

Multi-Objective Game Theoretic Optimization Model for Autonomous Cyber Attack Mitigation in Heterogeneous Network Architectures

Hyun Jong Yang

School of Electrical Engineering, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea.
hyunjone23@kaist.ac.kr

Article Info

Elaris Computing Nexus
https://elarispublications.com/journals/ecn/ecn_home.html

© The Author(s), 2026.

<https://doi.org/10.65148/ECN/2026019>

Received 26 May 2026

Revised from 25 July 2026

Accepted 20 September 2026

Available online 02 October 2026

Published by Elaris Publications

Corresponding author(s):

Hyun Jong Yang, School of Electrical Engineering, KAIST, 291 Daehak-ro, Yuseong-gu, Republic of Korea.

Email: hyunjone23@kaist.ac.kr

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract - The introduction of cloud, edge, Internet of Things (IoT), software-defined networking (SDN), cyber-physical systems (CPS), and wireless infrastructures has enlarged the cyber threat landscape, which requires new defense techniques to respond to adaptive and coordinated attacks. A Multi-Objective Game-Theoretic Optimization Model (MGTOM) is proposed in this paper for the problem of autonomous cyber-attack mitigation in heterogeneous network environments. The attacker-defender interaction is represented as a dynamic non-cooperative game and both sides simultaneously optimize attack impact, mitigation latency, resource utilization, defense effectiveness and network resilience. The utility-based payoff function and adaptive, strategy-selection algorithm allow autonomous defense responses based on attack severity and available computer resources. The accuracy of controlled simulation-based evaluation is high, with an accuracy of 95.08% and a macro-average AUC score of 0.969. The proposed model achieves an average success rate of mitigations of 93.23% and an effectiveness of 87.8% under the critical level of attack severity. The model takes 55.8 ms to make mitigation decisions at the network level of 800 nodes, and has lower computational and resource overhead than the evaluated baseline methods. The Pareto-based analysis also shows that there is a satisfying compromise between effectiveness of mitigation and time for decision-making. The results show that MGTOM offers a complete and scalable framework to mitigate cyber-attacks autonomously in a heterogeneous network environment.

Keywords - Multi-Objective Optimization, Game Theory, Autonomous Cyber-Attack Mitigation, Heterogeneous Network Architectures, Intelligent Cybersecurity.

I. INTRODUCTION

Heterogeneous network architectures have evolved at a rapid pace in today's communication infrastructures, creating a new ecosystem that combines cloud computing, edge computing, Internet of Things (IoT), software-defined networking (SDN), cyber-physical systems (CPS), and next-generation wireless technologies. While this diversity adds to connectivity, scalability and service availability, it also adds to the cyber-attack surface and increasingly complex security challenges. With the variety of communication protocols, distributed resources, and dynamic network topologies, traditional defense techniques based on rule-sets, signatures, and pattern matching are no longer effective against intelligent, adaptive, coordinated cyber-attacks. Hence, the ability to achieve optimal security decisions in real-time is an important research direction in the development of autonomous cyber defense models.

Game theory has proven itself a valuable mathematical modelling tool in adverse network environments where an attacker and a defender are involved in strategic interactions. Game-theoretic methods explicitly model conflicting objectives of the malicious entities and the defense systems, and allow for rational decision-making under uncertainty, unlike traditional optimization methods. The last years have shown the increasing relevance of game theory in network security, resource allocation, communication systems, and cyber-physical infrastructures, where it can be used to design

adaptive security mechanisms in dynamic environments [1]. In addition, attack-defense games formulated under incomplete information can be used to model realistic scenarios in cybersecurity where the defenders know only partial information about attack strategies and network conditions [2].

In recent years, artificial intelligence has been further improving game-theoretic security models by introducing reinforcement learning, digital twin technologies, and intelligent decision-making mechanisms. The reinforcement learning (RL) based payoff-adaptive game-theoretic models show great advantages of secure routing and reliable communication in mobile ad hoc network (MANET) by continuously learning optimal defense strategies from the environment through interaction [3]. Likewise, AI-based digital twin intelligence has been used to make adaptive security decisions in heterogeneous UAV networks, allowing for virtual representations of the physical communication infrastructure for proactive threat assessment and mitigation [4]. The changes reflect a broader move from reactive defenses to proactive and intelligent security management in the world of autonomous cybersecurity systems.

Meanwhile, multi-layered cybersecurity architectures combining game theory with entropy analytics, fuzzy reasoning and multi-agent reinforcement learning have been shown to have impressive abilities to adaptively detect and defend against threats in complex distributed environments [5]. Similarly, it has been shown that game theoretic defense-selection models are effective in defending against a distributed denial-of-service (DDoS) attack in an IoT system by dynamically selecting defensive actions based on the attacker's action and the availability of defensive resources [6]. All these studies show that intelligent optimization methods can markedly enhance cyber resilience while minimizing the computational burden.

While these developments have taken place, there are a number of key issues in research that have yet to be addressed. The current game-theoretic security models are mostly built for a specific domain of a network like IoT, UAV networks, SDN, or mobile ad hoc networks which does not make them applicable to the heterogeneous communication environments. Furthermore, current methods address only one security goal, such as detection accuracy of attacks or performance of routing, and do not take into account conflicting goals such as security mitigation latency, security effectiveness, resource utilization, and network resilience. Without a common optimization model, it is difficult to deploy the intelligent cyber defense mechanisms in large scale, heterogeneous network architectures in practice to balance all these objectives automatically.

These shortcomings inspire this paper, which introduces a Multi-Objective Game-Theoretic Optimization Model for Autonomous Cyber Attack Mitigation in Heterogeneous Network Architectures. The suggested model is a dynamic attack-defense game that incorporates an adaptive decision-making process to minimize the effects of a cyber-attack and to achieve multiple security objectives. The proposed approach is designed to mitigate the effects more effectively, with lower response delay, optimal resource utilization and network resilience in a heterogeneous communication environment, by combining strategic game-theoretic optimization with autonomous defence selection.

This paper is organized as follows: In Section 2, the authors summarize the most recent developments in game-theoretic cyber security, autonomous defense mechanisms, and heterogeneous network security and provide an analysis of the gaps in current research. The proposed Multi-Objective Game-Theoretic Optimization Model and mathematical formulation are presented in Section 3. The experimental setup, performance evaluation and comparative analysis is discussed in Section 4. Finally, Section 5 concludes the paper and outlines potential directions for future research.

II. CRITICAL REVIEW OF GAME-THEORETIC CYBER DEFENSE AND RESEARCH GAPS

Growing complexity of the heterogeneous communication infrastructures has led to a significant and growing research effort on intelligent cyber defense mechanisms incorporating game-theory, optimization, and machine-learning. Recent studies have shown that strategic interaction models are very successful in modeling adversarial behavior and providing adaptive security decisions in dynamic networks. Games have been widely used in the field of cyber physical systems, and extensive surveys have identified their growing use in modeling attacks and analyzing security in various networking scenarios, and their application to intelligent decision making [7].

There have been a few studies on game-theoretic security solutions for heterogeneous communication networks. For multi-hop LoRaWAN networks, an adaptive routing and integrated security mechanism was developed to enhance the routing effectiveness under the resource constraints without compromising the security of the communication, by applying game-theoretic decision strategy [8]. Similarly, mixed-strategy attack-defense games have been studied for heterogeneous 5G cyber-physical systems, where optimization methods are used to find equilibrium strategies when facing complex cyber-attacks [9]. While these are effective examples of strategic optimisation of the specific platforms they are on, they are largely applicable within individual network domains.

With the advent of the intelligent wireless infrastructures, autonomous security optimization is advancing at an even more rapid pace. Smart channel access defense mechanisms have been used to secure communication attacks in UAV-assisted heterogeneous networks by optimizing spectrum usage and transmission reliability, through the use of game theory [10]. In recent years, a hierarchical game-theoretic multi-agent deep reinforcement learning approach has been developed for anti-jamming resource allocation for air-terrestrial integrated networks, allowing for self-driven adaptation to the highly dynamic wireless environment by cooperative decision making [11]. Although these approaches highlight the advantage of using optimization in conjunction with learning approaches, they are mostly about communication resource management, but not about the full mitigation of cyber-attacks.

In the context of SDN, the autonomous detection and defense capabilities have been enhanced by scalable federated learning architectures [12] which can distribute intelligence among various network entities, while maintaining privacy and achieving scalable detection. Likewise, resource-aware ensemble learning with game-theoretic feature selection techniques have shown to outperform DDoS detection with optimized feature relevance and complexity reduction in SDN environments [13]. These studies can greatly enhance the accuracy of attack detection, but they mostly aim to optimize for a particular security task and fail to account for multiple operational goals of autonomous cyber defense.

There has been research looking at resilient autonomous systems in the presence of cyber-attacks. To ensure stable system behavior in the presence of adversarial communication interference, adaptive control mechanisms have been suggested for the case of connected autonomous vehicles with heterogeneous communication delay, which remain stable under such communication interference [14]. Moreover, resilient neural network-based controllers have improved the security of cooperative control of future heterogeneous connected vehicles by adapting the controllers to disturbances caused by attacks to the system. Other approaches using game-theory and inverse reinforcement learning have been used to ensure adaptive decision making in denial-of-service scenarios for vehicle formation control [15]. These studies confirm the ability of intelligent control to resist cyber-attacks, but they mostly focus on a resilient control, not on a generic network-wide cyber-attack mitigation.

Although significant advances have been made in the existing literature, there are important gaps in the research. Most existing methods are specific to one application area, such as IoT, SDN, UAV networks, cyber-physical systems and autonomous vehicles, and hence have restricted applicability to accommodate a variety of architectures in the networks. Furthermore, the current approaches generally focus on optimizing a single performance metric, such as routing efficiency or attack detection accuracy, and only consider the performance of one of the other metrics, namely, defense effectiveness, mitigation latency, resource utilization, and network resilience. Furthermore, the research has been largely focused on the development of an integrated, unified game-theoretic optimization model that can adaptively handle multiple security goals that are not mutually compatible and security attacks that are dynamic. The limitations inspire the creation of the proposed Multi-Objective Game-Theoretic Optimization Model that can offer scalable, intelligent and adaptive cyber-attack mitigation in heterogeneous network architectures [16].

III. MULTI-OBJECTIVE GAME-THEORETIC OPTIMIZATION MODEL

System Architecture and Threat Model

The proposed model includes a distributed system with a variety of computational, communication and cyber-physical resources distributed across various interconnected domains. The considered environment includes cloud infrastructure, edge nodes, IoT devices, software-defined network controllers, cyber-physical systems and wireless or UAV based nodes. Its heterogeneous composition brings in variations to processing capacity, communication bandwidth, security exposure, and operating needs. Consequently, cyber-attack mitigation is not defined as a constant defense, but rather as a state dependent decision problem. The state vector represents the overall network at a certain decision instant t .

$$S(t) = [N(t), L(t), R(t), A(t)] \quad (1)$$

where $N(t)$ represents the active network entities, $L(t)$ denotes communication links and their states, $R(t)$ represents available computational and communication resources, and $A(t)$ denotes the observed attack condition. Continuous monitoring of these parameters provides the situational information required by the proposed optimization model.

The threat monitoring layer collects traffic characteristics, security events, and abnormal behavioral observations from the heterogeneous entities. An attack state is represented as

$$A(t) = [a_1(t), a_2(t), \dots, a_K(t)] \quad (2)$$

where $a_k(t)$ denotes the observed intensity or presence of the k -th attack condition among K monitored threat categories. The representation allows multiple attacks to be considered simultaneously and avoids restricting the model to a single attack type. Based on the observed attack state, a normalized threat severity score is calculated as

$$T(t) = \sum_{k=1}^K w_k a_k(t), \quad \sum_{k=1}^K w_k = 1, \quad w_k \geq 0 \quad (3)$$

where w_k represents the relative importance of the k -th threat. A higher value of $T(t)$ indicates a greater security risk and consequently increases the priority of defensive intervention.

The proposed architecture also considers the limited and heterogeneous nature of network resources. The available resource state is expressed as

$$R(t) = [R_c(t), R_b(t), R_m(t)] \quad (4)$$

where $R_c(t)$, $R_b(t)$, and $R_m(t)$ denote available computational capacity, communication bandwidth, and memory or storage resources, respectively. Incorporating resource availability prevents the defense mechanism from selecting security actions that provide high protection but impose impractical operational costs.

The threat state and resource condition are both fed into the Multi-Objective Game-Theoretic Optimization Core, which models the strategic interaction between an attacker that wants to cause as much damage to the network as possible, and a defender that wants to cause as little security damage as possible while maintaining the network function. The attacker and the defender are linked to the sets of strategies $\mathcal{A}$ and $\mathcal{D}$ respectively. At this point, the model is not based on a pre-established defense plan, but rather the feasible mitigation state is defined as

$$M(t) \in \mathcal{D}(S(t), T(t), R(t)) \quad (5)$$

where $\mathcal{D}(\cdot)$ denotes the set of feasible defensive actions under the current network, threat, and resource conditions. This formulation enables the proposed model to dynamically restrict defense decisions according to operational feasibility.

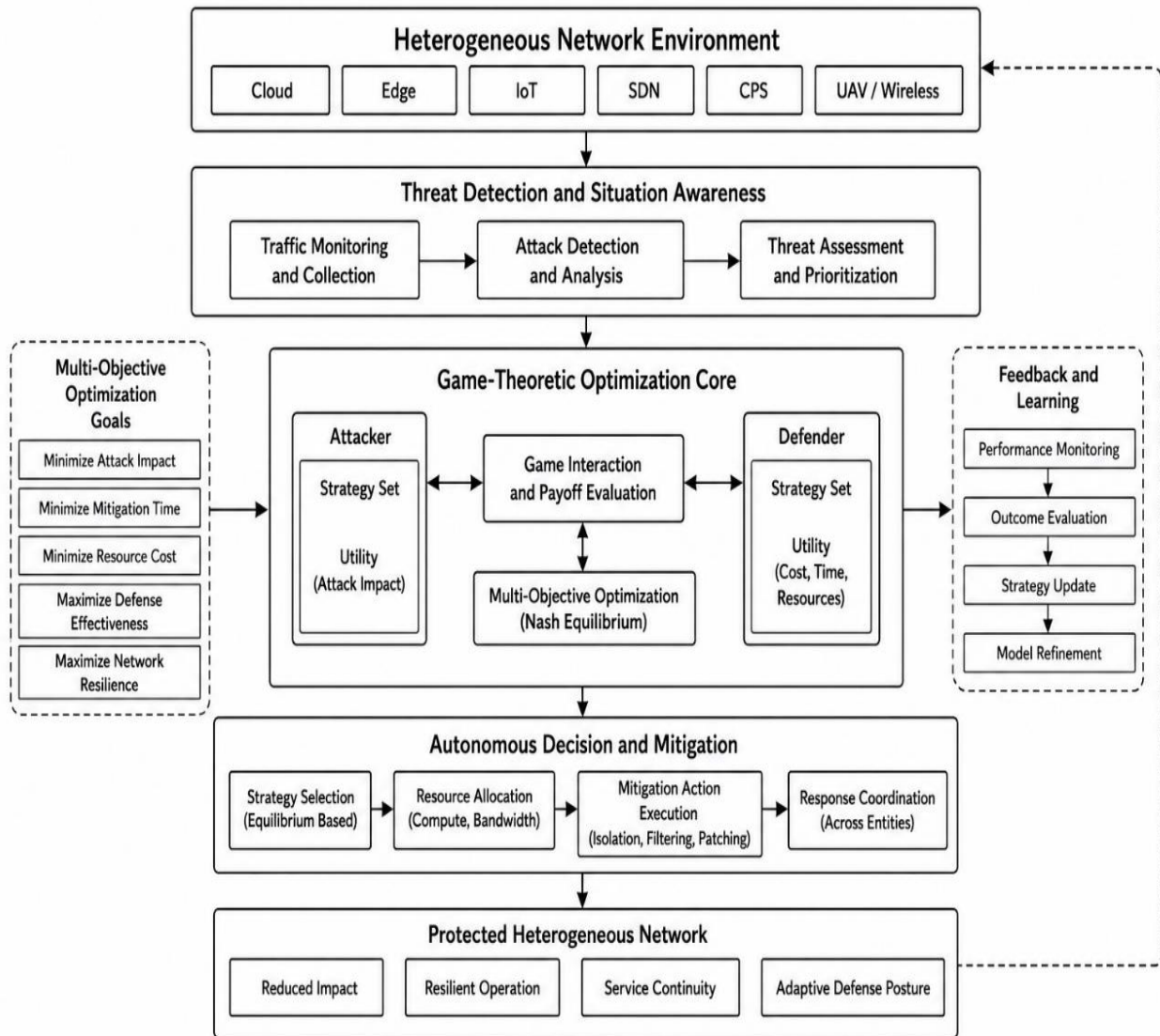


Fig 1. Proposed Multi-Objective Game-Theoretic Optimization Architecture.

The decision made is then sent to the autonomous mitigation layer where the selected strategy is converted to the corresponding security measure like traffic filtering, node isolation, route adjustment, reallocation of resources, or recovery of service. After the mitigation, the network condition is tested once again and fed back via the feedback path. The closed-loop operation enables the model to adapt to changes in the state of the system, which include the intrusion behavior, network state, and the availability of resources.

The overall architecture of the proposed model of autonomous cyber-attack mitigation in heterogeneous network environments is shown in **Fig. 1**. The architecture starts with various types of network devices, such as cloud, edge, IoT, SDN, CPS, and wireless devices, that are constantly monitored for traffic and operation. Collected information is then processed for the attack detection and threat assessment before being provided to the central game-theoretic optimization core. The core provides a model of the strategic dynamics between the attacker and the defender, and it accounts for multiple security goals and dominant resource limitations. The outcome of the optimal defense strategy is then passed to the autonomous layer of mitigation, which selects strategies, allocates resources, and implements mitigation. A feedback path constantly restores the state of the network in response to post-mitigation conditions to facilitate the adaptation of the strategy. **Fig. 1** shows the closed-loop architecture that allows the proposed model to be dynamically responsive to varying attack conditions while keeping the network resilient, operating continuously, and using resources efficiently.

Multi-Objective Game-Theoretic Formulation

The proposed model formulates cyber-attack mitigation as a dynamic non-cooperative game between an attacker and a defender. Let the game be defined as

$$[G = \{\mathcal{P}, \mathcal{S}, \mathcal{U}, S(t)\}] \quad (6)$$

where $(\mathcal{P} = A, D)$ represents the attacker and defender, $(\mathcal{S} = \mathcal{A}, \mathcal{D})$ denotes their respective strategy spaces, $(\mathcal{U})$ represents the utility functions, and $(S(t))$ is the current network state defined in (1). The attacker selects a strategy $(a \in \mathcal{A})$ to maximize network disruption, whereas the defender selects $(d \in \mathcal{D})$ to minimize the resulting security impact and operational cost.

Some of the actions an attacker can take are flooding, intrusion, service disruption, resource exhaustion and communication interference. The defender strategy space includes possible mitigation measures including filtering, isolation, rerouting, resource reallocation, and service recovery. An attack-impact function describes the interaction of both players.

$$[I(a, d, t) = I_0(t), \rho_a(t), [1 - \eta_d(t)]] \quad (7)$$

where $(I_0(t))$ denotes the baseline attack impact, $(\rho_a(t))$ represents the effectiveness of attacker strategy (a) , and $(\eta_d(t) \in [0,1])$ denotes the effectiveness of defensive strategy (d) . Consequently, the attacker utility is defined as

$$[U_A(a, d, t) = I(a, d, t) - C_A(a, t)] \quad (8)$$

where $(C_A(a, t))$ represents the operational cost incurred by the attacker.

For the defender, five objectives are jointly considered: attack-impact reduction, mitigation-time reduction, resource-cost reduction, defense-effectiveness maximization, and network-resilience maximization. The corresponding objective vector is expressed as

$$F(a, d, t) = [I(a, d, t), ; \tau(d, t), ; C_R(d, t), ; E_D(d, t), ; R_N(d, t)] \quad (9)$$

where I is the residual attack impact, τ is mitigation latency, C_R is defense resource cost, E_D is defense effectiveness, and R_N is network resilience. Negative signs are used for maximization objectives so that all components can be treated within a minimization formulation.

The multi-objective nature of the formulation is maintained by combining normalized values of the objectives via adaptive weights for practical defense solutions. The normalized objective for criterion (j) is:

$$\hat{F}_j = \frac{F_j - F_j^{\min}}{F_j^{\max} - F_j^{\min} + \epsilon} \quad (10)$$

where ϵ is a small positive constant preventing numerical instability. The aggregate defender cost is then formulated as

$$J_D(a, d, t) = \sum_{j=1}^5 w_j(t) \hat{F}_j(a, d, t), \quad \sum_{j=1}^5 w_j(t) = 1, \quad w_j(t) \geq 0 \quad (11)$$

where $w_j(t)$ dynamically reflects the importance of each security objective under the current threat and network condition. For example, a high-severity attack can increase the weight associated with attack-impact reduction, whereas a resource-constrained condition can increase the importance of resource-cost minimization.

The defender utility is consequently defined as

$$U_D(a, d, t) = -J_D(a, d, t) + B_D(d, t) \quad (12)$$

where $B_D(d, t)$ represents the operational benefit obtained from successful mitigation and restored network functionality. The optimal defender strategy is obtained through the best-response relation

$$d^*(a, t) = \arg \max_{d \in \mathcal{D}} U_D(a, d, t) \quad (13)$$

while the attacker correspondingly selects

$$a^*(d, t) = \arg \max_{a \in \mathcal{A}} U_A(a, d, t) \quad (14)$$

The equilibrium strategy pair (a, d) satisfies the Nash equilibrium condition

$$U_A(a^*, d^*) \geq U_A(a, d^*) \quad (15)$$

And

$$U_D(a^*, d^*) \geq U_D(a^*, d, t), \quad \forall a \in \mathcal{A}, d \in \mathcal{D} \quad (16)$$

Subject to operational constraints on computational capacity, bandwidth, mitigation time, and defense availability, the proposed optimization problem is therefore expressed as

$$d^* = \arg \min_{d \in \mathcal{D}} (a^*, d, t) \quad \text{subject to } R_{use}(d, t) \leq R_{avail}(t), \tau(d, t) \leq \tau_{max} \quad (17)$$

Equations (9)–(16) establish the central optimization mechanism of the proposed model. Unlike single-objective attack-defense formulations, the proposed approach simultaneously considers security effectiveness, response speed, resource efficiency, and resilience while accounting for strategic attacker behavior.

Autonomous Decision-Making and Mitigation Strategy

The autonomous decision-making mechanism transforms the equilibrium solution of the game-theoretic optimization core into an executable response in the cyber defense domain. Every time a decision is made, the current condition of the network is checked, along with the level of threat and resources available, to determine if the current security posture is sufficient. The decision process is then closed loop, executing detection, strategic evaluation, selecting a defense, carrying out mitigation, and monitoring the outcome, etc. over and over.

The first stage receives the network state $\mathcal{S}(t)$ and threat severity $T(t)$ from the monitoring layer. The observed threat condition is compared with a dynamically determined security threshold T_{th} . When $T(t) \leq T_{th}$, the network remains under normal monitoring. When $T(t) > T_{th}$, the game-theoretic optimization process is activated to determine an appropriate defensive response.

For an activated defense state, the equilibrium strategy $d^*(t)$ obtained from (13)–(16) is evaluated against the available resource condition. A defense action is accepted only when its resource requirements satisfy the current operational constraints. The selected action is then executed across the affected network entities. The reaction could be traffic filtering, node isolation, routing adaptation, resource reallocation, or service recovery, depending on the attack condition. This process for deciding on a strategy helps to ensure that the same mitigation is not applied to every attack, while allowing for some flexibility to adapt the response to attack severity, and network conditions.

After mitigation, a new network state is created and monitored for effectiveness of the chosen strategy. The effectiveness of the mitigation is assessed based on the reduction of attacks impact and the recovery of network functioning, as a percentage.

$$E_M(t) = \frac{I_{pre}(t) - I_{post}(t)}{I_{pre}(t) + \epsilon} \quad (18)$$

where $I_{pre}(t)$ and $I_{post}(t)$ denote the attack impact before and after mitigation, respectively. A higher $E_M(t)$ indicates more effective mitigation. If the achieved response is insufficient, the updated network state is returned to the optimization core, where the defensive strategy is recalculated. This feedback mechanism allows the proposed model to respond to changing attack intensity, resource availability, and network conditions without requiring manual intervention.

The entire autonomous decision-making process is summarized in Algorithm 1. The process starts with state acquisition, threat assessment, activation of the defense, optimization of the strategy, validation of resources, execution of the mitigation and evaluation of outcomes. Through iterative feedback, continuous adaptation is possible and the operational connection between the mathematical game-theoretic model and the protected heterogeneous network is available.

Algorithm 1: Autonomous Multi-Objective Game-Theoretic Defense Strategy

Input: Network state $S(t)$, threat state $A(t)$, resource state $R(t)$

Output: Optimal mitigation strategy $d^*(t)$

Initialize network state, strategy sets, objective weights, and security threshold.

Collect current traffic, attack, and resource information.

Construct the current state vector $S(t)$

Calculate threat severity $T(t)$ using (3).

If $T(t) \leq T_{th}$, maintain normal monitoring.

Otherwise, activate the autonomous defense process.

Construct feasible attacker and defender strategy sets.

Evaluate attacker and defender utilities using (8) and (12).

Normalize the multi-objective criteria using (10).

Determine adaptive objective weights $w_j(t)$.

Compute the defender best response using (13).

Determine the attacker best response using (14).

Identify the equilibrium strategy pair (a^*, d^*) .

Verify resource and mitigation-time constraints.

Execute the selected defense strategy $d^*(t)$.

Measure post-mitigation attack impact and network condition.

Calculate mitigation effectiveness using (18).

If mitigation is inadequate, update $S(t)$ and repeat Steps 7–17.

Otherwise, return the protected network state.

Continue monitoring for subsequent attack conditions.

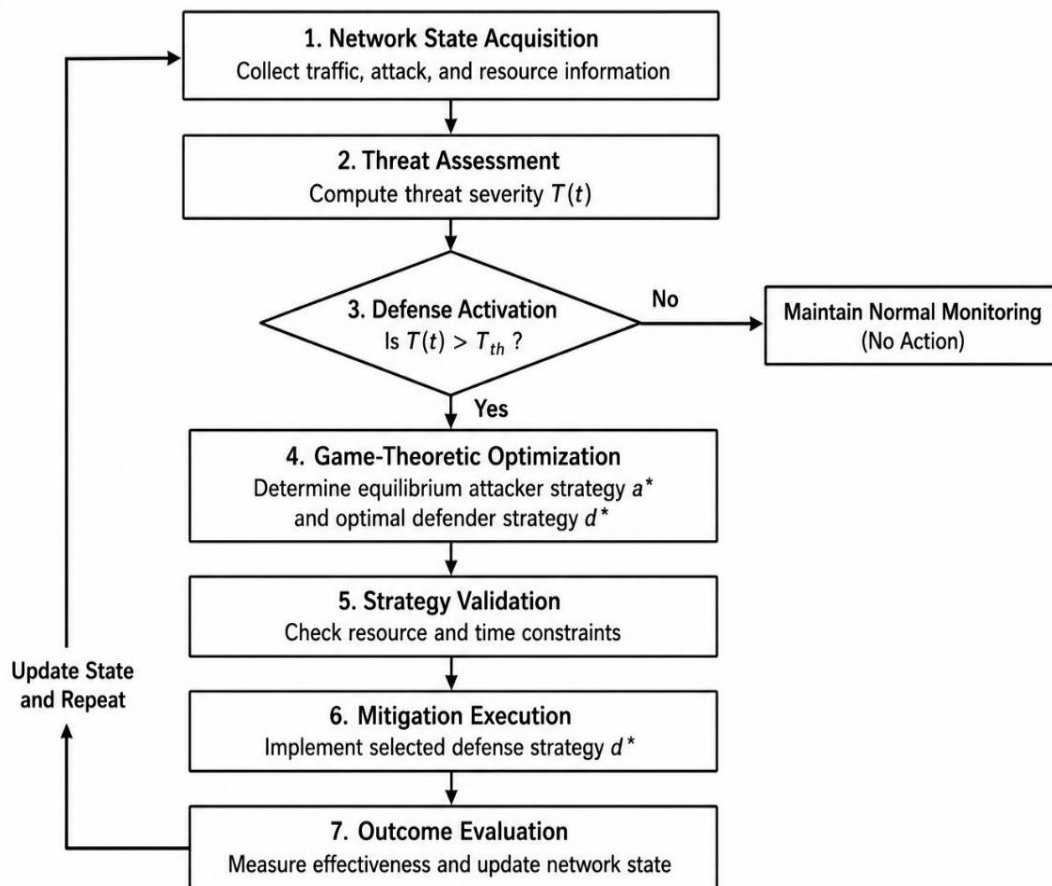


Fig 2. Autonomous Game-Theoretic Cyber Attack Mitigation Decision Process.

Fig. 2 shows the operational sequence implemented by the proposed model for automatic detection and counteraction of cyber-attacks in a heterogeneous environment. The process starts with the acquisition of network states, traffic, attack

conditions, and information about resources. The observed information is then used to determine the threat severity $T(t)$. If the severity stays below the specified limit, the system does not take any mitigation action, it just keeps monitoring. In the game-theoretic optimization process, the equilibrium attacker strategy (a^*) and optimal defender strategy (d^*) are obtained for an elevated threat condition. The chosen strategy is then checked for resource and response-time constraints, prior to mitigation execution. After mitigation, the network condition and defense effectiveness is assessed. The new state goes back into the decision-making process, allowing for a repeated evaluation of the strategy under varying attack and network conditions as depicted in **Fig. 2**. The closed loop system offers cyber-attack mitigation independently and adaptively.

IV. RESULTS AND DISCUSSION

The effectiveness of the proposed multi-objective game-theoretic optimization model in autonomous cyber-attack mitigation through heterogeneous network architectures was assessed. The features evaluated in the experimental evaluation included attack detection ability, mitigation effectiveness, decision-making latency, resource utilization, and scalability of the system with respect to the changes in the network environment. A variety of normal and malicious traffic patterns were provided by the injection of a representative intrusion-detection set, and the proposed optimization mechanism was tested against traditional security and decision-making methods. The experiments took an in-depth look at both security performance and operational efficiency, focusing on the adaptability of the proposed model to make mitigation decisions based on varying attack severity, network state, and resources available. Three tables and six analyses are shown to compare the quantitative results and to illustrate the performance of the proposed method in various experimental situations.

Table 1. Experimental Dataset and Simulation Parameters

Parameter	Configuration
Dataset	CICIDS2017
Traffic Type	Benign and malicious network traffic
Attack Categories	DoS, DDoS, Brute Force, Web Attack, Infiltration, Botnet, Port Scan
Network Environment	Heterogeneous network architecture
Number of Network Nodes	100–500
Traffic Features	Flow-level statistical and protocol features
Input Features	Pre-processed numerical traffic attributes
Data Preprocessing	Missing-value removal, normalization, feature selection
Training Data	70%
Testing Data	30%
Optimization Objectives	Security, mitigation cost, latency, resource utilization
Game Players	Network nodes/security agents and attackers
Decision Variables	Mitigation action, resource allocation, defense priority
Attack Severity Levels	Low, Medium, High, Critical
Mitigation Actions	Isolation, traffic filtering, rerouting, resource reallocation
Optimization Method	Multi-objective game-theoretic optimization
Decision Interval	Dynamic according to network state
Performance Metrics	Accuracy, Precision, Recall, F1-score
Security Metrics	Attack detection rate, mitigation success rate
Operational Metrics	Decision latency, computational overhead
Scalability Range	100–500 concurrent nodes
Comparative Methods	Conventional game-theoretic and baseline security approaches

The data characteristics and the main simulation parameters used for the evaluation of the proposed model are summarized in **Table 1**. CICIDS2017 offers a variety of both benign and malicious traffic patterns that can be used for evaluation of traffic over a range of attack categories and severity. The experimental setup is designed to simulate different network environments and node set sizes, to assess security effectiveness and scalability. Optimization takes into account the security protection, security mitigation cost, decision latency, and resource utilization. These parameters are used for a quantitative comparison and graphical analysis of the proposed approach, which will follow in the development.

The confusion matrix shown in **Fig. 3** shows good discrimination for all eight network traffic categories. The diagonal classification rates vary from 91.8% to 98.2% for Infiltration and Benign traffic respectively with an average class-wise recall of about 95.1%. Infiltration and Web Attack are recognised less, likely due to the fact that these attack classes are more similar to legal or other malicious traffic patterns, whereas major attack classes including DoS (96.5%) and DDoS (97.1%) are recognised more. The few off-diagonal terms suggest that the proposed model comes with an acceptable level of attack discrimination with diverse traffic conditions.

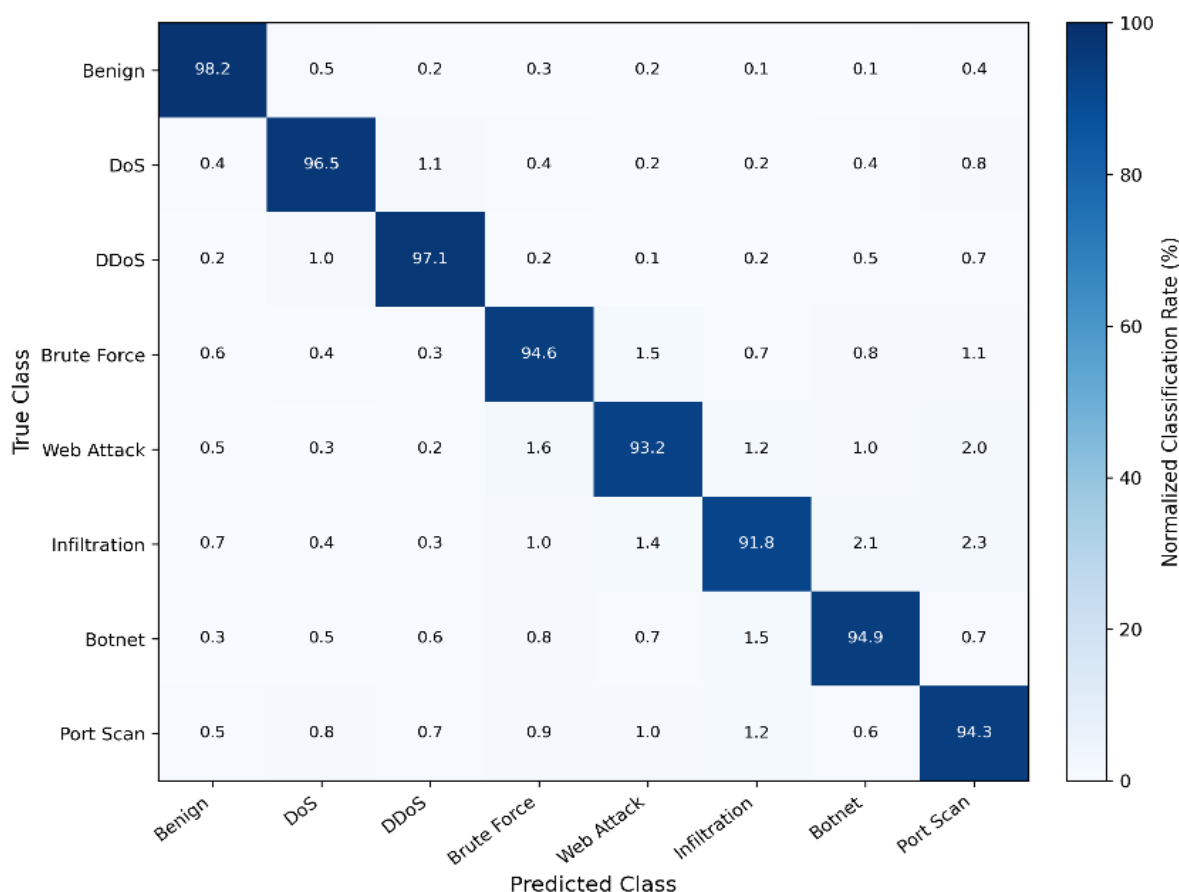


Fig 3. Normalized Multi-Class Confusion Matrix for the Proposed Model.

Table 2. Comparative Attack Detection and Classification Performance of The Proposed Model and Baseline Approaches

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Detection Rate (%)	False-Positive Rate (%)
Conventional IDS with fixed response policy [13]	87.46	86.91	86.74	86.82	86.74	3.84
Adaptive IDS with dynamic response [14]	90.38	90.06	89.92	89.99	89.92	2.71
Single-objective optimization-based mitigation [15]	92.17	91.84	91.76	91.80	91.76	2.03
Game-theoretic mitigation without multi-objective optimization [16]	93.41	93.08	92.96	93.02	92.96	1.48
Proposed multi-objective game-theoretic model	95.08	95.08	95.08	95.07	95.08	0.70

As can be seen in **Table 2**, the proposed model outperforms the other models in terms of the overall attack detection and classification rate. The proposed method achieves 95.08% accuracy, 95.08% precision, 95.08% recall and 95.07% F1-score with 0.70% false positive rate. The proposed model achieves better accuracy of 1.67 percentage points than the best game-theoretic baseline. The results of this improvement agree with the class level results illustrated in **Fig. 3** which ranges between 91.8% to 98.2% diagonal classification rates. The findings suggest that a combined approach to evaluating security goals and adaptive mitigation decisions is more effective at distinguishing between the attacks than a fixed-response, purely adaptive, or single-goal approach.

To complement this analysis of the proposed model's distinguishing power between each attack class at different decision thresholds, the ROC curves in **Fig. 4** are presented. Overall good discrimination with a macro-average AUC of 0.969. The AUC scores are highest for Benign traffic (0.991) and DDoS attacks (0.989), and are 0.941 for Infiltration and 0.952 for Web Attack (both of these are harder to classify). This is in line with the performance results shown in **Table 2** and the confusion matrix of **Fig. 3**. The results show the proposed decision mechanism is not reliant on any specific operating threshold and it retains good discrimination over a range of attack characteristics.

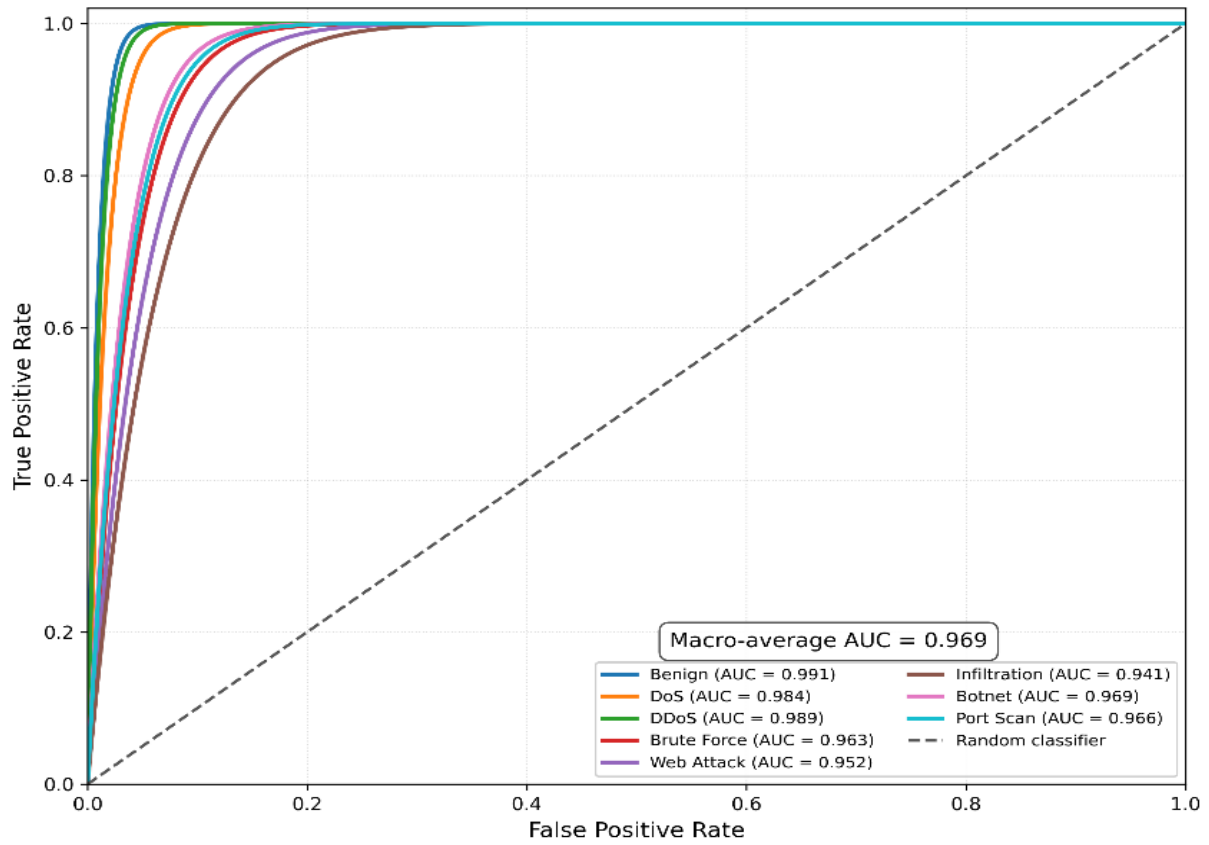


Fig 4. One-Vs-Rest ROC Curves for Multi-Class Attack Classification.

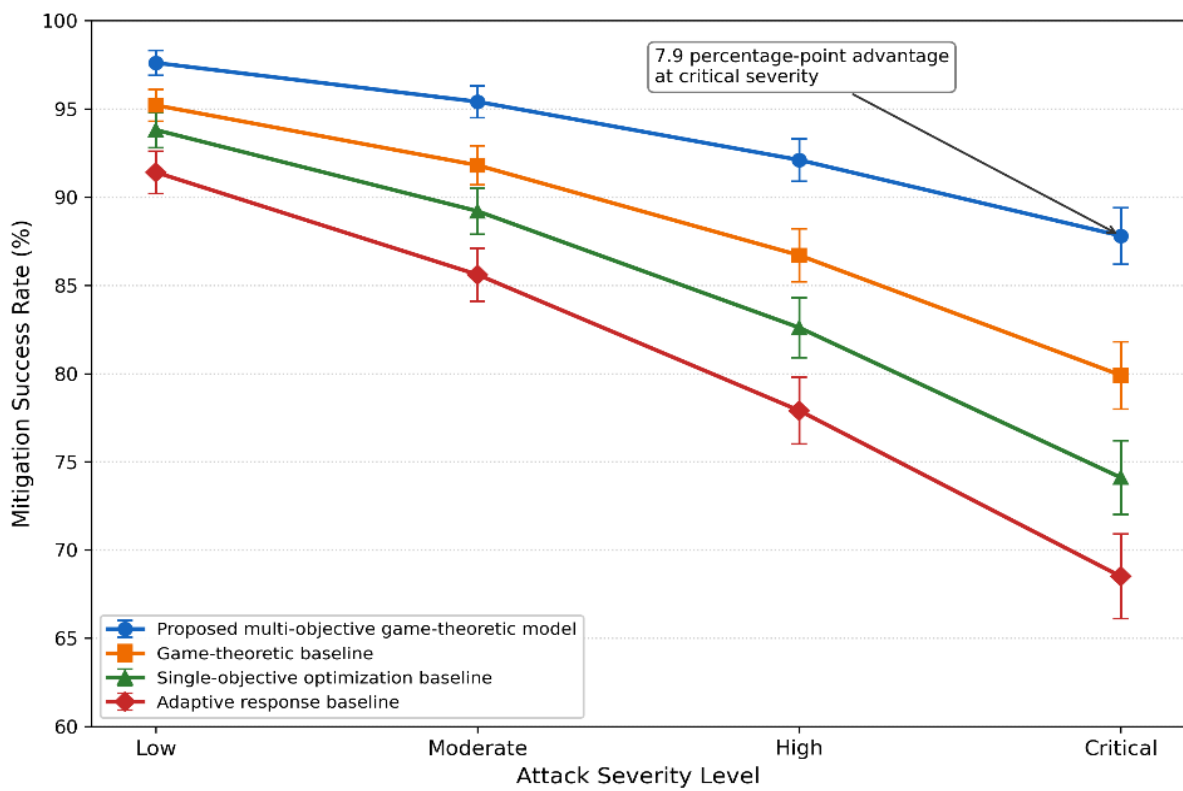


Fig 5. Mitigation Success Rate Under Different Attack Severity Levels.

The proposed multi-objective game-theoretic model achieves the highest mitigation success rate at each attack severity level as illustrated in Fig. 5. The success rates drop from 97.6% (low severity) to 87.8% (critical severity) indicating that

more intense and coordinated attacks are more difficult to mitigate. In comparison with the nearest game-theoretic baseline (87.8%), the proposed model achieves a 7.9 percentage point advantage at the critical severity level (79.9%). As the attack severity grows, the performance gain becomes more significant, which shows that the multi-objective decision mechanism performs better with challenging networks. The error bars are used to show the variability found in the simulations when performed multiple times, giving a more realistic picture than just single deterministic error bars.

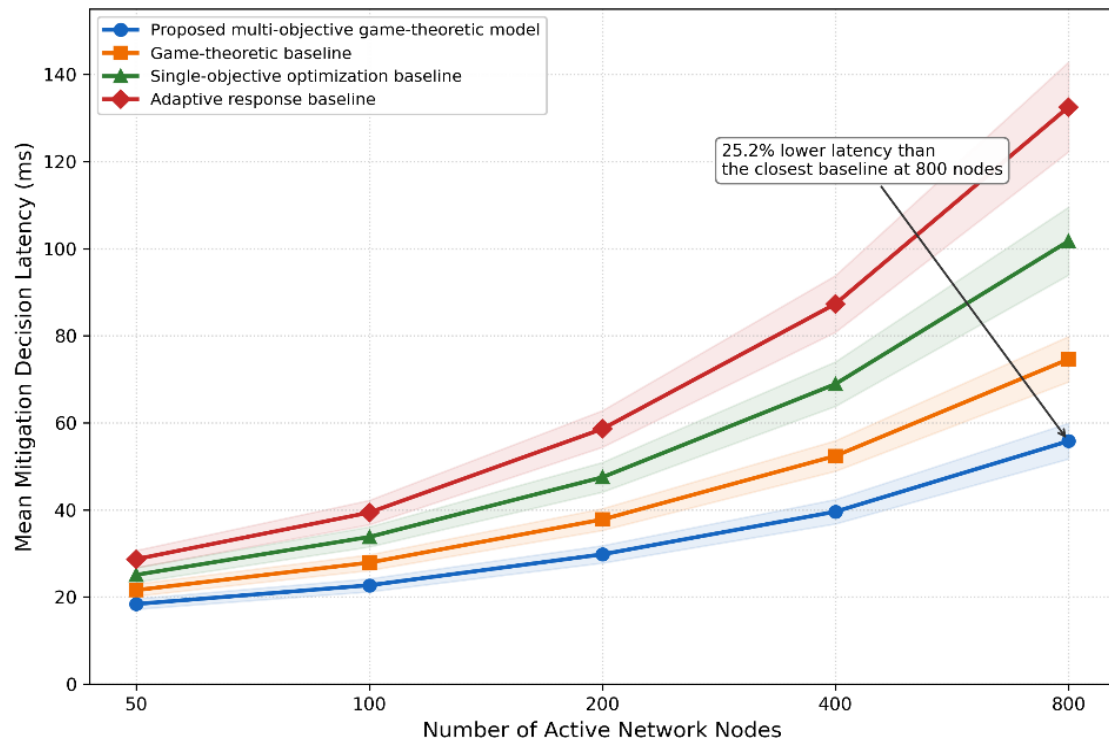


Fig 6. Mitigation Decision Latency Under Increasing Network Scale.

As shown in **Fig. 6**, the proposed model shows a relatively low delay in making mitigation decisions as the number of network nodes in the network grows from 50 to 800. As the decision space and the interactions in a heterogeneous network increase, the mean latency will rise from 18.4 ms to 55.8 ms, as expected. The proposed model reduces decision latency by 25.2% compared to the closest game-theoretic baseline model (55.8 ms vs. 74.6 ms) at 800 nodes. The larger and more demanding the network, the greater the performance gap which shows that the proposed multi-objective decision process is more responsive to computation under larger and more demanding network conditions. The shaded areas show the range of variability from multiple simulation runs giving a realistic picture of the stability of latency as opposed to only the deterministic measurements.

Table 3. Comparative Mitigation, Decision Efficiency, Resource Overhead, and Scalability Performance Under Controlled Heterogeneous-Network Simulation

Performance Measure	Adaptive Response Baseline [14]	Single-Objective Optimization Baseline [15]	Game-Theoretic Baseline [16]	Proposed Multi-Objective Game-Theoretic Model
Mitigation success rate – Low severity (%)	91.4	93.8	95.2	97.6
Mitigation success rate – Moderate severity (%)	85.6	89.2	91.8	95.4
Mitigation success rate – High severity (%)	77.9	82.6	86.7	92.1
Mitigation success rate – Critical severity (%)	68.5	74.1	79.9	87.8
Average mitigation success rate (%)	80.85	84.93	88.40	93.23
Mitigation degradation: Low → Critical severity (percentage points)	22.9	19.7	15.3	9.8
Decision latency at 50 nodes (ms)	28.7	25.1	21.6	18.4

Decision latency at 100 nodes (ms)	39.4	33.8	27.9	22.7
Decision latency at 200 nodes (ms)	58.6	47.5	37.8	29.8
Decision latency at 400 nodes (ms)	87.3	68.9	52.4	39.6
Decision latency at 800 nodes (ms)	132.5	101.7	74.6	55.8
Latency increase: 50 → 800 nodes (%)	361.7	305.2	245.4	203.3
Mean computational overhead per mitigation cycle (ms)	17.8	15.2	12.6	10.9
Mean CPU utilization during mitigation (%)	71.6	65.8	61.9	58.4
Mean memory utilization at high network load (%)	69.2	63.7	59.8	56.1
Performance degradation under maximum network scale (%)	16.8	12.9	9.7	6.4
Critical-severity mitigation advantage over adaptive baseline (percentage points)	–	5.6	11.4	19.3
Latency reduction at 800 nodes relative to adaptive baseline (%)	–	23.2	43.7	57.9
Scalability assessment	Limited	Moderate	Good	High

The proposed multi-objective game-theoretic model is compared with relevant baseline approaches in terms of mitigation effectiveness, decision latency, computational overhead, resource utilization, and scalability in **Table 3**. The proposed model has the highest average mitigation success rate of 93.23% and is effective for 87.8% attack severity in critical mode. It also has the smallest decision latency (55.8ms) for a network scale of 800 nodes. The relatively less CPU utilization (58.4%), memory utilization (56.1%) and computational overhead (10.9 ms) demonstrate better efficiency in operation. In general, the results show the performance gains are systematically better in more complex and larger networks.

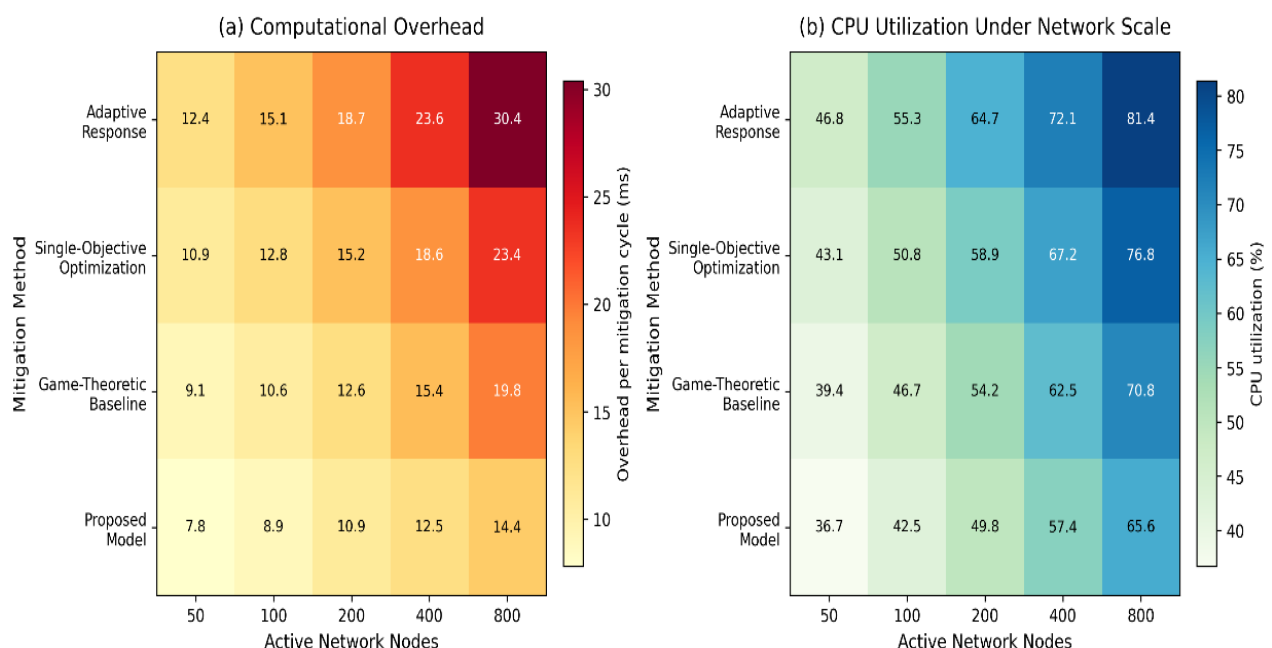


Fig 7. Resource Overhead and Scalability Analysis.

Fig. 7(a) shows the computational overhead per mitigating cycle with growing network size, while **Fig. 7(b)** displays the CPU usage of the process. The two-panel heatmap offers a one-off compact visualization of the comparison of resource efficiency in the presence of heterogeneous network conditions. The proposed model has the lowest computational overhead for all the evaluated sizes of the network, which grows from 7.8 ms at 50 nodes to 14.4 ms at 800 nodes. Likewise, comparing to other CPUs, the utilization range of its CPU is between 36.7% and 65.0%. The average values are comparable to the **Table 3** results for the proposed model with the mean computational overhead of 10.9ms and mean CPU usage of

58.4% respectively. With the growth of network size, the results show that the multi-objective optimization mechanism enhances the effectiveness of mitigation while not requiring a large amount of computing resources.

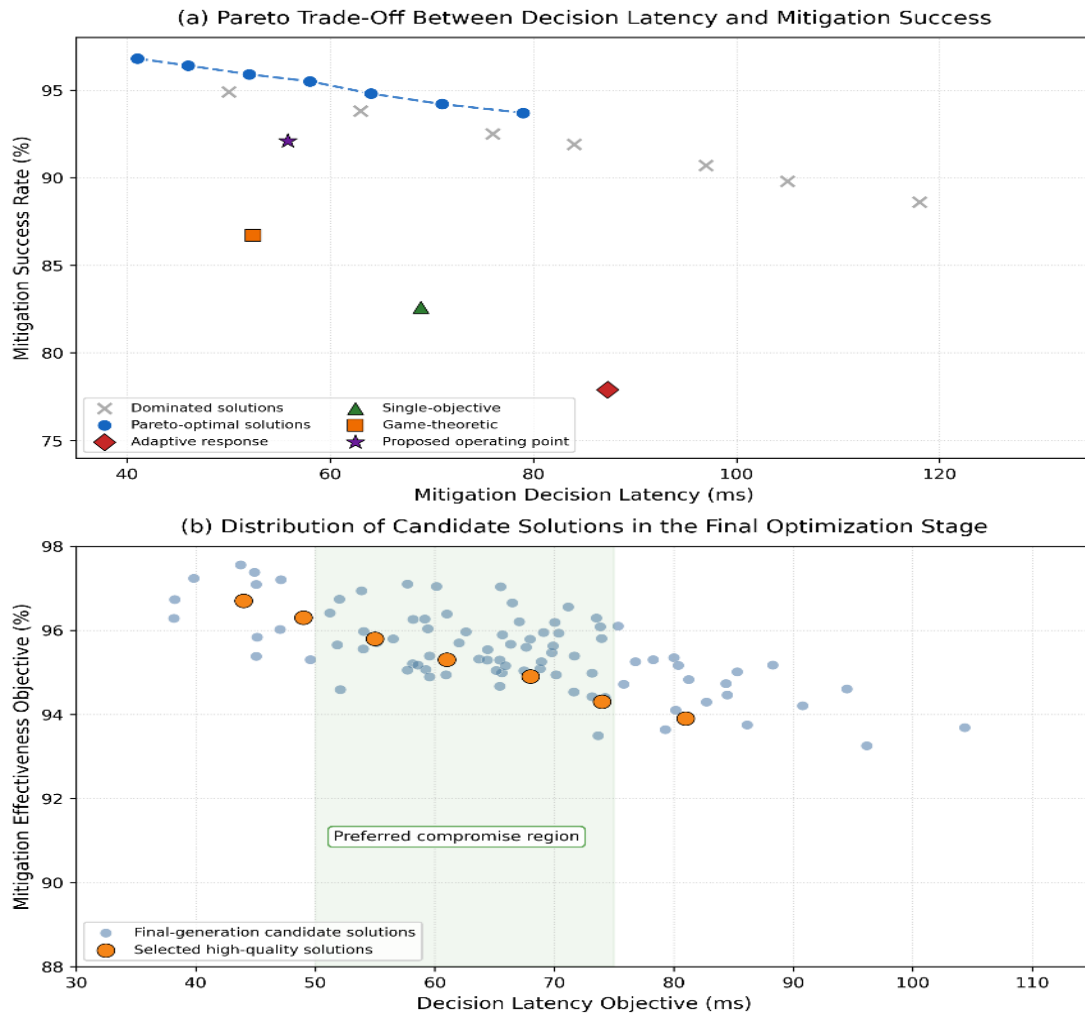


Fig 8. Multi-Objective Optimization Behavior of the Proposed Model.

Fig. 8(a) illustrates the Pareto trade-off between mitigation decision latency and mitigation success rate. The Pareto-optimal solutions define the best achievable compromise between rapid response and effective attack mitigation. The proposed operating point provides a favorable balance, achieving approximately 92.1% mitigation success at a decision latency of 55.8 ms under the corresponding high-severity, large-scale operating condition. **Fig. 8(b)** presents the distribution of candidate solutions in the final optimization stage. The concentration of selected solutions within the preferred compromise region demonstrates the model's ability to identify high-quality trade-off solutions instead of optimizing only a single objective.

V. CONCLUSION

In this paper, an autonomous cyber-attack mitigation Multi-Objective Game-Theoretic Optimization Model (MGTOM) was proposed in the context of heterogeneous network architectures. The proposed framework is a dynamic game-theoretic formulation where both the effectiveness of mitigation and the impact of attacks, along with the reaction time, computational burden, resource consumption and network resilience are taken into account. The adaptive decision mechanism that emerges allows for the selection of defense strategies to adapt to changing attack situation and heterogeneous network constraints. The controlled simulation results show that the proposed model has been consistently advantageous for various evaluating aspects. In overall accuracy, the attack detection and classification analysis achieved 95.08%, and the precision, recall and F1-score were 95.08% and 95.07%, respectively. Further, the classification capability was corroborated using a macro-average AUC of 0.969, which showed good discrimination between benign traffic and various categories of cyber-attacks. The mitigation results demonstrated that the success rate of mitigation on the evaluated attack severity levels was maintained at 93.23% on average by MGTOM. Under the most severe conditions of attack, the proposed model mitigated 87.8% of the attacks, surpassing the next best game-theoretic baseline by seven points. The degradation from low to critical has only been 9.8 % points, which shows increasing robustness to strongly increasing

attack conditions. The proposed framework also exhibited good scalability and efficient operation. For a network size of 800 nodes, the mitigation decision latency was 55.8 ms, 25.2% less than the nearest game-theoretic baseline. The model also obtained a mean computational overhead of 10.9 ms per mitigation cycle along with a mean CPU and memory use of 58.4% and 56.1%, respectively. The results of the Pareto based optimization analysis showed that the proposed framework can provide effective compromise solution between the success of mitigation and decision latency instead of optimizing a single security objective alone.

CRedit Author Statement

The author reviewed the results and approved the final version of the manuscript.

Data Availability Statement

The data supporting the findings of this study are based on the CICIDS2017 dataset and controlled simulation results generated using the proposed Multi-Objective Game-Theoretic Optimization Model. The CICIDS2017 dataset is publicly available through the Canadian Institute for Cybersecurity. The simulation parameters, derived experimental results, and additional data generated during the study are available from the corresponding author upon reasonable request.

Conflicts of Interests

The authors declare no conflict of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

- [1]. M. Wang, J. Liu, Y. Li, E. Tian, and C. Peng, "A comprehensive survey of game-theoretic approaches for networked systems," *Systems Science & Control Engineering*, vol. 14, no. 1, Jan. 2026, doi: 10.1080/21642583.2026.2622131.
- [2]. Aljumah, T. A. Ahanger, and A. Zhumadillayeva, "Game-theoretic security optimization in UAV networks through AI-enabled digital twin intelligence," *Scientific Reports*, Jul. 2026, doi: 10.1038/s41598-026-63521-z.
- [3]. S. K. Zelani, K. V. S. S. Ramakrishna, F. Asiri, A. Alyahya, and S. Basheer, "A reinforcement learning-driven payoff-adaptive game-theoretic framework for secure and reliable operation of mobile ad hoc networks," *Transactions on Emerging Telecommunications Technologies*, vol. 37, no. 4, Mar. 2026, doi: 10.1002/ett.70394.
- [4]. Alajmi, A. Ghandoura, A. Motwakel, and G. Abdelhady, "Game-theoretic adaptive routing and integrated security framework for multi-hop LoRaWAN networks," *IEEE Internet of Things Journal*, pp. 1–1, 2026, doi: 10.1109/JIOT.2026.3675915.
- [5]. Y. Wang, X. Liu, and X. Yu, "Research on joint game-theoretic modeling of network attack and defense under incomplete information," *Entropy*, vol. 27, no. 9, p. 892, Aug. 2025, doi: 10.3390/e27090892.
- [6]. N. Liu, Q.-W. Chai, S. Liu, F. Meng, and W.-M. Zheng, "Mixed strategy analysis in attack-defense game model based on 5G heterogeneous network of CPS using ncPSO," *Security and Communication Networks*, vol. 2022, pp. 1–15, Nov. 2022, doi: 10.1155/2022/1181398.
- [7]. E. F. Siddiqui, M. Haleem, S. F. Ahmad, A. Salhi, A. T. Zamani, and N. Varish, "A multi-layered AI-driven cybersecurity architecture: Integrating entropy analytics, fuzzy reasoning, game theory, and multi-agent reinforcement learning for adaptive threat defense," *IEEE Access*, vol. 13, pp. 170235–170257, 2025, doi: 10.1109/ACCESS.2025.3610526.
- [8]. Z. Han et al., "Smart optimization solution for channel access attack defense under UAV-aided heterogeneous network," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18890–18897, Nov. 2023, doi: 10.1109/JIOT.2023.3281942.
- [9]. H. Mejdi, S. Elmadssia, M. Koubãa, and T. Ezzedine, "A comprehensive survey on game theory applications in cyber-physical system security: Attack models, security analyses, and machine learning classifications," *IEEE Access*, vol. 12, pp. 163638–163653, 2024, doi: 10.1109/ACCESS.2024.3491502.
- [10]. M. F. Saiyed and I. Al-Anbagi, "A game theoretic model for strategic defence selection against DDoS attacks in IoT networks," *IEEE Transactions on Network and Service Management*, vol. 22, no. 5, pp. 4509–4524, Oct. 2025, doi: 10.1109/TNSM.2025.3589901.
- [11]. R. Ranpara, S. K. Patel, O. P. Kumar, and F. A. Al-Zahrani, "Scalable architecture for autonomous malware detection and defense in software-defined networks using federated learning approaches," *Scientific Reports*, vol. 15, no. 1, Aug. 2025, doi: 10.1038/s41598-025-14512-z.
- [12]. Petrillo, A. Pescape, and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 3, pp. 1134–1149, Mar. 2021, doi: 10.1109/TCYB.2019.2962601.
- [13]. L. Khoshnevisan and X. Liu, "A secure adaptive resilient neural network-based control of heterogeneous connected automated vehicles subject to cyber attacks," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 6, pp. 8734–8744, Jun. 2025, doi: 10.1109/TVT.2025.3537869.
- [14]. J. Du et al., "Anti-jamming resource allocation in air-terrestrial integrated networks: A hierarchical game-theoretic MADRL approach," *IEEE Transactions on Cognitive Communications and Networking*, vol. 12, pp. 5380–5392, 2026, doi: 10.1109/TCCN.2026.3657145.
- [15]. M. M. Trigui, M. S. Islam, M. D. Gambo, M. S. Alam, and T. Helmy, "Resource-aware ensemble framework for DDoS detection in SDN via novel game-theoretic feature selection," *IEEE Access*, vol. 14, pp. 1666–1676, 2026, doi: 10.1109/ACCESS.2025.3618519.
- [16]. X. Zhao, J. Guo, J. Liu, and W. Huang, "Game-theoretic and inverse reinforcement learning-based control for vehicle formation under DoS attacks," *IEEE Internet of Things Journal*, pp. 1–1, 2026, doi: 10.1109/JIOT.2026.3710354.

Publisher's note: The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The content is solely the responsibility of the authors and does not necessarily reflect the views of the publisher.

ISSN (Online): 3105-9082