Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.042607

ARTICLE

Adaptive Network Sustainability and Defense Based on Artificial Bees Colony Optimization Algorithm for Nature Inspired Cyber Security

Chirag Ganguli[1], Shishir Kumar Shandilya[2], Michal Gregus[3] and Oleh Basystiuk[4,*]

[1]Institute of Technology, VIT Bhopal University, Bhopal, India

[2]School of Data Science and Forecasting, Devi Ahilya University, Indore, 452001, India

[3]Department of Information Systems, Comenius University in Bratislava, Bratislava, 82005, Slovak Republic

[4]Department of Artificial Intelligence, Lviv Polytechnic National University, Lviv, 79013, Ukraine

*Corresponding Author: Oleh Basystiuk. Email: oleh.a.basystiuk@lpnu.ua, obasystiuk@gmail.com

Received: 05 June 2023 Accepted: 27 December 2023 Published: 20 May 2024

ABSTRACT

Cyber Defense is becoming a major issue for every organization to keep business continuity intact. The presented paper explores the effectiveness of a meta-heuristic optimization algorithm-Artificial Bees Colony Algorithm (ABC) as an Nature Inspired Cyber Security mechanism to achieve adaptive defense. It experiments on the Denial-Of-Service attack scenarios which involves limiting the traffic flow for each node. Businesses today have adapted their service distribution models to include the use of the Internet, allowing them to effectively manage and interact with their customer data. This shift has created an increased reliance on online services to store vast amounts of confidential customer data, meaning any disruption or outage of these services could be disastrous for the business, leaving them without the knowledge to serve their customers. Adversaries can exploit such an event to gain unauthorized access to the confidential data of the customers. The proposed algorithm utilizes an Adaptive Defense approach to continuously select nodes that could present characteristics of a probable malicious entity. For any changes in network parameters, the cluster of nodes is selected in the prepared solution set as a probable malicious node and the traffic rate with the ratio of packet delivery is managed with respect to the properties of normal nodes to deliver a disaster recovery plan for potential businesses.

KEYWORDS

Artificial bee colonization; adaptive defense; cyber attack; nature inspired cyber security; cyber security; cyber physical infrastructure

Nomenclature:

Abbreviation	Meaning
ABC	Artificial bees colonization algorithm
NICS	Nature-inspired cyber security
DoS	Denial of service
DDoS	Distributed denial of service

G	Connection between 2 routers
P	Connection from router to cluster
Q	Connection from cluster to router
H	Connection between 2 clusters
f	Immediate connection between router and cluster
R	Routers
C, SW	Switches or clusters
Tr	Throughput
EE	End-to-end delay
IoT	Internet of things
MITM	Man-in-the-middle attacks
ACO	Ant colony optimization

1 Introduction

The Internet is a vast network of nodes or systems connected to each other and is capable of sharing large bases of Information and raw data. This paper demonstrates an Adaptive Defense mechanism to optimize the network traffic flow and secure the process of data transfer in order to maintain the network performance in times of external or internal threats. In order to transform this approach into a working solution, this paper proposes an algorithm based on Nature Inspired Cyber Security (NICS) centred around Artificial Bees Colony (ABC) Algorithmic Approach.

Artificial Bees Colony Algorithm defines the foraging behaviour of the bees in an optimized manner to provide advanced search capabilities. In network security, where the primary focus lies in the fact that the malicious nodes attached externally to the network or the internal nodes that are infected by malicious threat actors are detected on a primary phase before the attack spreads through the production environment. Several modern firewall systems have the capability to match malicious signatures to detect such activities, however, these can have a disadvantage in efficiency and effective utilization of network resources. Artificial Bees Colonization algorithm in such cases, provides the required protocols to maintain the efficiency and efficacy of the network, thus providing an improved recovery from a state of attack to a stable condition.

The main challenge of using NICS lies in the complex and dynamic nature of cyber threats. Adapting nature-inspired algorithms to effectively handle evolving attack techniques and zero-day vulnerabilities requires continuous updates and sophisticated models. Furthermore, these algorithms may suffer from high computational overhead, hindering real-time application in large-scale networks. Nature-inspired algorithms offer innovative and robust approaches to tackle cybersecurity issues. They can enhance intrusion detection, optimize resource allocation, and improve network resilience by mimicking natural processes like swarm intelligence and genetic evolution. Designing adaptive networks is essential to enhance the cyber resilience. These networks can employ dynamic routing algorithms, self-healing mechanisms, and intelligent threat detection systems to continually assess the network's health and adapt in real-time. By enabling rapid response and reconfiguration in the face of disruptions, adaptive networks minimize downtime and limit the impact of cyberattacks, ultimately strengthening the overall resilience of cyber systems. Additionally, these algorithms provide the potential for proactive defense strategies and the ability to adapt to new threats rapidly. Leveraging nature-inspired algorithms effectively can significantly strengthen cyber defense, leading to more secure and sustainable digital environments.

The proposed approach has a distinct capability to detect malicious behaviour in a network by isolating the tentative malicious nodes to further investigate them and it also alters the traffic flow properties of those nodes to control them from unnecessarily flooding the network during a Denial-Of-Service attack. The proposed Nature Inspired Cyber Security Algorithm implementing Artificial Bees Colonization is used for inspecting the effect of a malicious node in a network based on the network properties such as Throughput, EEdelay and Node Packet Delivery Ratio which further helps to pre-detect danger and also helps to keep the network stable enough during an attack to help in faster Disaster Recovery. The said methodology uses a simulated network testbed to visualize the normal and attack throughput difference and compare the fitness of each network node with regard to the parametric graph that defines the effect of an attack on the network intermediaries. The defensive mechanism is then integrated using ABC to determine the effectiveness of presented algorithm to quantify and minimize the amount of packet transfer from the attached malicious nodes on the network, therefore maintaining its throughput ratio while keeping the network stable.

This approach includes a network topology involving 5 clusters consisting of nodes or computing devices and 3 routers connecting them. The nodes are connected in different topologies to have a wider variety of network designing possibilities and the proposed algorithm is applied, which helps in calculating the necessary network parameters like Average Throughput, Packet Delivery Ratio, EEdelay, etc., and taking network snapshots to revert to in specific cases of an attack. The probable malicious nodes are thereafter identified and the network properties are modified accordingly to provide better control over the network and prevent the network from coming to a halt in cases of an attack scenario on the said network or the nodes present in them.

The proposed approach displays the advantages of introducing a nature-inspired approach to cyber security that helps in better identifying malicious activity on a network and revert to a stable state in order to keep the systems available to its clients during an attack phase while containing the attack vectors for further investigation. This enables early detection of adaptive defence processes to Disaster Recovery activity for businesses, such that the businesses can stay in an operational state during an attack scenario.

The motivation behind the proposed research is to enable prompt Disaster Recovery Solutions for various organizations. Most modern-day organizations rely on the Internet to carry out their businesses effectively and they possess security researchers and analysts to mitigate risks in their systems. However, total mitigation of risk is a myth and there are always going to be some vulnerabilities that can disrupt the operations of the said organization. To revert to the attacks, by keeping the customer data safe and also available to them 24 × 7, this paper provides an approach to Recovery in cases of such a disaster.

The scope of this research lies in the domain of efficient response to an attack by an adversary. This includes but is not limited to the fact that the organizations should investigate the source of an attack and take necessary actions while hardening their systems, but also they need to have a plan of action (algorithm) ready that needs to work promptly in cases of an attack to maintain the online presence of the business running at limited capacity such that the resources are always available to the customers and the service providers at all times.

1.1 Paper Organization

In the next section, we have added a literature review of the related research work on Nature Inspired Cyber Security. The methods and methodology of the proposed work along with the algorithms is described in Section 3. The network architecture, results of the incorporated algorithms under different test scenarios and their comparison with existing solutions are presented in Section 4 of the paper. Section 5 provides the contributions in the field of Adaptive Defense. Finally, in Section 6, the paper is concluded and discusses the future research prospects of the work.

2 Related Work

This paper summarises the concept of Adaptive Defense based on a predefined Network Testbed [1], which is used as a base model for the implementation of Artificial Bees Colonization Algorithm based Nature Inspired Cyber Security. The said testbed provides a network infrastructure containing a specified number of nodes connected into different clusters which are further interconnected through routers thus providing a view of modern network systems to test and analyze the malicious nodes in the network.

The paper [2] provides an overview of the increasing effect of damage and socioeconomic losses caused by natural hazards and how the application of Artificial Intelligence approaches to the four phases of disaster management (preparedness, mitigation, response, and recovery) is an efficacious solution. A nature-inspired approach to this factor of disaster management can greatly improve the process. This is defined through an overview of implementing a nature-inspired trust model, which includes a distributed recommendation process of existing network maintenance services, as discussed in paper [3]. Similar applications of bio-inspired approaches have been summarized to be of greater impact in domains of Cloud Security as discussed in paper [4]. This paper provides a study of how swarm, immune and neural algorithms have displayed a prominent impact on cloud security.

There are several researchers that have utilized Nature-Inspired Algorithms for developing efficient solutions to real-world problems. The paper [5] proposes IDLACO (Improving Data Locality using Ant Colony Optimization) approach to improve the overall performance. The paper [6] focuses on IoT or the Internet of Things, learning-based methods, and difficulties after an attack. IoT provides several benefits such as data exchange, but they are vulnerable to cyber-attacks that have the capacity of causing physical and economical damage. Digital Infrastructures have increased the complexity of power grids which has also made them vulnerable to adversaries. Article [7] presents a network model of IEC 61850 based digital substations with DoS attacks. The complexities of these systems can cause uncertainties; therefore, adaptive or deep-learning algorithms are required to be implemented to improve the process of control and decision as discussed in book [8]. Monitoring of the critical infrastructures based on the installed sensors' accuracy and robustness of the algorithms is defined in paper [9]. Data injection attacks can affect the security and reliability of cyber-physical infrastructures. Attackers can hijack sensor measurements and send manipulated data, which could lead to blackouts. The paper [9] studies use cases of high information loss. They propose a Bayesian-based approximation filter to provide accurate supervision. The authors of article [10] propose a framework to make the ant colony optimization (ACO) algorithm more effective to optimize vehicular traffic. Paper [11] utilizes Artificial Bee Colony Algorithm to enable cyber defence. It also showcases the efficiency of implementing Nature Inspired Algorithms in Cyber Security. The article [12] expresses how Artificial Intelligence (AI) can be used to deliver fresh food while maintaining its quality using Artificial Bees Colony Algorithm.

Bio-inspired algorithms offer innovative approaches for enhancing cybersecurity. Genetic Algorithms evolve to detect evolving threats like intrusion patterns. They are effective for handling complex, evolving threats but might require significant computational resources; Ant Colony Optimization optimizes security configurations. They can optimize security configurations and resource allocation, but its performance might be affected by the complexity of the problem; Artificial Immune Systems adapt to anomalies. Their self-learning capabilities make it robust, but it may require extensive tuning for optimal performance; Particle Swarm Optimization efficiently searches for solutions. They are efficient in searching for optimal solutions, but its performance can be sensitive to parameter settings; Bacterial Foraging Optimization optimizes network settings. Their ability to adapt to changing environments is beneficial, but it might require careful parameter tuning; and Swarm Intelligence combines strengths for tasks like intrusion detection and cryptography. They exhibit adaptability and robustness but may have limitations in handling very large and complex systems. Effectiveness varies based on problem complexity and resource demands, making algorithm choice crucial.

In Table 1, we can view a relative distribution of AI-assisted Network Synchronization and Sustainability algorithms that can maintain EE delay, throughput, and packet delivery ratio of the network under sustained load, or which can be further extended to be used in the presence of malicious nodes or in times of attacks as discussed in the proposed algorithm.

Table 1: Exploring the literature on network stability and business continuity is incredibly insightful

Research	Proposed concept	Technology	Key contributions
Ensuring the stability of cyber-physical systems amid data packet dropout and replay attacks using a switching system approach [13].	Preventing packet drop	Mitigation of packet drop and replay attacks	The paper employs LMI techniques to define stability criteria for a system
Maintaining control stability in the presence of DoS attacks [14].	Analysis of networked control systems affected by DoS attacks	ISS of the closed-loop system	The proposed framework offers significant adaptability, allowing for the choice of implementation options that strike a balance between performance and communication resource utilization
Analysing the stability of cyber-physical systems when subjected to intermittent DoS attacks [15].	Investigation into the interaction amidst the cyber system and the physical system	Stability of cyber-physical microgrids	The suggested method highlights that the attack could prompt system-wide oscillations caused by information fluctuations in the attack scenario. As a result, a risk assessment technique is formulated to explore the cyber-physical microgrid system's stability under DoS attacks in greater detail
Ensuring stability in networked control systems using a hybrid-driven mechanism while addressing probabilistic cyber-attacks [16].	Stochastic analysis techniques in Lyapunov stability theory	Networked control systems controller design	Choosing the optimal transmission strategy within networked control systems

(Continued)

Table 1 (continued)

Research	Proposed concept	Technology	Key contributions
Developing a resilient event-triggered controller for networked control systems facing periodic DoS jamming attacks [17].	Conceptual integration of control systems within an RETCS and DoS attacks	Communication mechanism by events triggers	The methodology introduced in this paper emerges based on Lyapunov functional and the characterization of parameters related to DoS, such as triggering parameters, sampling time, and decay ratio
Implementing network event-triggered control systems while denied DoS attacks and application [18].	Investigation if designs and challenges approaches in networked control systems	Methodology with event triggers	The paper proposes a cohesive design strategy for obtaining controller gain, observer gain, and event-triggered weight matrix. Furthermore, it presents a technique to counter DoS attacks

The papers highlighted in Table 1 shows valuable contribution in the field of stabilization and their analysis. However, the primary limitation that the proposed algorithm attempts to solve is the response factor of businesses in case of an attack. This involves but is not limited to the steps the organizations must have in place to efficiently manage and investigate the situation while keeping their work running.

The novelty and contributions in this paper can be clearly proven from the cited research, which adds to the impact of implementing Nature Inspired Algorithms in security aspects of computing. The mentioned approaches have displayed better stability in the implementation process with higher flexibility and increased variation in the ways of effective execution. Selecting appropriate recovery mechanisms is an absolute necessity for businesses dealing with customer data. These can be small, medium or large scaled businesses, but the requirement of keeping effective disaster recovery algorithms in place proves to have a safer impact on the overall management process of the said businesses and helps in maintaining or growing their reputation among their clients. The proposed work provides the algorithmic implementation of an efficient Nature-Inspired process of providing disaster recovery mechanisms to such businesses.

3 Materials and Methods

3.1 Artificial Bees Colonization Algorithm

Artificial Bees Colony Algorithm operates on swarm intelligence principles that is popular for resolving complex problems which are in turn inspired by Nature-Inspired Algorithms that imitate the intelligent nature of natural organisms (for example, Bees) as defined in this paper. Honey Bees show intellectual behaviour for the food searching process which includes them recording ecological incidents [19].

Within the Artificial Bees Colony Algorithm, honey bees are categorized into three groups: Employed Bees, Onlooker Bees, and Scout Bees, with equal numbers of employed and onlooker bees. Employed bees undertake the task of locating and documenting food sources they encounter. Onlooker bees leverage the information gathered by employed bees to search for the most advantageous food sources. Scout bees, in turn, are tasked with exploring dismissed food sources in a randomized sequence [20].

The ABC algorithm originated in 2005 which defined a minimal structure of foraging behaviour of the bees which lead to a collective form of intelligence that included optimal food source, employed and unemployed foragers [21] which was developed to make in addition to today's Artificial Neural Network Training [22,23]. Later, ABC was proven to have a significant advantage over other optimization algorithms that included its simplicity, robustness and flexibility, and its process of handling easier hybridization mechanism with other optimization algorithms [24].

The food Searching process developed by Artificial Bees Colony algorithms includes the involvement of 2 major forms of bees-the Employed Bees and the Unemployed Bees. The said process takes the advantage of foraging behaviour of honey bees.

The ABC algorithm during the processing of an optimized food source undergoes the following options with their search pattern:

- Disown the found source of food
- Optimize the exploited source of food
- Continue exploitation of the nearby food sources
- Foraging in sources that are flagged as an abandoned source

Communication in modern-day computer networks is one of the most important attributes of the flowing process of web data. For an efficient flow of traffic with defined limits, proper use of packet transfer technologies must be in place [25–27]. In today's organizational space, consumers are in high demand for suppliers to get in compliance results with their daily requirements which make the said organizations plan and respond to incidents to add to their business continuity in times of crisis at a predetermined limit [28–32].

The adaptation of the Artificial Bees Colony Optimization algorithm can significantly enhance the sustainability and defense of cyber networks. By leveraging ABC's nature-inspired optimization techniques, cyber networks improve intrusion detection systems, optimize network routing and load balancing, and dynamically allocate resources for increased efficiency [33]. Additionally, ABC can strengthen cyber-physical systems' security and prioritize vulnerability patching. Its adaptive nature enables the development of flexible defense strategies, while optimizing security policies enhances overall network resilience.

The adaptation of the Artificial Bee Colony Optimization Algorithm offers a promising avenue to bolster the sustainability and defense of cyber networks. By mimicking the foraging behavior of bees, this algorithm can be utilized to optimize network resource allocation, improve load balancing, and enhance fault tolerance. Additionally, its decentralized and self-organizing nature aligns with the principles of resilient cyber systems, making it a valuable tool in fortifying networks against emerging threats and ensuring their long-term sustainability.

Adaptive networks can be strategically designed to bolster the resilience of cyber systems against disruptions and attacks. By incorporating self-learning mechanisms and real-time monitoring, adaptive networks can continuously analyze network behavior and identify anomalies indicative of potential threats. These networks can dynamically adjust their configurations and resources to mitigate ongoing attacks, redistributing traffic and implementing protective measures on the fly.

Managing the complexity and interdependencies of global socio-economic networks in the context of cybersecurity requires a multifaceted approach. 1. Establishing robust information-sharing mechanisms and collaboration between public and private sectors is vital to address shared cyber threats collectively. 2. Promoting the adoption of internationally recognized cybersecurity standards and best practices fosters a common ground for mitigating vulnerabilities. 3. Investing in advanced analytics and AI-driven tools aids in comprehending and managing intricate network interdependencies efficiently. Response diversity enhances cyber network sustainability by employing varied defense mechanisms to counter diverse threats, reducing vulnerabilities and aiding rapid recovery. However, implementing diverse responses may increase complexity, maintenance costs, and compatibility issues, necessitating careful balancing to achieve an effective and efficient cybersecurity strategy.

We can thus infer that the potential usage of Nature Inspired Cyber Security for maintaining the efficiency and stability of a computer network would enhance its performance under sustained load or against attack scenarios where one or more malicious nodes may attach themselves to an organization network, disrupting the network traffic flow and causing downtime.

3.2 Proposed Method

The proposed algorithm is based on the Artificial Bees Colonization approach to Nature Inspired Cyber Security which implements a method of Adaptive Defense on Modern Computing systems. Firstly, it generates a solution set of probable malicious nodes thus pre-analyzing attacks on the network and maintaining a dataset of in-flow and out-flow traffic through each node connected to the network. Therefore any change in the traffic flow would generate an alert that could cause a disruption to the network activity by lowering its throughput and increasing the nodes' end-to-end delay. On preliminary detection of the above scenario, the traffic flow is controlled in each node and the network is stabilized during the attack but to mitigate the attack under the reduced throughput and increased end-to-end delay, the network can revert to its previous operating state or previous snapshotted stage when the attack had not taken place thus providing enough time for network security engineers to patch the attacked part of the network. Also, it enhances the process of disaster recovery for a business that was under attack.

The implementation and conceptualization of the discussed algorithm are present in Algorithm 1 which provides a detailed view of the generation of solution sets of probable malicious nodes and analyzing them of their traffic flow to protect the network or at very least keep the network under working condition unless the disaster recovery plan of switching the network back the previously configured snapshot is implementing to reverse the attack scenario to a normal condition.

The network's sustainability is upheld through the analysis and adjustment of its properties, specifically focusing on the connections between routers and clusters, encompassing:

- Router-to-Router connections
- Cluster-to-Cluster connections
- Router-to-Cluster connections
- Cluster-to-Router connections
- Immediate connections

$$\lim_{x\to 500} G(x) + \lim_{x\to 300} P(x) + \lim_{x\to 300} Q(x) + \lim_{x\to 500} H(x) + \lim_{x\to 100} f(x) \tag{1}$$

where,

- x in limits start from 0
- Router to Router Connection *defined as* $G(x)$
- Router to Cluster Connection *defined as* $P(x)$

- Cluster to Router Connection *defined as* $Q(x)$
- Cluster to Cluster Connection *defined as* $H(x)$
- Direct connection between Router and Cluster *defines as* $f(x)$

$$G(x) = G_1(x) + G_2(x) + G_3(x) \tag{2}$$

$$G_1(x) = \left(\lim_{x\to 0} R_1(x) + \lim_{x\to 500} R_2(x) + \lim_{x\to 500} R_3(x)\right) \tag{3}$$

$$G_2(x) = \left(\lim_{x\to 500} R_1(x) + \lim_{x\to 0} R_2(x) + \lim_{x\to 500} R_3(x)\right) \tag{4}$$

$$G_3(x) = \left(\lim_{x\to 500} R_1(x) + \lim_{x\to 500} R_2(x) + \lim_{x\to 0} R_3(x)\right) \tag{5}$$

where, $R_1(x)$, $R_2(x)$ and $R_3(x)$are the pre-defined routing operations of the attached Routers 1, 2 and 3, respectively.

$$H(x) = H_1(x) + H_2(x) + H_3(x) + H_4(x) + H_5(x) \tag{6}$$

$$H_1(x) = \left(\lim_{x\to 0} C_1(x) + \lim_{x\to 500} C_2(x) + \lim_{x\to 500} C_3(x) + \lim_{x\to 500} C_4(x) + \lim_{x\to 500} C_5(x)\right) \tag{7}$$

$$H_2(x) = \left(\lim_{x\to 500} C_1(x) + \lim_{x\to 0} C_2(x) + \lim_{x\to 500} C_3(x) + \lim_{x\to 500} C_4(x) + \lim_{x\to 500} C_5(x)\right) \tag{8}$$

$$H_3(x) = \left(\lim_{x\to 500} C_1(x) + \lim_{x\to 500} C_2(x) + \lim_{x\to 0} C_3(x) + \lim_{x\to 500} C_4(x) + \lim_{x\to 500} C_5(x)\right) \tag{9}$$

$$H_4(x) = \left(\lim_{x\to 500} C_1(x) + \lim_{x\to 500} C_2(x) + \lim_{x\to 500} C_3(x) + \lim_{x\to 0} C_4(x) + \lim_{x\to 500} C_5(x)\right) \tag{10}$$

$$H_5(x) = \left(\lim_{x\to 500} C_1(x) + \lim_{x\to 500} C_2(x) + \lim_{x\to 500} C_3(x) + \lim_{x\to 500} C_4(x) + \lim_{x\to 0} C_5(x)\right) \tag{11}$$

where, $C_1(x)$, $C_2(x)$, $C_3(x)$, $C_4(x)$ and $C_5(x)$ are the predefined switching operations of the attached Switches/Clusters namely 1, 2, 3, 4 and 5, respectively.

The stated limit operations are applicable in accordance with the proposed algorithm which on preparing for probable malicious behaviour of nodes based on the unprecedented change in the overall network throughput, end-to-end delay and packet delivery ratio. The network is supposed to be sustainable under these given conditions or in an attack scenario by transferring the network load on the other attached network intermediaries and voiding the attacked intermediary to prevent the spread of malicious packets to the other nodes present on the network and also reduce the traffic flow in case of a Denial-of-Service attack thereafter switching the network back to a previous state of normal conditions for patching detected flaws and preventing further attacks from taking place thus adding value to the Disaster Recovery plan of the said network under attack.

Let us consider R_3 or Router 3 to be under attack then the routing operations would be switched to R_1 and R_2 to manage the network throughput and end-to-end delay although they will be hampered during an attack the routers would not completely shut down the network due to traffic overflow, rather the network would be operational under reduced capacity until the ROLLBACK operation is triggered by the network administrator.

The process of Disaster Recovery works on the basis of the Proposed Algorithm 2 which keeps monitoring the nodes present in the network. The algorithm keeps taking snapshots of the network and updates it at regular intervals. For every cluster present in the network, the Average Throughput, End to End Delay, and Average Packet Delivery Ratio are taken into consideration when selecting the probable node that could cause an adverse effect on the network. After the Normal and Attack Nodes are segregated, the network properties are modified based on the Packet Delivery Ratio of the network, such that the delivery rate is kept close to the normal ratio even during the time of the attack. This might limit the capacity of the said network but will efficiently keep the network operations running instead of completely letting the servers go down. Immediately after an attack is detected and confirmed, the proposed algorithm will immediately recover the network to a previously taken snapshot and report the possible point of attack to the network administrators to investigate and harden the said systems.

In Algorithm 1, the Adaptive Artificial Bees Colonization Algorithmic approach is displayed in a network architecture to mitigate risks and threats while keeping the network operational during the progress of an attack thus maintaining the stability of the network and reverting back to the safe previously snapshotted state to allow the network engineers to patch flaws in the network, prevent further attacks on the found vulnerabilities.

Algorithm 1: Adaptive ABC algorithm

```
    Input: Target Function
    Output: Optimized Solution Set (Solution)
1: Declare the Bees Colony Population
2: Record the Ratio of Employed and Unemployed bees present in the hive
3: Employed Bees Phase
4:              Choose a random food source
5: Monitor and Record the distance between the food source and the hive
6:      Measure and compare the Quality & Distance to the actual food source
7: if employed bees are done with the exploration phase then
                        [GOTO 8] end else
                        [REPEAT FROM 3] end
8: Onlooker Bees Phase
9:      Calculate the possibility of the chosen food source to the most optimal one
10:     Measure the level of optimization of the current chosen source and try to re-define the
        optimization level to a higher state
11:     Update the chosen food source based on 10
12:     if onlooker bees are done with the exploration phase then
                  [GOTO 13] end else
                  [REPEAT FROM 8] end
13: Scout Bees Phase
14:         Check and Measure the abandoned source of food
15:         Produce the percentage of functional food content from the abandoned source such that
            it is not left behind
16:         Measure the accuracy of the food search procedure outcome
17:             [YES]: Record the location of the optimal food source and the quantity of the usable
                food which can be drawn out from the abandoned source
18:             [NO]: [GOTO 3]
```

The Proposed Algorithm 2 provides a state of implementation of the Artificial Bees Colony Algorithm which is implemented to recover from the under-attack state of the said network thereby enhancing the network capability to remain stable under attack and also speedily recover to its normal condition thereby increasing the attack-reduced throughput and decreasing the attack-increased end-to-end delay in the network. The first part of the algorithm inputs the original network state and defines the nodes present in the same. Once the network architecture is identified, a stable snapshot is captured by the algorithm where all the nodes are in operational state. The second part of the algorithm calculates the network parameters such as Throughput, EEdelay and Packet Delivery Ratio of the nodes present in the network. Thereafter, for each node, Normal and Attack nodes are differentiated and the present network properties are modified in cases of a probable attack scenario. In the final part of the algorithm, the node properties are kept under control such that the network is kept operational during an attack event. Eventually the network is reverted back to the originally snapshotted state. The snapshotted state is the actual stable state of the network which is taken at regular intervals to maintain the running condition of the nodes present in the said network. Additionally, keeping stored states enables recovery to a stable condition faster and provides the required time to investigate raised incidents and improper configurations that could lead to an adversary taking advantage of security holes in a privileged network.

The Disaster Recovery Algorithm has a monitoring functionality in place that runs on each node in the network, which includes the clusters. The monitoring is done based on the output received out of the EE delay, Average Throughput, and Packet Delivery Ratio. Thereafter, each node is selected based on the Calculated value to determine if any attack vectors are observed in their functionality, like reduced throughput, or increased end-to-end delay. If confirmed, then the algorithm executes a set of calculations to efficiently Select the Attack Nodes, which are further controlled to achieve Disaster Recovery of the business based out of the said network.

4 Results

4.1 Architecture

The network architecture used as a reference is a modified version of [1]. The topological view is displayed herewith.

Algorithm 2: Disaster recovery solution using ABC algorithm

```
  Input: Targeted Network State
  Output: ABC Implementation for Network Sustainability Analysis and Disaster Recovery (Solution)
Declare and Node Monitor: 8 (Start: 0, End: 7)
Update Stable Network Snapshot SNAPSHOT  LATEST
$Cluster \leftarrow AverageThroughput, AverageE2EDelay, AveragePacketDeliveryRatio$
SelectAnomalousNode():
        loop $nodes$ for 0 to $7$ do
                SelectNormalNode= chooseAnomalousNode  (NormalOutput  (nodes),
                            AverageThroughput  (normal nodes), AverageED(normal nodes),
        AveragePDR  (normal nodes), start, end)
                SelectAttackNode  = chooseAnomalousNode(AttackOutput(nodes),
            AverageThroughput(attack nodes), AverageED(attack nodes),
```

(Continued)

Algorithm 2 (continued)

```
            AveragePDR(attack nodes), start, end)
        if $SelectNormalNode > SelectAttackNode$ then
            Select Normal node with a parameter value of SelectNormalNode end
else
                Select attack node with a parameter value of SelectAttackNode end
end
ModifyNetworkProperties():
for $nodes \leftarrow 0$ to $7$ do
        if $AttackNode$ then
                Define Network Properties: Packet Flow Rate/Traffic Transfer Ratio
                Modify AttackNode Properties to match Normal Network Properties
    end
        else
                Continue;
    end
  end
RecoverState():
Revert to SNAPSHOT LATEST
```

Within the illustrated network in Fig. 1, three routers—R0, R1, and R2—are interconnected and linked to five clusters: C1SW, C2SW, C3SW, C4SW, and C5SW. Each of these clusters is additionally connected to 10 nodes.

The layout and configuration of the nodes are detailed in Table 2.

To add to the attack defence mechanism, a malicious node is attached to the network to demonstrate DoS attack.

4.2 Comparative Analysis

This section critically compares the proposed method with the existing adaptive defensive algorithm [1].

To contrast the current solution with the proposed approach, this paper showcases multiple attack scenarios referenced from [1]. Additionally, it details the implementation of the adaptive defence strategy employing the Artificial Bees Colony Algorithm, as outlined in this paper's methodology.

The attached Fig. 2 demonstrates the Throughput and EEdelay difference based on the application of the proposed adaptive defence algorithm on the existing attack scenario on an AI-assisted testbed.

The Fig. 2 depicts the performance of the proposed defence mechanism on the Cluster 5 Nodes 2, 3 and 4. In accordance with the presented graph, the Throughput factor has increased by a factor when the defence algorithm is implemented on the attacked nodes 2, 3 and 4, respectively. Also, to add to the existing work, another network parameter (EE delay) was taken under consideration that clearly shows a decrease in the delay in the implementation of the proposed Defense Approach.

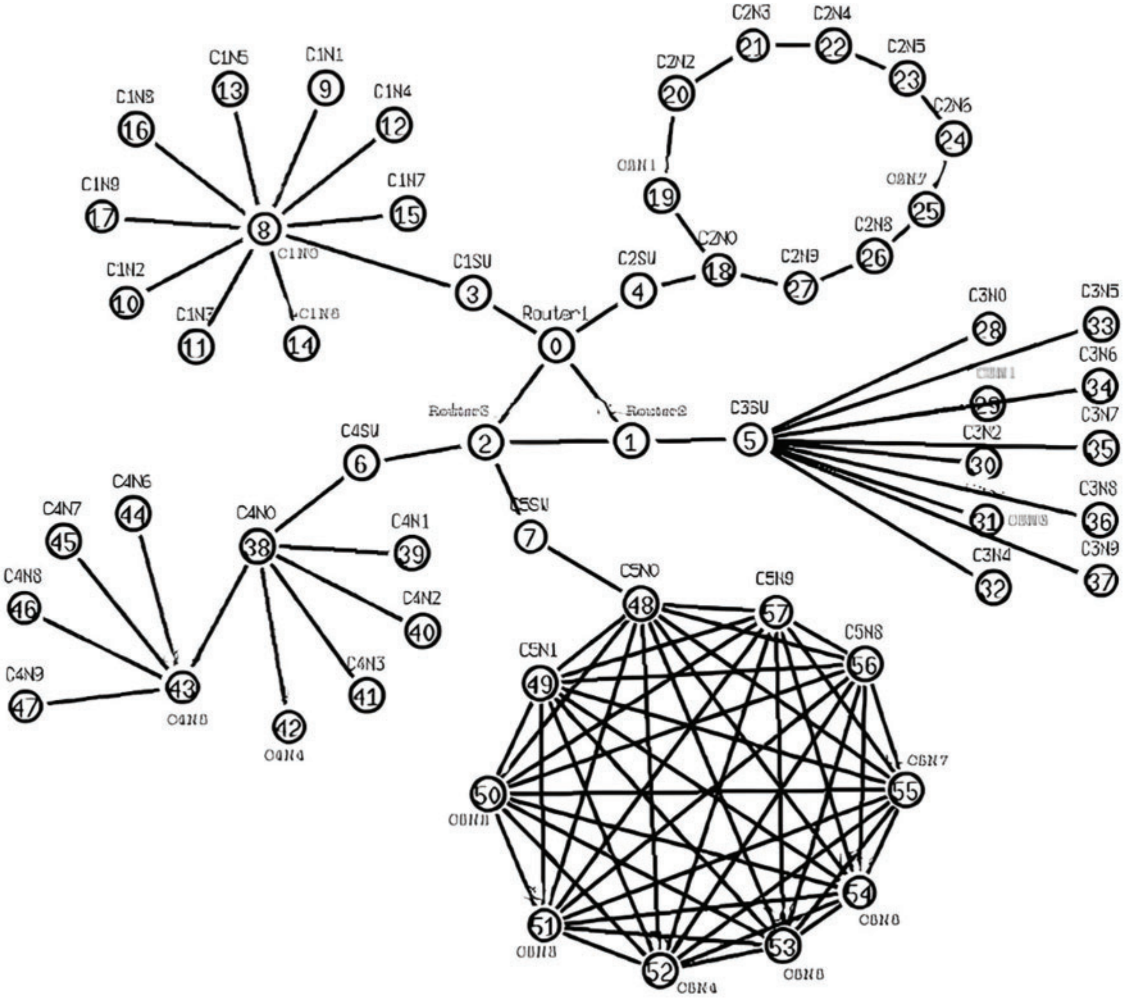

Figure 1: Network testbed architecture [1]

Table 2: Proposed cluster inspection

Cluster	Device label	Topology	Number of nodes
R1–Node #0	1-Router	–	–
R2–Node #1	2-Router	–	–
R3–Node #2	3-Router	–	–
C1SW–Node #3	1 Switch-Cluster	Star	10
C2SW–Node #4	2 Switch-Cluster	Ring	10
C3SW–Node #5	3 Switch-Cluster	Star	10
C4SW–Node #6	4 Switch-Cluster	Tree	10
C5SW–Node #7	5 Switch-Cluster	Mesh	10

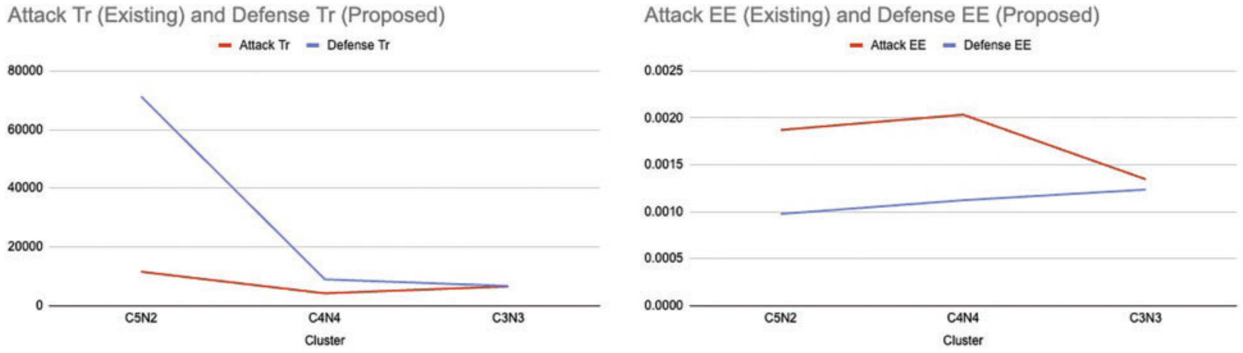

Figure 2: Throughput and EE delay difference on application of proposed defence on the cited attack scenario.
Note: In the presented figure, Red line denoted the existing attack scenario and the Blue line denotes the proposed defence approach

4.3 Test Scenarios

In order to exemplify the efficiency and working principle of the proposed methodology, this paper presents both normal and attack scenarios for the presented network architecture which includes 5 switches interconnected using 3 routers and each cluster is connected to 10 nodes or end-devices. The attack scenario is presented using nodes attached to the original network which are stated to have a higher packet flow ratio as compared to the normal nodes. The normal nodes have a traffic flow rate of 50 Mb and has a capacity of transferring 1000 packets in a pre-determined window whereas the attack nodes are defined to have a packet flow rate of 150 Mb which is more than double the normal node transfer rate and a capacity of transferring 10,000 packets in the same predetermined window. The proposed algorithm generates a graphical overview of the data under attack and defence conditions as proposed in this paper which is capable of stabilizing the network conditions and preparing the network to remain active during the presence of attack nodes by increasing the network throughput and decreasing the EEdelay between the nodes. This enables faster recovery of a business from an attack condition as the network does not completely go offline but instead keeps working under a limited load. The malicious nodes are attached to the nodes and clusters as defined in Table 3.

Table 3: Experimental nodes

Case	Attachment of malicious node
1	Node 2 of Cluster 5
2	Node 4 of Cluster 4

In Case 1: If the malicious node becomes linked to Cluster 5 Node 2, it triggers an alert for a network attack. This connection disrupts the traffic flow and packet transfer rate for current nodes, ultimately reducing the network's throughput and elevating the EE delay.

In Fig. 3, the throughput difference is defined under attack and defence scenarios. The defence mechanism, in the beginning, is not triggered till 2 units of time and on early detection of the presence of an attack node, the algorithm takes control of the node properties and slowly increases the throughput of the network thus stabilizing it under attack and making disaster recovery easier by keeping the network alive and thereafter reverting to a stable state.

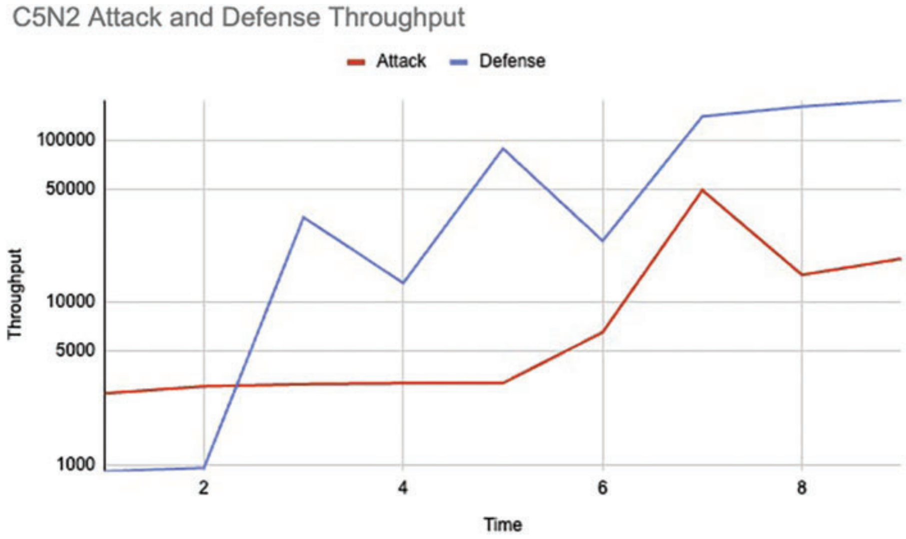

Figure 3: Case 1: average throughput

In Fig. 4, the EE delay graph clearly depicts the increase of the delay when one or more attack nodes are introduced in the network thus causing a lower packet delivery ratio and an unstable network. When the proposed defensive algorithm is aware of the presence of the foreign malicious node, it works on keeping the network alive by reducing the EE delay by controlling the packet transfer rate of the affected nodes.

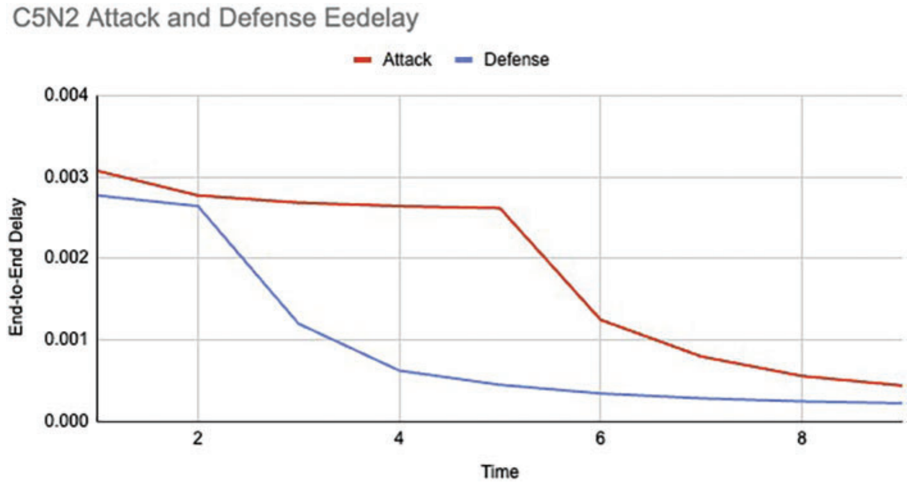

Figure 4: Case 1: average EE delay

–The average Throughput (3) and EE delay (4) the attack scenario in this instance is outlined as follows:

In Case 2: If the malicious node links up with Cluster 4 Node 4, it triggers an alert indicating a network attack. This connection disrupts traffic flow and packet transfer rates for existing nodes, resulting in reduced network throughput and increased EE delay.

In Fig. 5, the throughput difference between attack and defence scenarios is defined. The proposed defence mechanism is not triggered till 2 units of time as seen in the previous scenario, after which it modified the existing nodes' properties to regulate the stability of the network and increase the network throughput to an extent to keep it alive under such an attack scenario.

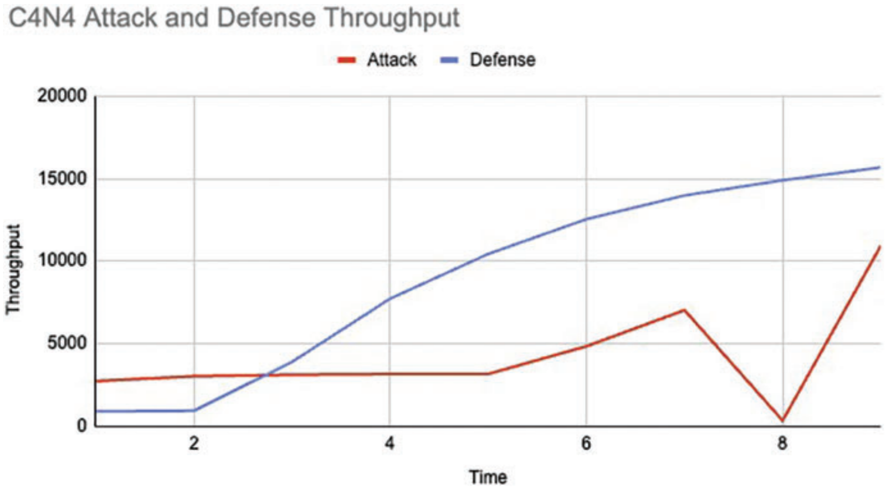

Figure 5: Case 2: average throughput

In Fig. 6, the EE delay difference under attack and defence conditions is displayed which clearly shows the increase of the packet delay under attack conditions thus causing a disruption in the packet transfer rate but the proposed defence algorithm comes into play on detection of an attack, decreasing the End-to-End delay and keeping the network alive thus making disaster recovery more smooth by reverting back to previous stable network state thus giving more time for Incident Response team to fix the vulnerability in the said network.

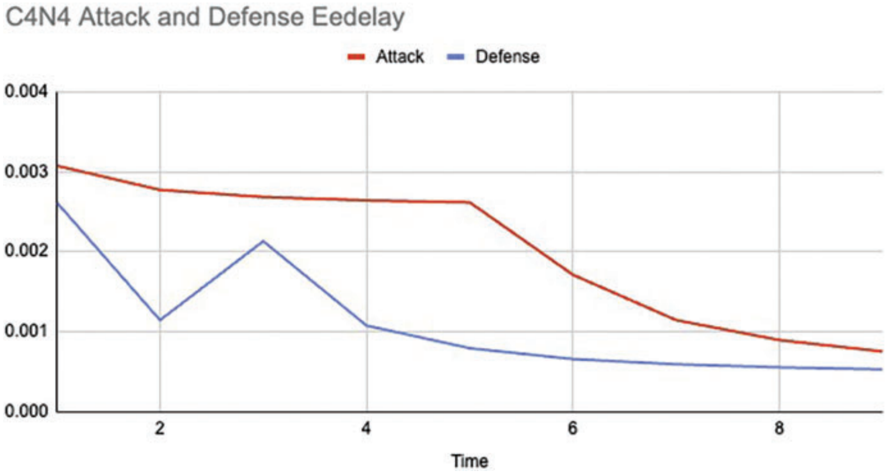

Figure 6: Case 2: average EE delay

–The average Throughput (5) and EE Delay (6) during the generated attack scenario are as follows:

Therefore we can conclude that using Artificial Bees Colony Algorithm's Adaptive Defense to solve various network issues including malicious network activity.

5 Contributions

The proposed algorithm in this paper demonstrates an adaptive defense mechanism that monitors the attack and defense state of the nodes and the clusters collectively in the network for malicious activity which includes abnormal traffic flow and packet transfer rate which causes a significant change in the Network parameters such as Throughput, EE delay and Packet Delivery Ratio. These parameters are responsible for flagging nodes under the defined solution set of performing probable malicious activity. This malicious activity is considered to be a Denial-of-Service attack in this paper. This paper adds on to the existing method defined in [1], by displaying the throughput and EE delay difference under attack and defense scenarios and modifying the nodes' internal packet transfer properties thus early-detecting an attack and preventing them. Before a packet is flagged by a firewall, it is early detected by the proposed algorithm and the attack would be prevented to make sure that the network properties are under control and the network remains alive during an attack thus simplifying the business recovery plan of an organization. The proposed algorithm installs a methodology combining The integration of Nature-Inspired Cybersecurity and Adaptive Defense aims to identify and handle malicious nodes within a network, thereby identifying potential attack scenarios to protect the network. This paper explores the Artificial Bee Colony algorithm, a nature-inspired approach that models and regulates the foraging behaviours of honey bees. The methodology discussed in this paper is having the capability to respond to attacks caused by foreign entities/nodes connected to the network. This enables early detection of attack nodes before the packet reaches the firewall to be flagged. This improves the packet delivery ratio of the network. If the proposed algorithm is not implemented, then under an attack scenario, the network could go offline causing a disruption in business continuity thus making disaster recovery a tougher job. In this case (as discussed in this paper), the network remains online even during an attack thus, preventing a network disruption and maintaining network stability. This also enables businesses to recover from disasters/attacks thus serving the main purpose of this paper. More details and contribution you could check at the Table 4.

Table 4: Summary of paper contribution

Concept proposed	Domain	Contribution
New monitoring and attack prediction model, based on traffic flow analyse	Design of network control system	Approach that monitors the attack and defence state of the nodes and the clusters collectively in the network for malicious activity which includes abnormal traffic flow
Alert flags for performing probable malicious activity	Communication mechanism triggered by events	The proposed framework provide feature for flagging nodes under the defined solution set of performing probable malicious activity

(Continued)

Table 4 (continued)

Concept proposed	Domain	Contribution
Approach that integrates nature-inspired cybersecurity with adaptive defense	Design of network control system	Feature to detect malicious nodes present in a network and manage them thus detecting an attack scenario to safeguard an existing network
Network remains online even during an attack	Adaptive event-triggered methodology	Decentralized and self-organizing nature aligns with the principles of resilient cyber systems, making it a valuable tool in fortifying networks against emerging threats and ensuring their long-term sustainability
Sustainability of the network is maintained by analysing and alerting the network properties	Preventing replay attacks and packet drop	The methodology suggested in this paper emerges within the context of bee colony algorithm, and capability to respond to attacks caused by foreign entities/nodes connected to the network

6 Conclusions

The superiority of the proposed algorithm lies in the factor that it has the capability to constantly monitor the nodes or systems connected to a network based on several network parameters like Throughput, End-to-End Delay, and Packet Delivery Ratio. Thereafter, it can investigate and determine an attack vector or attack node that might have attached itself to the network based on the Adaptive Defense approach, thus maintaining the flow of the network at reduced capacity in order for the business based on the said network to recover quickly and efficiently from the attack posed onto them. Since the algorithm is based on Nature Inspired Cyber Security, its efficiency and efficacy in the execution process remain in the highest order and eliminate chances of false positives and negatives. The efficiency of the proposed algorithm can be optimized to a greater extent by utilizing Nature Inspired Cyber Security Approach.

Future Scope of the Research: The future work on the proposed research could be to reduce the throughput of the attack nodes once they are identified by the presented algorithm to minimize the network outage. Early detection and use of adaptive defense to prevent malicious traffic from the detected nodes could broadly help in securing the network of an organization from a probable attack.

Acknowledgement: Not applicable.

Funding Statement: Not applicable.

Author Contributions: Chirag Ganguli: Data curation, Writing–original draft, Visualization, Investigation, Shishir Kumar Shandilya: Conceptualization, Data curation, Michal Gregus: Methodology, Formal analysis, Oleh Basystiuk: Conceptualization, Methodology.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. K. Shandilya, S. Upadhyay, A. Kumar, and A. K. Nagar, “Ai-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis,” *Fut. Gen. Comput. Syst.*, vol. 127, no. 6, pp. 297–308, 2022. doi: 10.1016/j.future.2021.09.018.

[2] W. Sun, P. Bocchini, and B. D. Davison, “Applications of artificial intelligence for disaster management,” *Nat. Hazards*, vol. 103, no. 3, pp. 2631–2689, 2020. doi: 10.1007/s11069-020-04124-3.

[3] D. Kostoulas, R. Aldunate, F. P. Mora, and S. Lakhera, “A nature-inspired decentralized trust model to reduce information unreliability in complex disaster relief operations,” *Adv. Eng. Inf. Intell. Comput. Eng. Arch.*, vol. 22, no. 1, pp. 45–58, 2008.

[4] M. M. Ahsan, K. D. Gupta, A. K. Nag, S. Poudyal, A. Z. Kouzani, and M. A. P. Mahmud, “Applications and evaluations of bio-inspired approaches in cloud security: A review,” *IEEE Access*, vol. 8, pp. 180799–180814, 2020. doi: 10.1109/ACCESS.2020.3027841.

[5] G. Singh, A. Sharma, R. Jeyaraj, and A. Paul, “Handling non-local executions to improve mapreduce performance using ant colony optimization,” *IEEE Access*, vol. 9, pp. 96176–96188, 2021. doi: 10.1109/ACCESS.2021.3091675.

[6] O. Basystiuk, N. Melnykova, and Z. Rybchak, “Machine learning methods and tools for facial recognition based on multimodal approach,” in *Proc. Modern Mach. Learn. Technol. Data Sci. Workshop (MoMLeT&DS 2023)*, Lviv, Ukraine, 2023, pp. 161–170.

[7] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, “Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways,” *Sens.*, vol. 21, no. 19, pp. 6415, 2021. doi: 10.3390/s21196415.

[8] M. Havryliuk, R. Kaminskyy, K. Yemets, and T. Lisovych, “Interactive information system for automated identification of operator personnel by schulte tables based on individual time series,” in Z. Hu, Q. Zhang, M. He (Eds.), *Advances in Artificial Systems for Logistics Engineering III*, Cham: Springer, 2023, pp. 372–381.

[9] O. Basystiuk, I. Farmaha, and Z. Rybchak, “Exploring multimodal data approach in natural language processing based on speech recognition algorithms,” in *2023 17th Int. Conf. Exp. Design. Appl. CAD Syst. (CADSM)*, Jaroslaw, Poland, 2023, pp. 1–3.

[10] H. M. Khalid and J. Peng, “A bayesian algorithm to enhance the resilience of wams applications against cyber attacks,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016. doi: 10.1109/TSG.2016.2544854.

[11] A. Rehman, M. M. Rathore, A. Paul, F. Saeed, and R. W. Ahmad, “Vehicular traffic optimisation and even distribution using ant colony in smart city environment,” *IET Intell. Transp Syt.*, vol. 12, no. 7, pp. 594–601, 2018. doi: 10.1049/iet-its.2017.0308.

[12] C. Ganguli, C. S.Ganguli, M. Nehrey, and M. Havryliuk, “Adaptive artificial bee colony algorithm for nature-inspired cyber defense,” *Syst.*, vol. 11, no. 1, pp. 27, 2023. doi: 10.3390/systems11010027.

[13] S. K. Sapna Katiyar and R. Khan, “Artificial bee colony algorithm for fresh food distribution without quality loss by delivery route optimization,” *J. Food Qual.*, vol. 2021, no. 4881289, pp. 9, 2021. doi: 10.1155/2021/4881289.

[14] R. E. Abbadi and H. Jamouli, “Stabilization of cyber physical system with data packet dropout and replay attack via switching system approach,” in *4th Conf. Control Fault Toleradnt Syst. (SysTol)*, Casablanca, Morocco, 2019, pp. 325–329.

[15] C. de Persis and P. Tesi, “Input-to-state stabilizing control under denial-of-service,” *IEEE Trans. Automat. Control*, vol. 60, no. 11, pp. 2930–2944, 2015. doi: 10.1109/TAC.2015.2416924.

[16] R. Fu, X. Huang, J. Sun, Z. Zhou, D. Chen, and Y. Wu, “Stability analysis of the cyber physical microgrid system under the intermittent DoS attacks,” *Energ.*, vol. 10, no. 5, pp. 667, 2017. doi: 10.3390/en10050680.

[17] J. Liu, Z. G. Wu, D. Yue, and J. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks," *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. 51, no. 2, pp. 943–953, 2021. doi: 10.1109/TSMC.2018.2888633.

[18] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4271–4281, 2019. doi: 10.1109/TCYB.2018.2861834.

[19] N. Zhao, P. Shi, W. Xing, and C. P. Lim, "Event-triggered control for networked systems under denial of service attacks and applications," *IEEE Trans. Circ. Syst. I: Regular Papers*, vol. 69, no. 2, pp. 1–10, 2021.

[20] J. Bansal, H. Sharma, and S. Jadon, "Artificial bee colony algorithm: A survey," *Int. J. Adv. Intell. Paradig.*, vol. 5, no. 1/2, pp. 123–159, 2013. doi: 10.1504/IJAIP.2013.054681.

[21] S. Kumar, V. K. Sharma, and R. Kumari, "Memetic search in artificial bee colony algorithm with fitness based position update," in *Int. Conf. Recent Adv. Innov. Eng. (ICRAIE-2014)*, Jaipur, Poornima University, 2014, pp. 1–6.

[22] I. Izonin, R. Tkachenko, S. Fedushko, D. Koziy, K. Zub, and O. Vovk, "RBF-based input doubling method for small medical data processing," in *Proc. Int. Conf. Artif. Intell. Logist. Eng.*, Berlin/Heidelberg, Germany, Springer, 2021, pp. 23–31.

[23] D. Karaboga and B. Akay, "Artificial bee colony algorithm on training artificial neural networks," in *Nature Inspired Cooperative Strategies for Optimization (NICSO 2013)*, Springer, 2007, vol. 512, pp. 1–4.

[24] H. Alrezaamiri, A. Ebrahimnejad, and H. Motameni, "Parallel multi-objective artificial bee colony algorithm for software requirement optimization," *Requir. Eng.*, vol. 25, no. 3, pp. 363–380, 2020. doi: 10.1007/s00766-020-00328-y.

[25] D. Karaboga, B. Akay, and C. Ozturk, "Artificial bee colony (ABC) optimization algorithm for training feed forward neural networks," in *Int. Conf. Model. Decis. Artif. Intell.*, Berlin, Heidelberg, 2007, pp. 318–329.

[26] A. Bolaji, A. T. Khader, M. Al-Betar, and M. Awadallah, "Artificial bee colony algorithm, its variants and applications: A survey," *J. Theor. Appl. Inf. Technol.*, vol. 47, no. 2, pp. 434–459, 2013.

[27] L. Kobylyukh, Z. Rybchak, and O. Basystiuk, "Analyzing the accuracy of speech-to-text APIs in transcribing the Ukrainian language," in *Proc. 7th Int. Conf. Comput. Linguist. Intell. Syst.*, Kharkiv, Ukraine, 2023, pp. 217–227.

[28] N. Boyko, L. Mochurad, U. Parpan, and O. Basystiuk, "Usage of machine-based translation methods for analyzing open data in legal cases," in *Proc. Int. Workshop Cyber Hygiene (CybHyg-2019) Co-Located 1st Int. Conf. Cyber Hygiene Conflict Manag. Glob. Inf. Netw.*, Kyiv, Ukraine, 2019, pp. 328–338.

[29] L. Zhihan, S. Minyu, H. Wang, J. Hu, and X. Wu, "A clonal selection optimization system for multiparty secure computing," *Complex.*, vol. 2021, no. 2, pp. 1–14, 2021.

[30] H. Wang, X. Zhang, Y. Xia, and X. Wu, "A differential privacy preserving deep learning caching framework for heterogeneous communication network systems," *Int. J. Intell Syst.*, vol. 37, no. 12, pp. 11142–11166, 2022. doi: 10.1002/int.23036.

[31] V. Manikandan, M. Sivaram, A. Salih Mohammed, and V. Porkodi, "Nature inspired improved firefly algorithm for node clustering in WSNs," *Comput. Mater. Contin.*, vol. 64, no. 2, pp. 753–776, 2020. doi: 10.32604/cmc.2020.010267.

[32] D. di Caprio, A. Ebrahimnejad, H. Alrezaamiri, and F. J. Santos-Arteaga, "A novel ant colony algorithm for solving shortest path problems with fuzzy arc weights," *Alex. Eng. J.*, vol. 61, no. 5, pp. 3403–3415, 2022. doi: 10.1016/j.aej.2021.08.058.

[33] J. Latif, S. Tu, C. Xiao, A. Bilal, S. Ur Rehman, and Z. Ahmad, "Enhanced nature inspired-support vector machine for glaucoma detection," *Comput. Mater. Contin.*, vol. 76, no. 1, pp. 1151–1172, 2023. doi: 10.32604/cmc.2023.040152.