h}_i' \| \boldsymbol{h}_j']) \tag{14}$$

where $\boldsymbol{a} \in \mathbb{R}^{2F'}$is a learnable attention weight vector, and ∥ denotes concatenation.

The attention coefficients are then normalized using a softmax function over all neighbors of node i:

$$\alpha_{ij} = \frac{exp(e_{ij})}{\sum_{k \in \mathcal{N}(i)} \quad exp(e_{ik})} \tag{15}$$

Finally, the updated feature representation of the target node is computed by aggregating the features of its neighbors, weighted by their attention scores:

$$\boldsymbol{h}_i'' = \sigma\left(\sum_{j \in \mathcal{N}(i)} \quad \alpha_{ij}\boldsymbol{h}_j'\right) \tag{16}$$

where σ (·) is an activation function, typically ELU or ReLU.

This mechanism allows GAT to capture the diverse contributions of neighboring nodes to the target node representation, improving performance on tasks such as node classification.

Multi-head attention is additionally a mechanism introduced in Graph Attention Networks (GAT) that enhances representation capacity by leveraging different perspectives on neighbor contributions. Through this mechanism, the model can learn several feature representations for the target node simultaneously, with each representation being learned from its own attention head. Next, the feature representations collectively inform a better node embedding.

Specifically, let us consider K attention heads. The attention head k will learn a weight matrix W((k)) and an attention vector a((k)) independently of the other attention heads. The new representation of node iii, from the k-th attention head is as follows:

$$\boldsymbol{h}_i^{(k)} = \sigma\left(\sum_{j \in \mathcal{N}(i)} \quad \alpha_{ij}^{(k)}\boldsymbol{W}^{(k)}\boldsymbol{h}_j\right) \tag{17}$$

where $\alpha_{ij}^{(k)}$ is the attention coefficient of neighbor j to target node iii under the k-th head, and σ (·) is a non-linear activation function (e.g., ReLU or ELU).

Finally, the outputs of all attention heads are averaged to obtain the final embedding of the target node:

$$\boldsymbol{h}_i = \frac{1}{K}\sum_{k=1}^{K} \quad \boldsymbol{h}_i^{(k)} \tag{18}$$

This approach effectively integrates information from multiple attention channels, improving the expressiveness and robustness of node representations—particularly beneficial in complex and attribute-rich graph data such as threat intelligence networks for report node classification.

Figure 5 depicts the structured framework of the homogeneous graph attention mechanism model. The model input is the node feature matrix $\boldsymbol{X} \in \mathbb{R}^{N \times F}$, where N is the number of nodes and F is the dimension of the original node features. The original nodes representations $\boldsymbol{H}^{(0)}$ is produced after an embedding transformation and then fed to the first layer of the GAT.

At each layer, the model computes a linear transformation on its given node and neighbours, and computes the attention coefficients to measure the importance of its neighbours for the feature update of each node. Formally, the attention coefficient α_ijrepresents the relevance of a neighbouring node j for the feature update of a node ii, for any $j \in \mathcal{N}(i)$. The attention coefficients are then used to update the features of the neighbouring nodes to obtain updated node representations$\boldsymbol{H}^{(1)}$. The application of the attention mechanism can then be applied in multiple layers in order to obtain higher level structural and semantic features.

After several attention layers, the final output is the node embedding matrix$\boldsymbol{Z} \in \mathbb{R}^{N \times F'}$, where F′F' is the output feature dimension. This representation is suitable for downstream node-level tasks such as classification or clustering. A fully connected layer followed by a softmax classifier is then used to predict the class label for each node representation$\boldsymbol{z}_i$:

$$\hat{y}_i = \text{softmax}(\mathbf{W}_{\text{cls}} \cdot \boldsymbol{z}_i + \boldsymbol{b}) \tag{19}$$

where $\boldsymbol{W}_{\text{cls}}$and $\boldsymbol{b}$are trainable parameters of the classifier. This model effectively integrates both graph structure and node attributes to enable accurate classification of threat intelligence report nodes.

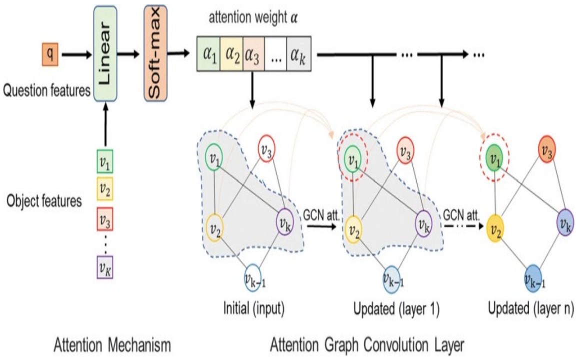

Figure 5. Model of isomorphic attention mechanism

6. Experiments and Results

This section describes the dataset and experimental setup, and conveys the nature of the experiments and the results. The experimental results suggest that the GAT was a better detection model than any of the models as experiments were run to detect threats. When we used it to test against ransomware data, it had a higher level of accuracy than the other models, which suggests that the GAT-based model was superior in treating difficult cyber threats.

6.1 Dataset

For the purposes of this study, we used a publicly available dataset compiled by a university-affiliated cybersecurity research lab, and that consists of threat intelligence reports on APT (Advanced Persistent Threat) attacks. The dataset contains multiple entity types and relationships, thereby creating a complex and well-defined heterogeneous threat intelligence knowledge graph. The raw data offers the following core data points:

- **Threat Intelligence Reports (Report):** Descriptive documents released by security vendors about APT attacks.
- **IP Addresses (IP):** Addresses of attack sources or suspicious servers mentioned in the reports.
- **Domains (Domain):** Command-and-control (C&C) server domains associated with APT campaigns.
- **Malware Samples (Malware):** Extracted malicious codes or tools referenced in reports.
- **Techniques/Tactics:** Behaviors labeled according to the MITRE ATT&CK framework.
- **File Hashes, Attack Groups, URLs,** and other auxiliary elements.

Data Processing:

- After constructing the heterogeneous knowledge graph, it is mapped into a homogeneous graph containing only the "Threat Intelligence Report" nodes as classification targets Table1;
- Edges are established between nodes that share common threat elements;
- Textual entities are vectorized using Word2Vec for attribute initialization;
- The resulting graph contains 3,526 nodes and 21,045 edges.

Table 1. Sample entities and attributes in the threat intelligence dataset

Report ID	Report Name	Malware	IP Address	Domain	Technique (ATT&CK)	Category (Label)
R001	APT29 Campaign	CobaltStrike	104.26.12.91	fsportal.net	T1071: Application Layer	State-Sponsored
R002	Lazarus Target Bank	WannaCry	185.92.73.44	myupdate.info	T1204: User Execution	Financial APT
R003	OceanLotus Activity	PlugX	43.250.56.89	gov-update.net	T1059: Command-Line Interface	Government APT

6.2 Experimental Environment

The model proposed in this study was implemented using PyTorch in the Python environment. The hyperparameters configured for the model training are summarized in Table 2, with detailed explanations as follows:

- **seed:** The random seed number used to ensure reproducibility of results.
- **weight_decay:** The weight decay coefficient applied as a regularization parameter to prevent overfitting.
- **nb_head:** The number of attention heads utilized in the graph attention mechanism.
- **α (alpha**): The regularization hyperparameter that regulates the penalty term in the loss function.
- **lr (learning rate):** The optimizer's initial learning rate that is set for training.
- **hidden:** The size of the hidden layer embeddings in the neural network.
- **dropout:** The dropout rate, which indicates the number of neurons that are randomly turned off during training to help prevent overfitting.
- **patience:** The number of epochs that training is allowed to continue without having any improvement before stopping the process early.

The goal of this configuration is to find the right point between model complexity and generalization ability while at the same time optimizing the efficiency of the training process. The empirical tuning and validation on the training dataset were the basis for the selection of these hyperparameters.

Table 2. Model Hyperparameter Settings for the GAT Implementation

Parameter	Value	Description
seed	42	Random seed
weight_decay	0.0005	Weight decay factor

nb_head	8	Number of attention heads
α (alpha)	0.2	Regularization parameter
lr	0.01	Learning rate
hidden	64	Hidden layer dimension
dropout	0.5	Dropout rate
patience	50	Number of epochs to stop training

6.3 Model Analysis of the Proposed Method

This section examines the performance of the proposed approach from these three primary measurements: the impact that static feature extraction from malicious code has on classification performance, the effect of varying the number of attention heads in the GAT model, and the overall effectiveness of the method on the threat intelligence report classification.

6.3.1 Importance of Extracting Malicious Code Attributes

To assess the contribution of attribute extraction for malicious samples, the model integrates multiple analysis methods to extract static properties. By comparing similarity between disassembled code segments, potential homology relationships between samples are identified and used to construct sample associations. An ablation study was conducted to remove these attribute-derived relationships, and the accuracy of the model decreased by nearly 4%, which demonstrates the strong role that static code properties play in enriching the network structure. The need to model the functional and behavioral relationships of the malicious sample highlights the power of attack organizations to perform coordinated campaigns based on these relationships.

6.3.2 Impact of the Number of Attention Heads

To investigate the effect of the number of attention heads in the graph attention mechanism, we performed the same investigation with the number of heads set to 8, 16, and 32. As shown in Figure 6, increasing the number of heads results in increased performance to evaluate structural information in the model ability to capture diverse types of neighborhood information. The 32-head architecture produced the highest classification performance among architectures evaluated, indicating that increased depth through richer attention mechanisms allows the model to better differentiate between the subtle structural variation of the threat intelligence network.

6.3.3 Effectiveness Evaluation of the Model

To assess the classification performance of the proposed method we used three standard evaluation metrics, including precision (P), recall (R), and F1. Precision checks for how correct the predicted threat categories are, Recall checks how much of the relevant instances are covered, and F1 is a metric that considers the previous two metrics. The results in Table 3 show that the model obtained higher scores in the test set on all three measures, suggesting that it showed effective classification of instances, when compared to the performance of thrill intelligence reports. The model's consistent performance across categories reinforces the potential for constructing node representation based on static attributes of a threat.

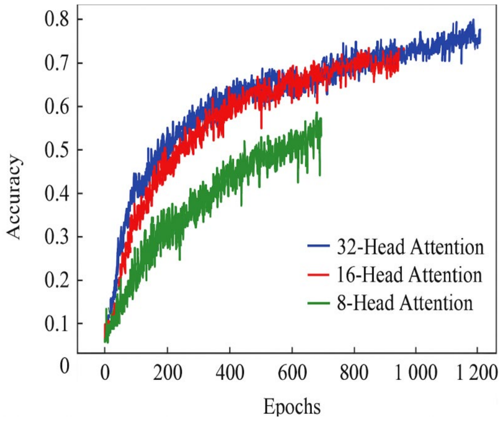

Figure 6. Accuracy of multi-attention mechanisms

Table 3. Comparison of performance metrics of the Threat Intelligence Report Classification Model across categories

Category	Precision (P)	Recall (R)	F1-Score
Malware Sample	0.912	0.897	0.904
IP Address	0.885	0.869	0.877
Domain Name	0.901	0.883	0.892
Vulnerability	0.876	0.860	0.868
Threat Actor	0.890	0.872	0.881

After analysis, it was found that the proposed method achieves an identification accuracy above 0.72 for 15 attack groups, indicating strong recognition capability for the majority of positive samples. However, three attack groups (Kimsuky, DarkHotel, and APT33) had classification accuracies of less than 0.35. When examined further, the sample sizes for DarkHotel and APT33 were small and the reports showed no connections with one another as isolated nodes, resulting in lower recognition performance. Lazarus and Turla got mislabeled with seven reports due to Kimsuky. A study revealed that Kimsuky shares similarities in their intrusion methods and equipment with those of Lazarus and Turla, which led to the difficulty in separating them. The varying levels of activity of the APT groups corresponds to a difference in the number of reports collected per group, resulting in an unavoidable class imbalance. This study examined model performance using the micro-F1 score which considers the number of samples per class and is useful for imbalanced datasets. The tests' outcomes suggest that the recommended approach obtained a micro-F1 score of 0.80 based on three assessment criteria, providing evidence of reliable and successful classification even on imbalanced class distributions.

6.3.4 Comparative Evaluation of Different Models

To evaluate the efficacy of the graph attention mechanism used in the created knowledge graph, comparative experiments were run between two classical homogeneous graph models: a frequency-domain model based on GCN and a spectral-domain model based on GraphSage. More information about the comparative experiments is provided in the next section (Section 5.2), and the results comparing the three models are summarized in Table 4.

Table 4. Comparison of Different Models on the Knowledge Graph

Model	Accuracy	Precision	Recall
Frequency-domain GCN	0.74	0.72	0.70
Spectral-domain GraphSage	0.76	0.75	0.73
Graph Attention Network (GAT)	0.81	0.79	0.78

The table quantitatively displays that the graph attention mechanism based GAT model exhibits higher accuracy than both frequency-domain GCN and spectral-domain GraphSage models across all evaluation measures, demonstrating superior performance.

7. Network Ransomware Attack and Defense Posture Modeling and Simulation Analysis

7.1 Ransomware Attack and Defense Behavior Characteristics and Model Construction

In recent years, cyber ransomware attacks have occurred frequently, typically represented by a number of high-impact viruses, including WannCry, BadRabbit, GandCrab and Sodinokibi. Typically, viruses are disseminated by taking advantage of the vulnerabilities in systems or through social engineering attacks, such as phishing, or malware, like Trojans. After a device has been infected, the virus may encrypt the files stored on it, which are typically unrecoverable unless a ransom is paid. This can generate significant losses to individuals and businesses. Ransomware viruses are evolving quickly and there are so many variants that simply relying on traditional measures of protection can be difficult. For these reasons it is particularly important to enhance the defensive strategies against ransomware viruses.

An effective defence against ransomware should address the issue from both technical means and management measures. On the technical side, it is necessary to deploy antivirus software and update virus databases in a timely manner, quickly patch operating system vulnerabilities, close unnecessary shared ports, and adopt complex and dynamically updated password policies. On the management side, it is recommended to regularly back up critical data and raise employees' security awareness to prevent social engineering attacks.

For the attack and defense process of ransomware, this paper constructs a network attack and defense model based on game theory to simulate the dynamic interaction between attackers and defenders. Defenders are divided into two categories of “enhanced defense” and “basic defense” based on their security awareness and defense capabilities, with the former having strong system maintenance and patch update capabilities, and the latter being relatively weak. For example, in the patch release for the MS17-010 vulnerability and the WannCry outbreak in 2017, some users upgraded their systems in a timely manner, which can be regarded as strengthened defense, while those who did not update their systems in a timely manner are regarded as basic defense. The proportion of reinforced defense is expressed as a parameter.

Attackers are also categorized into “advanced attacks” and “common attacks”, with the former mastering sophisticated vulnerability scanning and social engineering tools and more mature attack techniques, and the latter having limited capabilities and relying mainly on simple attacks. Taking GandCrab virus as an example, it has been gradually upgraded from its initial version, and its low version has been gradually detected and blocked by the defense system. The percentage of advanced attackers is parameterized as.

This paper further refines the attack and defense strategies by defining a variety of strategy types respectively, and the specific attack and defense types and corresponding strategy contents are detailed in Table 5.

Table 5. Ransomware Attack and Defense Categories with Strategy Types

No.	Attacker Type	Attack Strategy Type	Defender Type	Defense Strategy Type	Description
1	Advanced Attack	Combined Vulnerability Scanning and	Enhanced Defense	Comprehensive Patch Management and	Attacker uses advanced techniques;

		Deep Social Engineering		Dynamic Protection	defender has strong security awareness
2	Advanced Attack	Combined Vulnerability Scanning and Deep Social Engineering	Basic Defense	Basic Protection Measures	Attacker is strong; defender has weak security awareness
3	Ordinary Attack	Simple Vulnerability Scanning and General Social Engineering	Enhanced Defense	Comprehensive Patch Management and Dynamic Protection	Attacker is moderate; defender is strong
4	Ordinary Attack	Simple Vulnerability Scanning and General Social Engineering	Basic Defense	Basic Protection Measures	Both attacker and defender have relatively weak capabilities

During the attack and defense of ransomware, the attacker's revenue mainly comes from the ransom paid by users as well as its reputation and influence enhancement in the hacker circle, and the more the number of infected devices is, the more significant the reward gained. At the same time, the attacker needs to bear the cost of producing malware and spreading viruses, and if the attack is detected in time, it may also face additional risks such as countermeasures or legal penalties by the defender (see Figure 7).

The benefits to the defender are mainly reflected in the reduction of downtime and damage caused by data leakage by taking effective defense measures to avoid data loss or recovering the system in a timely manner after being infected. In addition, the resources invested by the defender to implement the security policy, such as security equipment procurement, operation and maintenance management and personnel training, also constitute a certain defense cost. At the same time, if an infection occurs, the cost of repairing data and resuming business cannot be ignored.

Based on a large amount of historical case data and expert assessment, this paper combines statistical analysis and regression modeling to quantify the overall system loss (SDC), attacker cost (AC) and defender cost (DC). The defense gain and attack gain under different combinations of attack and defense strategies are calculated, and the specific results are detailed in Table 6, which demonstrates the dynamic change law of the gain and cost of each party under diverse attack and defense postures.

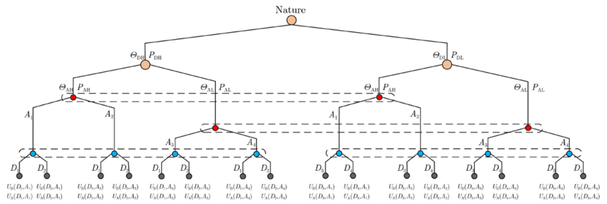

Figure 7. Bayesian game tree for ransomware virus

Table 6. Evaluation of Attack and Defense Returns and Costs under Different Strategy Combinations

Attack Strategy	Defense Strategy	Attack Return (AR)	Attack Cost (AC)	Defense Return (DR)	Defense Cost (DC)	System Damage Cost (SDC)
Ordinary Attack	Basic Defense	50	20	30	25	40
Ordinary Attack	Enhanced Defense	40	20	45	35	25
Advanced Attack	Basic Defense	80	35	25	25	60
Advanced Attack	Enhanced Defense	70	35	50	40	30

The game model demonstration project for ransomware attack and defense was constructed using Gambit 15.0 software, as shown in Figure 8. By solving the model through this simulation platform, the Bayesian Nash equilibrium solution of the ransomware attack and defense game is obtained, which effectively reflects the optimal behaviors of the two sides and their equilibrium states under different attack and defense strategy choices. The results provide a theoretical basis for an in-depth understanding of the strategic interaction between the attacker and the defender, and help to formulate a more scientific and reasonable security protection program.

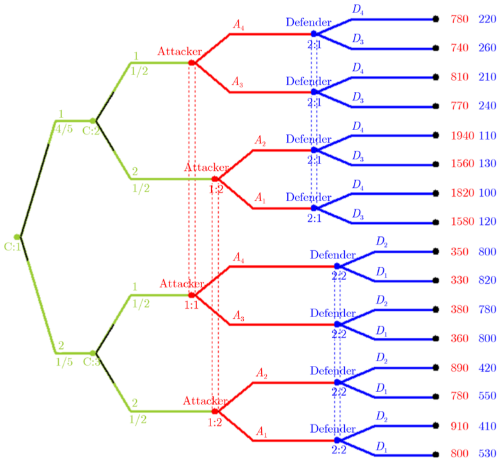

Figure 8. Gambit project example of a ransomware assault and defense game model

7.2 Dynamic Simulation of Ransomware Attack and Defense Situations

Network information systems are typically composed of a large number of interconnected nodes, where the attack and defense behavior of a single node cannot fully reflect the overall security posture of the entire network. Therefore, simulation methods that model and analyze the interactive attack-defense processes among multiple nodes provide an effective approach to reveal the evolving security situation of the network. This study employs NetLogo, an open-source multi-agent simulation platform capable of simultaneously modeling intelligent behaviors of a large number of nodes.

In the simulation experiment, a network model consisting of 1,000 nodes is constructed, with an average node degree set to 6. Among these, 10 initial infection nodes (IN), representing compromised hosts, are designatedThe enhanced defense nodes (RN), represented by blue, are nodes in the network that exhibit high defense capabilities. The ordinary defense nodes (SN), represented by gray, are nodes in the network that behave in a changeable and less effective manner. The defense attack in a baseline network illustrates the initial network attack-defense posture in Figure 9.

After changing the simulation parameters, the dynamic evolution of the network attack-defense posture under various contexts is generated, and respective results are presented in Figures 10-12. The horizontal axis on each figure represents the simulation time, and the vertical axis presents the ratio of each node type in the entire simulation. When considering the confidentiality, integrity, and availability (CIA) needs of the network, when the ratio of infection nodes (IN) surpasses 5%, a large scale ransomware outbreak could be noted, and when it as fact exceeds 50%, the network information system could be deemed severely incapacitated as a result of the ransomware attack [38].

Therefore, this simulation model not only illustrates visually the trend changes of the number of nodes with different defense strength (SN, RN) and infected nodes (IN), but also provides a theoretical approach for evaluating the effectiveness of the defense and formulating adaptive protection strategies.

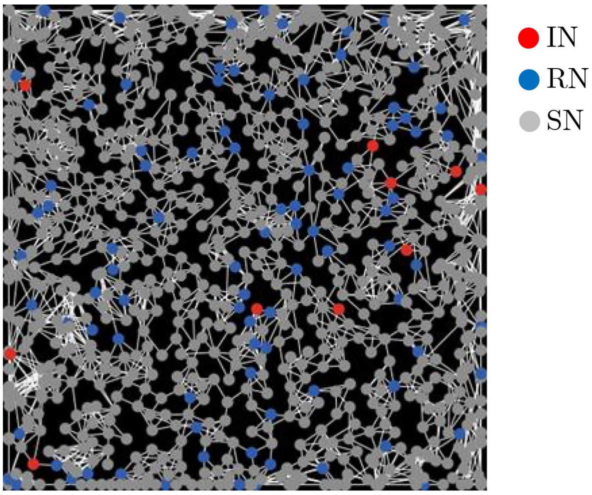

Figure 9. Initial attack and response on a network

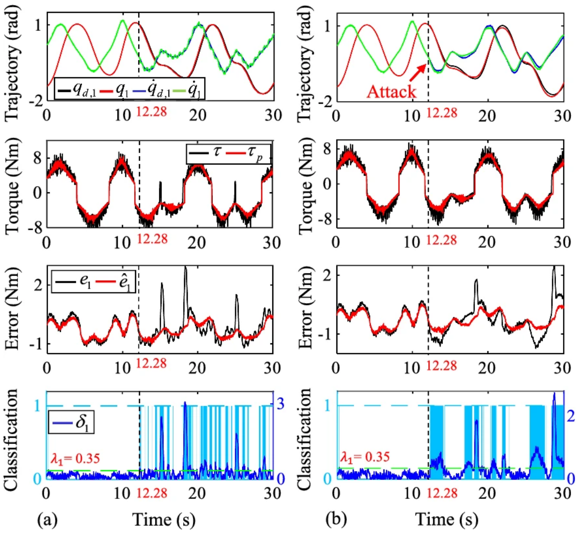

Figure 10. At RN=100, attack and defense stance

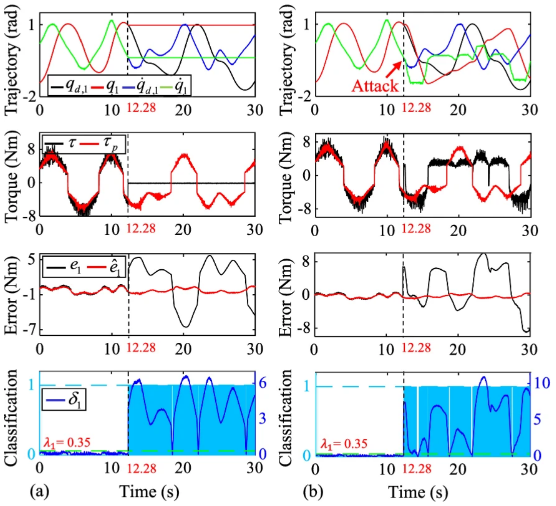

Figure 11. At RN=200, attack and defense stance

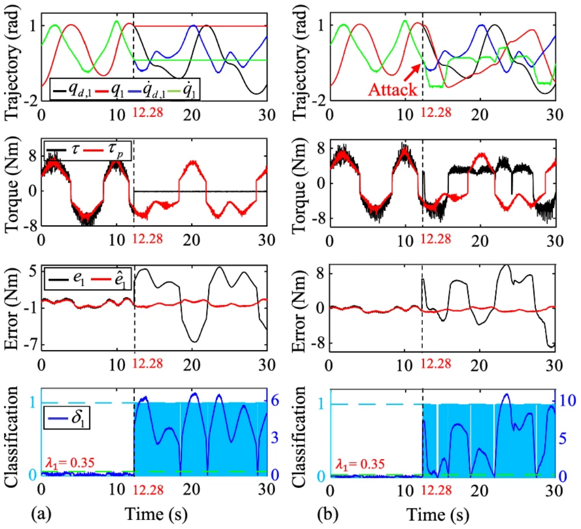

Figure 12. At RN=300, attack and defense stance

(1) The interactions of attack-defense at a micro level are the mechanisms defining the evolution of the security posture at a macro level. Different combinations of attacks and defense will lead to various outcomes of the game. In summary, the comparative evidence suggests that once the game has reached equilibrium, the peak proportion of infected nodes (IN) is significantly lower if the defender received higher payoffs and the attacker received lower payoffs, suggesting that the ransomware took less time to survive and had a limited spread, resulting in a network security posture in favor of the defender. Given the attack-defense behaviors (i.e., a series of microscopic behaviors) the study of game payoffs and the exploration of macroscopic dynamics through equilibrium solutions helps better understand the evolution of network security posture, advanced theoretical consideration of ideal micro defense strategy, followed by maximizing the effectiveness of macro protection.

(2) Strengthening the defense capabilities of individual nodes is an essential piece of improving the overall network attack-defense posture. By comparing Figures 10 and 11, we can see that at or below a probability of 0.363 of a node using enhanced defense the proportion of infected nodes, or IN, has a meaningful peak that could lead to a potential large-scale ransomware outbreak within the network. Even in Figure 12, we can see that the peak infection ratio is above 50%, which can create a complete white-out of the network system. On the other hand, we need to reinforce proactive attack detection along with collective punitive measures after an attack. This will deter potential attackers but also harden attacks and increase cost, which in turn reduces their expected payoff. If we are able to increase cost of attacks and the expected payoff of attacks in these decision points we should take comfort that this decision point moves slightly in favor of the defender, as all dynamics do change and evolve based on attacker and defender capabilities.

The results of this study have been compared with similar literature, as noted in Table 7. For the game information, this study is based on an incomplete information game model, where the attacker and defender can take on multiple types he more closely model real world scenarios of attack-defense in networks. For examining evolutions of the state, the study adopts the theory of epidemiological dynamics to propose a new definition and method for the dynamic analysis of the network attack-defense posture. For the experimental scenarios, the study uses the NetLogo multi-agent simulation platform to model interactions among large-scale network nodes dynamically, and thereby models the temporal evolution of the attack-defense posture. Compared to existing work, the proposed framework accounts more closely for the real-world environment of incomplete information, in which macroscopic posture evolutions can be analyzed and interpreted from microscopic attack-defense behaviors. This method also is suited for large-scale scenarios and provides clear and intuitive visualizations of the successive situational evolutions.

Table 7. Comparison of This Study with Related Literature

Evaluation Dimension	This Study	Related Literature	Remarks
Game Informatio n Type	Based on incomplete information; multiple attacker and defender types	Mostly based on complete informatio n or single type	More consistent with real network attack-defense environment s

Situational Evolution Analysis Method	Integrates epidemiological dynamics theory; dynamic definition and analysis of network posture	Often static or simplified models	Captures dynamic changes in network attack-defense posture
Experimental Simulation Platform	NetLogo multi-agent simulation supporting large-scale node interactions	Often small-scale or single-agent simulation	Suitable for large-scale network scenarios; more intuitive posture presentation
Attack-Defense Behavior Analysis Level	Analyzes macroscopic posture evolution from microscopic game behaviors	Mostly focuses on macroscopic or static analysis	Combines micro and macro perspectives for more comprehensive explanation
Applicable Scenarios	Large-scale network security posture analysis	Mostly medium or small-scale or specific scenarios	Has stronger potential for broader application

8. Conclusion

This research tackles the issues of protecting complex network environments from coordinated and persistent cyber threats while developing an integrated framework for combining threat intelligence analysis, action auditing, and attack traceability. The unified knowledge graph provides a common and consistent view of the heterogeneity with threat intelligence reported by assessing and sharing threats corresponding to attacker tactics and capabilities. The Bayesian game model based on NADGM quantifies and optimizes attacker and defender strategies in incomplete information structural situations for defensive decision-making. The graph attention network leverages relationship semantics to improve the guidance of classification and attribution of threat intelligence reports. The simulation experiments conducted in NetLogo support that increased defender capability at the node level in combination with greater attacker costs are central to managing the evolution of attack-defense situations. The comparative experimentation highlights that an adaptable, agile approach can accurately identify responding to the threats and plan the defender body in an efficient and scalable way, while supporting dwell time for situation awareness. Future work will focus on exploring the integration of heterogeneous graph neural networks and real-time data streams to further improve the defender framework's adaptability and resilience. In summary, this work provides contributions, both theoretical and practical, in aiding toward evolving attack/defense conditions with proactive, and adaptable, cybersecurity defense operations.

Declarations

Funding: Authors did not receive any funding.

Conflicts of interests: Authors do not have any conflicts.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Code availability: Not applicable.

Authors' Contributions: Hushuang Zeng is responsible for designing the framework, analyzing the performance, validating the results, and writing the article. Xiangyu Lei is responsible for collecting the information required for the framework, provision of software, critical review, and administering the process.

References

[1.] Santoso PA. The role of threat intelligence sharing in strengthening collective cyber defense across organizations. Glob Res Perspect Cybersecur Gov Policy Manag. 2024;8(12):24-33.

[2.] Alarood AA, Alzahrani AO. Interoperable defensive strategies of network security evaluation. IEEE Access. 2024;12:33959-33971.

[3.] Tahmasebi M. Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. J Inf Secur. 2024;15(2):106-133.

[4.] Khaleel YL, Habeeb MA, Albahri AS, Al-Quraishi T, Albahri OS, Alamoodi AH. Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods. J Intell Syst. 2024;33(1):20240153.

[5.] Wang L, Zhang C, Chen Q, Liu Z, Liu S, Yang Z, Li H. A communication strategy of proactive nodes based on loop theorem in wireless sensor networks. In: Proc Int Conf Intell Control Inf Process (ICICIP). 2018; pp. 160-167.

[6.] Arifkhodzhaieva T. Digitalisation and counteraction to information threats in the state security management system. Visegrad J Hum Rights. 2024;(5):6-12.

[7.] Sengupta A, Ramteke V. Leveraging next-generation business intelligence for proactive cybersecurity defense. In: Proc IEEE Int Conf Commun Syst Netw Technol (CSNT). 2025; pp. 414-419.

[8.] Priyadharshini SL, Al Mamun MA, Khandakar S, Prince NNU, Shnain AH, Abdelghafour ZA, Brahim SM. Unlocking cybersecurity value through advance technology and analytics from data to insight. Nanotechnol Percept. 2024;:202-210.

[9.] Lysenko S, Bobro N, Korsunova K, Vasylchyshyn O, Tatarchenko Y. The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. Econ Aff. 2024;69:43-51.

[10.] Basholli F, Juraev DA, Egamberdiev K. Framework, tools and challenges in cyber security. Karshi Multidiscip Int Sci J. 2024;1(1):94-104.

[11.] Samonte MJC, Laurenio ENB, Lazaro JRM. Enhancing port and maritime cybersecurity through AI-enabled threat detection and response. In: Proc Int Conf Smart Grid Smart Cities (ICSGSC). 2024; pp. 412-420.

[12.] Alanezi M, AL-Azzawi RMA. AI-powered cyber threats: A systematic review. Mesopotamian J Cybersecur. 2024;4(3):166-188.

[13.] Malve D, Reddy CKK, Meenal H, Indira P, Lippert K. AI-enhanced threat detection and response framework for advanced cyber-physical smart ecosystems. Inf Secur Gov Artif Intell Things Smart Environ. 2024;:111-128.

[14.] Ji R, Padha D, Singh Y, Sharma S. Review of intrusion detection system in cyber-physical system based networks: Characteristics, industrial protocols, attacks, data sets and challenges. Trans Emerg Telecommun Technol. 2024;35(9):e5029.

[15.] Talakola S. Security challenges in autonomous systems: A zero-trust approach. Int J Emerg Trends Comput Sci Inf Technol. 2025;:56-66.

[16.] Papalkar RR, Alvi AS. A Hybrid CNN Approach for Unknown Attack Detection in Edge-Based IoT Networks. EAI Endorsed Transactions on Scalable Information Systems. 2024;11(6):10.

[17.] Lv H, Ding Y. A Hybrid Intrusion Detection System with K-means and CNN+LSTM. EAI Endorsed Transactions on Scalable Information Systems. 2024;11(6).

[18.] Yin J, Hong W, Wang H, Cao J, Miao Y, Zhang Y. A Compact Vulnerability Knowledge Graph for Risk Assessment. ACM Transactions on Knowledge Discovery from Data. 2024;18(8):1–17.

[19.] Manoharan P, Hong W, Yin J, Wang H, Zhang Y, Ye W. Optimising Insider Threat Prediction: Exploring BiLSTM Networks and Sequential Features. Data Science and Engineering. 2024;9(4):393–408.

[20.] Mohamed N, Taherdoost H, Madanchian M. Enhancing Spear Phishing Defense with AI: A Comprehensive Review and Future Directions. EAI Endorsed Transactions on Scalable Information Systems. 2025;12(1).

[21.] Chaure S, Mane V. Digital forensic framework for protecting data privacy during investigation. EAI Endorsed Transactions on Scalable Information Systems. 2023;11(2).

[22.] Pashaj K, Tomço V, Gjika E. From threat to response: Cybersecurity evolution in Albania. Smart Cities Reg Dev J. 2025;9(1):17-27.

[23.] Iacovazzi A, Wang H, Butun I, Raza S. Towards cyber threat intelligence for the IoT. In: 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT); 2023 Jun; pp. 483-490. IEEE.

[24.] Zabihi A, Parhamfar M, Khodadadi M. Strengthening resilience: A brief review of cybersecurity challenges in IoT-driven smart grids. J Mod Technol. 2024;:106-120.

[25.] Abomakhelb A, Jalil KA, Buja AG, Alhammadi A, Alenezi AM. A comprehensive review of adversarial attacks and defense strategies in deep neural networks. Technol. 2025;13(5):202.

[26.] Reddy DR, Ramani S, Mohan D, Sahukar L, Ramaswamy T. Secure IoTNet: A graph-residual adversarial network integrated with Hawk-Bee optimizer for intrusion detection in IoT wireless networks. Int J Data Sci Anal. 2025;:1-19.

[27.] Morić Z, Dakić V, Kapulica A, Regvart D. Forensic investigation capabilities of Microsoft Azure: A comprehensive analysis and its significance in advancing cloud cyber forensics. Electron. 2024;13(22):4546.

[28.] Pashaj K, Tomço V, Gjika E. From threat to response: Cybersecurity evolution in Albania. Smart Cities Reg Dev J. 2025;9(1):17-27.

[29.] Iacovazzi A, Wang H, Butun I, Raza S. Towards cyber threat intelligence for the IoT. In: 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT); 2023 Jun; pp. 483-490. IEEE.

[30.] Adil M, Khan MK, Kumar N, Attique M, Farouk A, Pahlevan M, Voulkidis A, Velivassaki TH. Secure exchange of cyber threat intelligence using TAXII and distributed ledger technologies - application for electrical power and energy system. In: Proceedings of the 16th International Conference on Availability, Reliability and Security; 2021 Aug; pp. 1-8.

[31.] Gržinić, T., & González, E. B. (2022). Methods for automatic malware analysis and classification: a survey. *International Journal of Information and Computer Security*, *17*(1-2), 179-203.

[32.] Sengupta S, Roy S. Artificial intelligence (AI) in cybersecurity: A revolution in threat detection and prevention. In: Int Ethical Hack Conf. 2024; pp. 497-514.

[33.] Reis J. EU space security–An 8-step online discourse analysis to decode hybrid threats. PLoS One. 2024;19(7):e0303524.

[34.] Adil M, Khan MK, Kumar N, Attique M, Farouk A, Guizani M, Jin Z. Healthcare internet of things: Security threats, challenges, and future research directions. IEEE Internet Things J. 2024;11(11):19046-19069.

[35.] Neoaz N. Role of artificial intelligence in enhancing information assurance. Bull J Multidisiplin Ilmu. 2024;3(5):749-758.

[36.] Röttinger R. Implementing the capabilities of the ATLAS network to improve the European Union's counter-terrorism efforts. In: Proc Int Sci Pract Conf Environ Technol Resour. 2025; 5:247-253.

[37.] Sowmya N, Rao BS. Adaptive honeypot strategies: Redefining security in cloud environments. Metall Mater Eng. 20=25;:1679-1686.

[38.] Kala EM. Public-private synergy in cybersecurity: Advanced strategies for bridging regulatory gaps and enhancing digital resilience. Int J Res. 2024;10(2):31-40.