Research on Cooperative Defense Strategy of Swarm Intelligence Awareness Network Based on Bee Colony Algorithm

Zixuan Wan, Kaiwen Lou

School of Computer Science and Information Technology, Harbin Normal University, Harbin, China

Abstract: The Mobile Crowdsensing (MCS) network is susceptible to large-scale task disruptions and systemic collapses under complex attacks due to limited node resources and generalized attack surfaces. Current collaborative defense technologies are still in their nascent stages, lacking a universal collaboration mechanism, and struggling to support precise threat mitigation in dynamic open environments. This paper proposes a security collaborative defense framework that integrates an ensemble learning algorithm with dynamic policy adjustments and an artificial bee colony algorithm. This framework comprises modules such as data access and sharing, proactive prevention, joint sensing, and collaborative response. The study explores an ensemble learning algorithm with dynamically adjustable collaborative strategies, applying it to an attack event detection model to enhance detection accuracy. Meanwhile, the artificial bee colony-empowered collaborative response mechanism establishes a lightweight communication protocol based on three types of messages (active, updated, and summary). It facilitates cross-entity threat intelligence sharing and strategy coordination through TTL hop limits, focus level thresholds, and dynamic neighborhood reconstruction. A dual-loop response chain is established for homogeneous and heterogeneous entities. Homogeneous entities achieve self-healing through logical isolation, link disconnection, offline scanning and removal, and vulnerability patching. Heterogeneous entities rely on traffic filtering, access control, and feature synchronization to establish a defense-in-depth mechanism.

Keywords: Group Intelligence Perception; Collaborative Defense; Artificial Bee Colony

1. Introduction

With the continuous advancement of information technology, the frequency of cyber attacks targeting national critical information infrastructure has surged dramatically, while attack vectors have become increasingly diverse. The challenge of implementing effective cybersecurity defenses in high-intensity cyber warfare scenarios has emerged as a focal point in modern cyber security confrontations. New attack paradigms such as social engineering and advanced methodologies like automation and intelligent targeting have fundamentally reshaped the cybersecurity landscape. This urgent reality underscores the imperative to develop cutting-edge defense technologies that can keep pace with evolving threats.

The openness and wide use of the swarm intelligence perception network (MCS) make it vulnerable to various attacks initiated by malicious users. Under complex network attacks (such as distributed denial of service, worm propagation), it is easy to cause large-scale task interruption and system collapse [1]. Existing collaborative defense mechanisms face three critical challenges: First, the lack of coordination among heterogeneous security entities (endpoints, gateways, servers) hinders effective threat intelligence sharing and policy coordination, making it difficult to establish comprehensive defense synergy. Second, static defense strategies fail to adapt dynamically to evolving attack patterns, resulting in significant delays in detecting and containing advanced persistent threats (APT). Third, resource constraints become evident as centralized detection models increase energy consumption at edge nodes, hindering large-scale deployment. These bottlenecks severely compromise the robustness and service continuity of Management Control Systems (MCS) in high-confrontation environments. To overcome these limitations, this paper proposes a novel collaborative defense paradigm integrating swarm intelligence. The contributions include:

(1) Design an integrated learning algorithm with dynamic strategy adjustment capability, which

can significantly improve the accuracy of attack event recognition by optimizing the weight of weak detectors.

(2) The lightweight communication protocol (based on three types of messages: active, updated, and summarized) was developed using the Artificial Bee Colony (ABC) algorithm to enable low-cost threat intelligence dissemination. A groundbreaking dual-loop response chain-enables self-healing for homogeneous entities through a sequence of "logical isolation-link disconnection-offline scanning-vulnerability remediation", while heterogeneous entities implement layered defense mechanisms via "traffic filtering-access control-signature synchronization".

(3) The collaborative neighborhood is dynamically reconstructed by adopting TTL hop limit and attention level threshold mechanism, which significantly reduces the load of edge nodes.

This scheme provides a verifiable and efficient collaborative defense path for MCS to resist composite attacks.

2. Cyber Security Collaborative Defense Framework based on Swarm Intelligence

The cybersecurity collaborative defense framework based on swarm intelligence comprises four core modules: data access and sharing, proactive prevention, joint perception, and coordinated response. Through inter-module collaboration, this framework not only achieves intelligent spatiotemporal information correlation across security components to generate high-confidence attack event traceability analysis, but also leverages multi-component coordination mechanisms to implement multidimensional collaborative handling of cyber attacks.

The data access and sharing module forms the essential foundation for collaborative perception, with its core function being the aggregation, storage, parsing, and standardization of heterogeneous data from various security components, while enabling efficient cross-component distribution. The proactive prevention technology based on swarm intelligence models potential cyber attack behaviors to construct attack graphs, utilizing swarm intelligence algorithms to identify high-threat critical attack paths, thereby establishing decision-making foundations for joint perception and collaborative response. The swarm-intelligent joint perception mechanism significantly enhances detection accuracy and situational analysis capabilities for complex attack incidents through spatiotemporal correlation analysis of multi-source security data. The collaborative response module leverages multi-component coordination mechanisms, implementing distributed collaborative strategy execution to systematically disrupt and suppress complex cyber attack chains.

3. Network Security Collaborative Detection Technology based on Integrated Learning

Artificial intelligence algorithms have achieved notable progress in detecting cyber attack incidents, yet existing detection algorithms suffer from significant algorithmic errors, sluggish computational speeds, and limited generalization capabilities. Developing integrated network detection models that combine high precision with strong generalization ability has become crucial. To address this, this paper proposes and validates an integrated learning algorithm with a dynamic collaborative strategy adjustment mechanism. When applied to attack detection models, this innovative approach demonstrates substantial performance optimization.

3.1 Integrated Learning Algorithm

Integration learning is a machine learning technology that uses multiple basic learners to form an integrated learning system to achieve better generalization of the learning system. It has achieved great success in various AI applications and has attracted wide attention in the field of machine learning [2]. The Boosting algorithm, a landmark achievement in recent AI research, is a machine learning technique that reduces bias in supervised learning. It achieves this by continuously modifying sample distributions and combining weighted weak detectors to form a robust detector, thereby minimizing generalization errors. The algorithm trains unstable weak detectors in successive iterations, generating a sequence of sub-detectors. Each subsequent sub-detector's training sample subset probability distribution is adjusted using errors from its predecessor, resulting in distinct sub-detectors across generations. The final robust detector combines these sub-detectors through weighted aggregation. Given an input vector containing detector algorithms and training data corresponding to class labels, the algorithm begins with equal weighting for all samples. Subsequently, weak classifiers iteratively train on the dataset. After each iteration, the algorithm adjusts the weight distribution of misclassified samples. This process ultimately produces a set of base classifiers, where superior-performing ones receive higher weight coefficients while weaker ones are assigned lower weights.

3.2 Network Attack Event Detection Technology based on Integrated Learning Algorithm

The core strength of ensemble learning algorithms lies in their ability to develop high-precision detection models through iterative training of weak detectors. Boosting algorithms significantly enhance the accuracy of unstable detection methods like decision trees, neural networks, and support vector machines. Each training iteration produces a sub-detector that improves upon the previous version's performance, making the training process an iterative optimization journey—from unstable to stable detectors. This approach enables the creation of robust detection systems by iteratively training weak detectors through boosting algorithms to meet error thresholds, then combining these weak detectors into a powerful ensemble. Future research should focus on selecting more suitable weak detectors for network security and developing effective weighting formulas for training samples to achieve system-compliant performance, thereby enabling real-time network monitoring and improving detection accuracy.

4. Multi-Security Component Collaborative Response Technology based on Artificial Swarm Algorithm

The hierarchical organization and dynamic topology of modern networks make it challenging to apply intelligent security decision-making methods, which need to deal with and respond to increasingly complex network security situations[3]. In cybersecurity, attack-defense interactions can be modeled as a non-cooperative game between attackers and defenders. Given the significant uncertainties inherent in this process, defense strategies depend not only on the security system's operational status but also on the attacker's strategic choices. Under this strategic coupling relationship, selecting efficient defense strategies has become a critical challenge requiring urgent solutions. The artificial bee colony algorithm achieves swarm intelligence optimization by simulating bees' foraging behavior, demonstrating advantages such as structural simplicity, efficient convergence, and strong robustness.

In the PMABC algorithm, Alrezaamiri et al. defined the effectiveness of implementing artificial bee colony algorithm [4]. The aim is to optimize multiple objectives in software requirements engineering, such as minimizing costs and maximizing performance. A similar algorithm based on bee foraging behavior is implemented in Article [5], which is used to solve the shortest path problem with fuzzy arc weight. Other natural style algorithms, such as the Ant Collection algorithm, have also been implemented to solve this problem, as Di Caprio et al. stated [6]. Another algorithm implementation is FACRO algorithm [4], which can effectively optimize software requirements and outperform other optimization methods in terms of solution quality and computational efficiency.[7]

Therefore, this paper innovatively introduces the algorithm into the multi-security component collaborative defense system, and the specific implementation steps are as follows:

(1) Realize the intelligence of network security entities, so that they have the ability to cooperate and interact with homogeneous and heterogeneous security entities.

(2) Establishing a Multi-Security Entity Interaction Framework. The security entities are uniformly modeled as intelligent nodes supporting periodic and event-triggered message exchanges. To prevent excessive protocol complexity, three standardized message types are designed:-Active Messages,-Update Messages, and-Summary Messages, enabling secure communication between entities. The specific mechanism is as follows:

1) Active messages, serving as neighborhood interaction carriers between cybersecurity entities, are broadcast at 10-30 second intervals. Their packet structure includes message type, TTL (Time To Live), and dynamic threat priority levels. These priority levels dynamically correlate with real-time network threat trends, requiring preset thresholds: communication between entities is not triggered if thresholds are not met; otherwise, information coordination among heterogeneous security entities is

activated. Such messages are strictly confined to neighborhood propagation. The TTL value indicates logical hop count between entities: directly adjacent entities are defined as physical adjacency (TTL=1), while entities requiring intermediary nodes for communication form secondary adjacency relationships (TTL=2).

2) To prevent redundant active information exchange between entities, an update message mechanism is introduced. This mechanism inherits the structural paradigm of active messages. When attention levels dynamically fluctuate due to threat situation changes or neighborhood status updates, update messages will be autonomously triggered for generation, strictly confined to transmission between physically adjacent entities.

3) The summary message is disseminated to participating nodes via multicast mechanism, notifying identified attack events and entity topology positions. This enables dynamic adjacency relationship reconstruction based on neighbor policies, network topology dynamics, or emerging attack trends. The message transmission cycle can be configured as hourly, daily, or weekly intervals. Its lifetime (maximum hop count) is constrained by TTL=255, with a maximum limit of 20 malicious source/target IP addresses per message. Neighbor policies fundamentally characterize the logical distance between entities and physically adjacent nodes. Security entities must synchronize and share network threat alert levels with both their physical neighbors and second-order physical neighbors (physical neighbors of physical neighbors).

(3) To establish an information-sharing mechanism for network threat detection among similar entities, it is essential to address the complexity of composite cyberattacks.-These attacks typically involve multiple atomic attack components, necessitating coordinated multi-component responses. When a single node detects a network threat or anomaly, it automatically disseminates updated or active alerts to peer entities within its physical/logical vicinity. Receiving nodes continuously relay this information to neighboring nodes, creating a chain reaction. Ultimately, all nodes converge on a complete message set. After localized data fusion, they autonomously initiate new rounds of neighborhood broadcasting, thereby generating an iterative aggregation enhancement effect. If the alert level of active messages remains above the security threshold, the system triggers cross-entity cybersecurity interaction protocols (Step 4).

(4) A collaborative sharing mechanism for cyber threat intelligence must be established among heterogeneous security components. This mechanism is designed to automatically trigger message notifications to heterogeneous entities when the threat alert threshold of a specific entity is exceeded, specifically targeting composite attacks originating from multi-dimensional entities including terminals, servers, network devices, gateways, and security perception platforms. Taking the terminal-server-gateway-security-perception-platform architecture as an example, this mechanism enables cross-domain synchronization of threat intelligence, which then transitions into the policy generation phase (Step 5).

(5) The fully-aware platform drives the generation of collaborative response strategies. Serving as the core hub of network information systems, this platform dynamically generates cybersecurity policies through situational awareness and in-depth analysis of multi-source threat intelligence, powered by a decision engine. To collaboratively contain cyber threats initiated by attackers (particularly APT-level attack chains), distributed defense strategies must be deployed across heterogeneous entities to effectively block attack traffic and implement proper response measures.

(6) Isomorphic security node clusters implement threat response strategies through distributed collaboration mechanisms. Taking worm infection incidents on servers as an example, the collaborative response process is shown as follows:

1) Implement logical isolation of infected nodes and cut off network sessions independently;

2) The remaining nodes in the cluster immediately terminate the communication link with the infected node;

3) Start the offline scanning process in the isolation environment to remove malicious code;

4) Deploy vulnerability patches and disable non-essential ports in the topology neighborhood of the infected node to build a defense in depth barrier.

(7) Heterogeneous security entities need to coordinate and consistent response measures to achieve network threat disposal. Taking the server worm infection event as an example, the cross-entity collaborative defense mechanism is

designed as follows:

1) Flow filtering mechanism: The firewall at all levels blocks the worm propagation traffic at the host and network layer;

2) Access control isolation: dynamic access control policies are configured through switches, routers and firewalls to forcibly isolate infected host networks.

3) Feature intelligence synchronization: synchronize worm attack features to intrusion detection system, application firewall and other security components, and establish a closed-loop defense system.

After completing phase (7), the system will re-enter phase (3) through continuous iterative cycles, achieving dynamic evolution of information sharing and response coordination among entities. In engineering deployment scenarios, it is essential to establish highly compatible and comprehensive core parameters such as communication protocols, neighborhood policies, and priority function based on actual cybersecurity conditions and defense architecture requirements.

5. Conclusion

This paper proposes a cybersecurity collaborative defense framework based on swarm intelligence. The technology is designed around collaborative detection and response mechanisms, creating four specialized communication protocols for cybersecurity entities to achieve global awareness and coordinated defense across multiple security components. As swarm intelligence technology remains underdeveloped, the design of these communication protocols requires experimental exploration tailored to specific cyber attack characteristics. Further in-depth research is essential to develop practical and scalable technical solutions that can be widely adopted.

References

[1] ZHAO G, LI Z, WANG J. Hybrid attacks collaborative defense model using an ensemble honey badger algorithm[J/OL]. Computer Networks, 2025, 261: 111149.

[2] YANG Y, LV H, CHEN N. A Survey on ensemble learning under the era of deep learning[J/OL]. Artificial Intelligence Review, 2023, 56(6): 5545-5589.

[3] TANG Y, SUN J, WANG H, et al. A Hierarchical Multi-Agent Reinforcement Learning-Based Network Attack-Defense Game and Collaborative Defense Decision-Making Method [J/OL]. Computer & Security, 2024,142:103871.

[4] ALREZAAMIRI H, EBRAHIMNEJAD A, MOTAMENI H. Parallel multi-objective artificial bee colony algorithm for software requirement optimization[J/OL]. Requirements Engineering, 2020, 25(3): 363-380.

[5] EBRAHIMNEJAD A, TAVANA M, ALREZAAMIRI H. A novel artificial bee colony algorithm for shortest path problems with fuzzy arc weights[J/OL]. Measurement, 2016, 93: 48-56.

[6] DI CAPRIO D., EBRAHIMNEJAD A., ALREZAAMIRI H., et al. A novel ant colony algorithm for solving shortest path problems with fuzzy arc weights [J/OL]. Alexandria Engineering Journal, 2022,61(5):3403-3415.

[7] ABBASZADEH SORI A, EBRAHIMNEJAD A, MOTAMENI H. Elite artificial bees' colony algorithm to solve robot's fuzzy constrained routing problem[J/OL]. Computational Intelligence, 2020, 36(2): 659-681.