NICS_ABC_Defense_J2 (9).pdf

WORD COUNT	6460	TIME SUBMITTED	02-MAY-2023 06:36PM
		PAPER ID	99295039

Design and Implementation of Adaptive Network Stabilization based on Artificial Bees Colony Optimization for Nature Inspired Cyber Security

Chirag Ganguli[a], Shishir Kumar Shandilya[a], Ivan Izonin[b]

[a] *Vellore Institute of Technology, VIT Bhopal University, Bhopal, India*

[b] *Lviv Polytechnic National University, , Lviv, Ukraine*

Abstract

Adaptive Defense has become an important factor in order to maintain device safety and security on the Internet. In 2021, there were more than 10 billion devices connected to the Internet which is estimated to exceed 25.4 billion by 2030. In order to implement the defensive mechanism approach to security, this paper demonstrates the implementation of the Artificial Bees Colonization (ABC) Approach as Nature Inspired Cyber Security Algorithm. This paper analyzes the defensive approach to Distributed Denial-of-Service attack which limits the amount of traffic flow from each node, therefore, minimizing the attack surface. The simulated network shows the difference between the normal and attack throughput and compares the fitness of the network intermediaries with reference to the parametric graph that shows the effect of a simulated attack on each network intermediary. Thereafter, the state of defense from the ABC's point of view shows the effectiveness of the proposed algorithm in detecting and minimizing traffic flow from malicious nodes thus, maintaining the network throughput while keeping the network stable.

The proposed algorithm introduces an Adaptive Defense Approach that works recursively on the nodes attached to a network of clusters that prepares a solution set of probable malicious nodes that are attached to the network. The detected nodes are then analyzed by their properties based on the network parameters such as Network Throughput, End-to-End Delay, and Packet Delivery Ratio. On change in any of the factors in the devised properties, the

node or cluster of nodes is marked as malicious and the rate of traffic flow along with the packet delivery ratio is reduced to match the normal node's generic properties such that the hammering of the network with traffic is done under a controlled environment and the network works with reduced performance but does not halt even under attack thereby, maintaining business continuity under attack scenario.

Keywords: Nature Inspired Cyber Security (NICS), Artificial Bee Colonization Algorithm (ABC), Network Simulation, Adaptive Defense, Business Continuity

1. Introduction

Internet as a whole is a very large scale, complex and dynamic system that is difficult to model and analyze [1]. With the ever-growing popularity of the Internet, keeping users safe on the Internet should be a primary focus. Since there exists no possibility of preventing attackers from doing cyber crimes, we can at least protect our systems from being attacked by following certain rules and guidelines and implementing top-notch security solutions like Adaptive Defense Approach to Network Security. To implement this, we use the optimized Nature Inspired Cyber Security Algorithm as they tend to provide far more accuracy as compared to the traditional algorithms. For critical infrastructures, that are complex cyber systems forming the core area of modern-day computing, reliable and secure operation is mandatory. The ever-growing threats to physical and cyber-based systems are categorized into three domains: (i) Attack on the system themselves (ii) Attack by the internal systems, and (iii) attack using the internal systems [2].

The Adaptive Defense mechanism has enhanced the process of continuously securing Cyber Systems from adversaries. Nature Inspired Cyber Security (NICS) inspired Adaptive Defense has proved to have a better experimental analysis of system vulnerabilities and therefore better performance as compared to traditional algorithms. This paper demonstrates the implementation of the Artificial Bees Colonization Nature Inspired Cyber Security Algorithm in detecting and analyzing the effect of an attack on the End-to-End Delay, Throughput, and Packet Delivery Ratio of a network. The Artificial Bees Colony Algorithm hereby implemented is an optimization algorithm for

detecting Intrusions in a network and preparing an approach to reduce the attack surface by early detection mechanism on the said attack.The Adaptive Defense approach is introduced to enhance the concept of early detection using continuous monitoring of the nodes in the network. Without the proposed approach of defense, a modern-day firewall implements signature-based detection which may increase undesirable false positives and negatives. This proposed algorithmic approach not only performs early detection of malicious activity in the network but also prevents an attacker from bombarding a network with a high traffic rate, therefore, maintaining the stable state of the network while the business tries to recover from the attack. The process of the Early Detection phase as defined in the proposal, provides an improved way to secure the network architecture while keeping into consideration the present state of the network as compared to an earlier stage which was a working stable configuration with minimal concerns. This includes continuous monitoring of the state of network parameters of all the nodes connected to a network and adding onto the existing match of signatures to the newly identified ones, thus identifying attack scenarios on an adaptive defense scale. This ensures the detection of probable malicious packets sent/received by the network before they are transmitted to modern-day firewalls for further validation and mitigation.

2. Related Work

AI-assisted Network Testbed is a base testbed used to provide Nature Inspired Cyber Security based adaptive defense [3]. The testbed explains experimental solutions on the application of adaptive defense mechanisms on different network topologies like star, bus, and mesh thus providing a method to implement Nature Inspired Cyber Security for Modern Day Systems.

The effectiveness of implementing the Artificial Bees Colony algorithm is defined in The PMABC algorithm, [4] which is designed to simultaneously optimize multiple objectives in software requirement engineering, such as minimizing cost and maximizing performance. A similar algorithmic implementation based on the foraging behavior of bees is defined in article [5] which is used for solving shortest path problems with fuzzy arc weights. Other nature-inspired algorithms like the Ant Colony algorithm are also implemented to solve this problem as mentioned in [6] . ABC is also used for solving Robot's Fuzzy constraint routing problems as defined in article [7]

. Another algorithmic implementation is the FACRO algorithm [4] which is able to effectively optimize software requirements while outperforming other optimization methods in terms of both solution quality and computational efficiency.

Table 1 gives a detailed summary of several Network Stabilization Algorithms which introduced the Machine Learning Approach to stabilize a network under load. These approaches can be modified using the proposed algorithm to make use of Nature Inspired Cyber Security based Adaptive Defense to enable stabilizing a network under attack thus maintaining the business continuity model for small to large businesses that are solely dependent on online distribution and management of resources.

PAPER	CONCEPT PROPOSED	DOMAIN	CONTRIBUTIONS
Stabilization of Networked Control Systems With Hybrid-Driven Mechanism and Probabilistic Cyber Attacks [8]	Lyapunov stability theory and stochastic analysis techniques	controller design problem of networked control systems	Selecting appropriate transmission strategy in networked control systems
Stability Analysis of the Cyber Physical Microgrid System under the Intermittent DoS Attacks [9]	Analysis of interaction between the cyber system and the physical system	Cyber-physical microgrid stability	The proposed method shows that attack could cause system level oscillation with the information variation in attack scenario, thus a risk assessment method is prepared to further investigate the cyber physical microgrid system's stability under DoS attacks.
Input-to-State Stabilizing Control under Denial-of-Service [10]	Analysis of networked control systems in the presence of Denial-of-Service (DoS) attacks	Input-to-state stability (ISS) of the closed-loop system	The proposed framework has high flexibility that allows choice between implementation options that trade-off performance and communication resources
Stabilization of Cyber Physical System with Data Packet Dropout and Replay Attack via Switching System Approach [11]	Stabilization of Cyber Physical System with Data Packet Dropout and Replay Attack via Switching System Approach	Stabilization of Packet Drop and Replay Attacks	The paper makes use of Linear matrix inequality (LMI) to provide stabilized condition to a system.
Event-Triggered Control for Networked Systems Under Denial of Service Attacks and Applications [12]	Investigation of controller designs and synthesis issues of networked control systems under denial-of-service (DoS) attacks	Adaptive Event-Triggered Methodology	The paper proposes a joint design method to obtain controller gain, observer gain and event-triggered weight matrix. It also proposes a method to eliminate Denial-of-service attacks.
Resilient Event-Triggered Controller Synthesis of Networked Control Systems Under Periodic DoS Jamming Attacks [13]	Synthesis concept of networked control systems under Event-triggered communication scheme (RETCS) and Denial-of-Service attacks	Event-triggered Communication mechanism	The proposed methodology in this paper surfaces under Lyapunov functional and characterization of DoS parameters, triggering parameters, sampling time and decay ratio.

Table 1: Summary of Related Work in Network Stability and Business Continuity

2.1. Comparison with other nature-inspired algorithms

ABC (Artificial Bee Colony) Approach has been used to several optimisation issues, including network security. It is crucial to compare the ABC method with that of other typical nature-inspired algorithms for network security. The Particle Swarm Optimisation (PSO) method is one of the most used algorithms in network security. It is based on the social behaviour of fish and birds, is renowned for its speedy discovery of ideal solutions. Studies have

shown that PSO performs better than the ABC method in some optimisation situations, particularly those with a lot of variables. The Ant Colony Optimisation (ACO) algorithm is another method that draws inspiration from nature and is utilised in network security. ACO, which is frequently used in routing and network optimisation, is based on the foraging behaviour of ants. The ACO algorithm has demonstrated higher performance in various network security applications when compared to the ABC strategy, particularly those that involve path-finding issues. In some optimisation challenges, Genetic Algorithms (GAs), which are also frequently employed in network security, outperform the ABC strategy. GAs is frequently utilised in network security applications like intrusion detection and network routing since they are based on the principles of genetics and evolution. In conclusion, the ABC method is an algorithm that draws inspiration from nature and has been used to several optimisation issues, including network security. Nevertheless, depending on the optimisation problem and the application in network security, its performance varies with respect to other nature-inspired algorithms like PSO, ACO, and GA.

3. Modified Artificial Bees Colonization Algorithm (ABC)

The artificial Bees Colony meta-heuristic technique is revitalized through the spontaneous food-foraging behavior of bees. Bees tend to show specific intellectual conduct while scouting for a food source by memorizing the ecological incidents and gathering and distributing the information [14]. However, for optimization purposes, ABC preserves use the use of exploring the entire search space at the loss of better solution search [15].

The Artificial Bees Colony Algorithm grows back to 2005 when it was evaluated using multi-dimensional and multi-variable optimization problems [16] which was later used in 2007 for the training of Artificial Neural Networks [17] [18]. In 2011, a huge increase in the number of ABC algorithms was utilized, where a series of applications, modifications, and hybridization with different optimization algorithms were used to better the performance of ABC [19].

The artificial Bees Colony Algorithm comprises 2 types of bees functioning - the Employed and the Unemployed Bees, who perform their own set of actions to help find an optimal food source. The employed bees are in charge

of carrying nectar from a random food source and putting it in the hive. They perform 3 sets of actions based on their way of exploiting food sources:

- Abandon the exploited food source
- Call unemployed bees to optimize the found food source
- Keep exploiting the existing source

The unemployed bees consist of onlookers and scout bees. The onlooker bees keep track of the employed bees and exploit food sources based on the greedy search mechanism, thus selecting an optimal source. The scout bees then confirm the food source set or start searching for a better food source.

Network Stability and Efficacy are of core importance in the enterprise and in daily aspects of modern computing. Enterprise strategy is centered around processes and their associated services where processes include activities that are expected to deliver value to its customers [20]. Organizations and the impact in their business are aimed at business sustainability and their efficient response system to entail added value to the organizational artifacts [21].

On proper consideration of the current network dynamics, it is necessary for a network to adapt to current status automatically which is not possible in traditional networks as they are difficult to be configured [22].

Therefore, the use of Nature Inspired Cyber Security for network stabilization would enhance the efficiency and efficacy of the network not only under load but also under an attack scenario through the attachment of a single malicious node or a cluster of malicious nodes.

4. Proposed Method

The proposed work discussed in the paper is based on implementing the Modified Artificial Bees Colony Algorithm to stabilize a network during an attack scenario. It includes early detection of malicious behavior of a network and stabilizing it by controlling the in and out traffic flow from each node present in a cluster on a network. This is made possible by implementing Adaptive Defense Approach to learn about an attack mechanism and implement a defensive approach to mitigate the attack while keeping the nodes live on the network.

The algorithmic implementation of ABC that is used to define the objective of this paper is displayed in 1. In this proposed method, the scout bees not only store the optimal food source but also store the food available that can be utilized at an initial state from an abandoned food source. This will keep the abandoned source active for backup for a certain period of time.

The stabilization of the network can be mathematically represented as shown below by limiting the traffic flow between Router - Router, Cluster - Cluster, Router - Cluster, Cluster - Router, and Direct Connections.

$$\int_0^{500} G(x)\,dx + \int_0^{300} P(x)\,dx + \int_0^{300} Q(x)\,dx + \int_0^{500} H(x)\,dx + \int_0^{100} f(x)\,dx$$

where,

- G(x) is Router to Router Connection
- P(x) is Router to Cluster Connection
- Q(x) is Cluster to Router Connection
- H(x) is Cluster to Cluster Connection &
- f(x) is Direct connection between Router and Cluster

$$G(x) = G_1(x) + G_2(x) + G_3(x)$$

$$G_1(x) = (\int_0^0 R_1(x)\,dx + \int_0^{500} R_2(x)\,dx + \int_0^{500} R_3(x)\,dx)$$

$$G_2(x) = (\int_0^{500} R_1(x)\,dx + \int_0^0 R_2(x)\,dx + \int_0^{500} R_3(x)\,dx)$$

$$G_3(x) = (\int_0^{500} R_1(x)\,dx + \int_0^{500} R_2(x)\,dx + \int_0^0 R_3(x)\,dx)$$

where,

$$R_1(x), R_2(x)$$

and

$$R_3(x)$$

are routing operations of Routers 1, 2, and 3 respectively.

$$H(x) = H_1(x) + H_2(x) + H_3(x) + H_4(x) + H_5(x)$$

$$H_1(x) = (\int_0^0 C_1(x)\,dx + \int_0^{500} C_2(x)\,dx + \int_0^{500} C_3(x)\,dx + \int_0^{500} C_4(x)\,dx + \int_0^{500} C_5(x)\,dx)$$

$$H_2(x) = (\int_0^{500} C_1(x)\,dx + \int_0^0 C_2(x)\,dx + \int_0^{500} C_3(x)\,dx + \int_0^{500} C_4(x)\,dx + \int_0^{500} C_5(x)\,dx)$$

$$H_3(x) = (\int_0^{500} C_1(x)\,dx + \int_0^{500} C_2(x)\,dx + \int_0^0 C_3(x)\,dx + \int_0^{500} C_4(x)\,dx + \int_0^{500} C_5(x)\,dx)$$

$$H_4(x) = (\int_0^{500} C_1(x)\,dx + \int_0^{500} C_2(x)\,dx + \int_0^{500} C_3(x)\,dx + \int_0^0 C_4(x)\,dx + \int_0^{500} C_5(x)\,dx)$$

$$H_5(x) = (\int_0^{500} C_1(x)\,dx + \int_0^{500} C_2(x)\,dx + \int_0^{500} C_3(x)\,dx + \int_0^{500} C_4(x)\,dx + \int_0^0 C_5(x)\,dx)$$

where,

$$C_1(x), C_2(x), C_3(x), C_4(x)$$

and

$$C_5(x)$$

are switching operations of Switches / Clusters 1, 2, 3, 4 and 5 respectively.

These operations are applicable under attack. When the attack is identified by the proposed algorithm at any of the network intermediaries, the load will be shifted to a different node, therefore, maintaining the network stability even under attack. To show the attack, this paper presents the integral limit from 0 to 0 to nullify the network traffic to/from the attacked node.

For example, if Router 1 is identified to be under attack, the routing would be shifted between Router 2 and 3 to maintain the network packet transfer

with a percentage of network performance loss but no hindrance/drop in the network connectivity. This helps in business continuity and prevents complete network shutdown when under attack.

In algorithm 1, the algorithmic implementation of the Modified Artificial Bees Colony algorithm is displayed in a live network to detect and mitigate threats while keeping the network live even under sustained attack, therefore maintaining network stability and performance metrics even under attack.

The algorithm 2 defines the process of implementing the Artificial Bees Colony Algorithm which is focused majorly on stabilizing the network performance. In the proposed modified algorithm, the bees go through a list of malicious nodes solution set and select probable malicious nodes, and modify their network properties by limiting their traffic flow rate and delaying the point at which the packet flow starts, thereby making the node as any other normal node, reducing the End-to-End delay and maintaining the network stability.

The proposed algorithm studies the Network properties of each node that are present in the network and selects them based on certain parameters as defined in algorithm 2 . These selected nodes are determined as probably malicious nodes that have some differences in the Average Throughput, End to End Delay, and Packet Delivery Ratio. On determining the differences in the selected nodes they are stored in an array where the comparison of the properties is made according to a previous stable state of the said network. On determining the difference, the network properties are modified to try and match the previous stable state. This reduces the attack scenario effects, on the network where a bulk of unintended packets are bombarded for disrupting internal services, thereby reducing the disruption to the said network and preventing a halt in the business available, and ensuring its continuity.

5. Experimental Setup

5.1. Network Architecture

The Network Architecture used in this paper is derived from [3]. The network architecture diagram is present herewith in figure 1.

Algorithm 1: Modified ABC Algorithm

Input: Target Function

Output: Most Optimal Bees Solution Set (Solution)

Initialize the bees' population in the hive

Measure the density of Employed & Unemployed Bees present in the population

Employed Bee Phase

    Select a food source location

    Measure the distance of the food source from the hive and its quality

    Compare the quality and distance to the original source

if *employed bees have completed the exploitation process* **then**

    [GOTO 8]

end

else

    [REPEAT FROM 3]

end

Onlooker Bee Phase

    Measure the probability of the selected food source to be optimal

    Try to increase the level of optimization from the above source.

    Compare and update the food source

if *onlooker have completed the exploitation process* **then**

    [GOTO 13]

end

else

    [REPEAT FROM 8]

end

Scout Bee Phase

    Evaluate the abandoned or non-healthy food source

    Try to gain a percentage of useful food content from the abandoned source such that the abandoned food source is not left undervalued.

Evaluate the optimized food search process.

    [YES]: Gather the position of the optimal food source and the quantity of the food that can be drawn out from the abandoned food source.

    [NO]: [GOTO 3]

Algorithm 2: Network Stabilizer using ABC Algorithm

Input: Target Function

Output: ABC Implementation for Network Stability (Solution)

Initialize Nodes: 8 (Start: 0, End: 7)

$Cluster \leftarrow$
$AverageThroughput, AverageE2EDelay, AveragePacketDeliveryRatio$

SelectAnomalousNode():

for $nodes \leftarrow 0$ ***to*** 7 **do**

    SelectNormalNode =
     selectAnomalousNode(Normal_Output(nodes),
     AverageThroughput(normal_nodes), AverageED(normal_nodes),
     AveragePDR(normal_nodes), start, end)

    SelectAttackNode = selectMaliciousNode(Attack_Output(nodes),
     AverageThroughput(attack_nodes), AverageED(attack_nodes),
     AveragePDR(attack_nodes), start, end)

    if *SelectNormalNode* > *SelectAttackNode* **then**

        Select Normal node with parameter value of
         SelectNormalNode

    end

    else

        Select attack node with 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

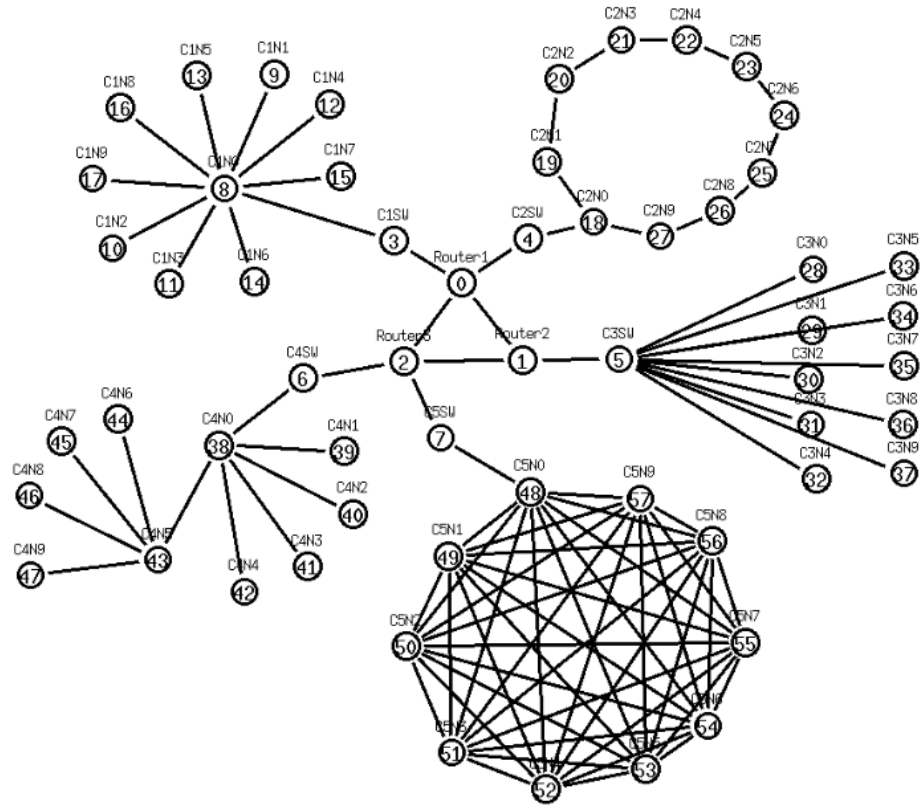

Figure 1: Network Architecture [3]

In the defined network architecture with cluster information as described in table 2, there exist 3 routers - R0 (Router 1), R1 (Router 2), and R3 (Router 3). The routers are in turn connected to 5 clusters - C1SW, C2SW, C3SW, C4SW, and C5SW. The clusters consist of 10 nodes and 15 nodes for different scenarios as described in the paper.

To demonstrate the attack-defense scenario, a malicious node is attached to perform a Denial-of-Service attack scenario on the architecture. The malicious node mentioned in the paper is defined to have a higher network traffic flow as compared to the node properties and is therefore defined to transfer more packets per time period.

CLUSTER NAME	NETWORK DEVICE	TOPOLOGY	NUMBER OF NODES
R1 - Node 0	Router (Router 1)	-	-
R2 - Node 1	Router (Router 2)	-	-
R3 - Node 2	Router (Router 3)	-	-
C1SW - Node 3	Switch (Cluster 1)	Star Topology	10 / 15
C2SW - Node 4	Switch (Cluster 2)	Ring Topology	10 / 15
C3SW - Node 5	Switch (Cluster 3)	Star Topology	10 / 15
C4SW - Node 6	Switch (Cluster 4)	Tree Topology	10 / 15
C5SW - Node 7	Switch (Cluster 5)	Mesh Topology	10 / 15

Table 2: Cluster Information

The defense scenario is expressed in the form of modification of the malicious node properties by minimizing the traffic flow and maximizing the packet delivery ratio from and to the normal node, thereby making the network work as expected.

The active testing scenarios as demonstrated below show the testing phase network performance under attack. The defense mechanism is clearly shown to reduce the End-to-End delay of the network as compared to the attack scenario. Although the delay is not the same as the metric calculated under normal conditions.

6. Comparison of Proposed Method with Existing Solution

The following subsection provides an overview of the effectiveness of the proposed algorithm against the existing defensive approach.

In order to compare the existing solution [3] with the proposed method, this paper uses the attack scenario from [3] and implements the defense mechanism using Artificial Bees Colony Algorithm.
The throughput difference in applying the proposed defense algorithm on the attack scenario described in [3] is displayed below in figure 2. This provides an overview of the effectiveness of the proposed method when the attack node is attached to Node 9 of Clusters 3, 4, and 5 respectively.

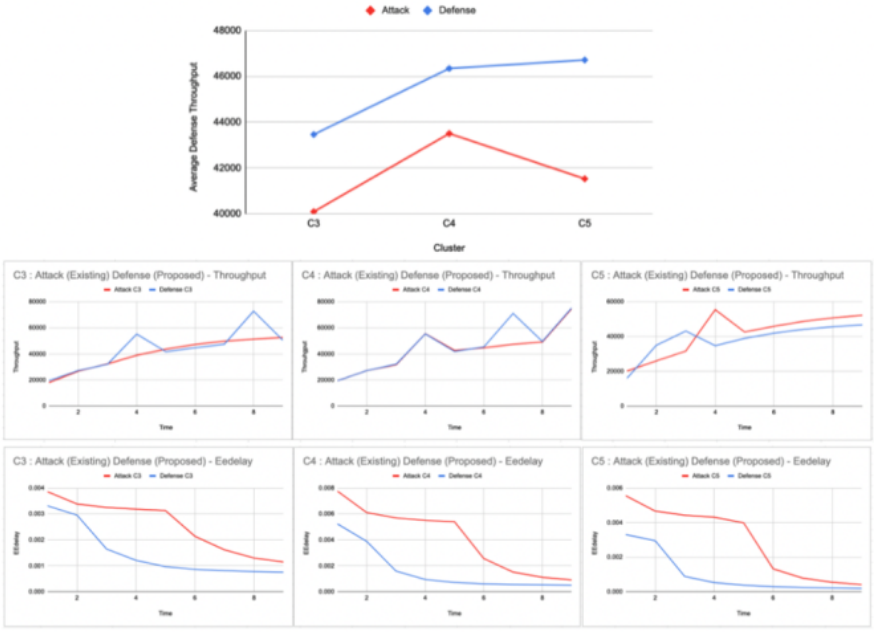

Figure 2: Throughput difference on the application of proposed defense on the cited attack

To further enumerate the proposed defense mechanism, this paper uses another network property (End-to-End Delay) to determine the efficacy of its performance under attack and the stability of the network thereby adding to the business continuity as focused on in this paper.

7. Test Scenarios

7.1. Scenario - 1

To demonstrate the working of the proposed algorithm, this paper uses the normal and attack scenarios for the network architecture comprising 3 routers, 5 switches, and 10 nodes or end nodes connected to each switch/cluster. For an attack scenario, a malicious node having a higher rate of traffic flow is introduced in the network. The node has a property of traffic flow of 10,000 packets and a packet flow rate of 100Mb. The defense mechanism used in this recognizes the malicious node and reduces the network properties, therefore, decreasing the end-to-end delay due to the attack. The proposed algorithm

also generates a graph demonstrating the network condition under normal and attack conditions and the defense approach that stabilizes the network and reduces the delay.

The results display the defense end-to-end delay is lowered on application of the proposed algorithm, than the attack scenario and the algorithm manages to reduce the delay close to normal conditions, thereby maintaining the stability of the network. In each demonstrated case, the normal and attack scenario show a greater deviation in a delay which has the possibility of disrupting the availability of the network for legitimate users. The defense, however, reduces the under-attack delay, ensuring that the underlying services are available in reduced load, enabling better usability during a malicious event.

1. Case 1: Malicious Node is attached to Cluster 3 - Node 1
2. Case 2: Malicious Node is attached to Cluster 2 - Node 1
3. Case 3: Malicious Node is attached to Cluster 1 - Node 3

- In Case 1: When the malicious node is attached to Cluster 3 Node 1 as shown in figure 3, the attack scenario is triggered and the traffic rate and flow are hindered for certain nodes therefore increasing the end-to-end delay. The defense algorithm works here to identify and regulate the traffic flow from the malicious node.
  - The average End-to-End under attack generated in this case is as follows:

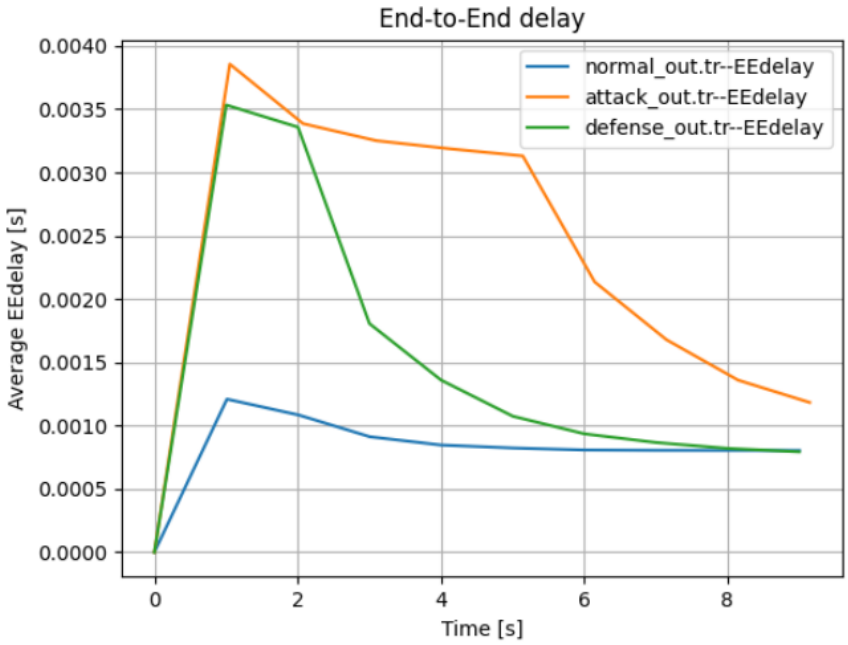

Figure 3: Average End-to-End Delay

- In Case 2: The malicious node is connected to Cluster 2 Node 1 as shown in figure 4, the attack is triggered by the malicious node and the defense algorithm sorts the active nodes and determines the node with higher traffic flow and reduces the rate of packer transfer therefore maintaining network stability.
  - The average End-to-End under attack generated in this case is as follows:

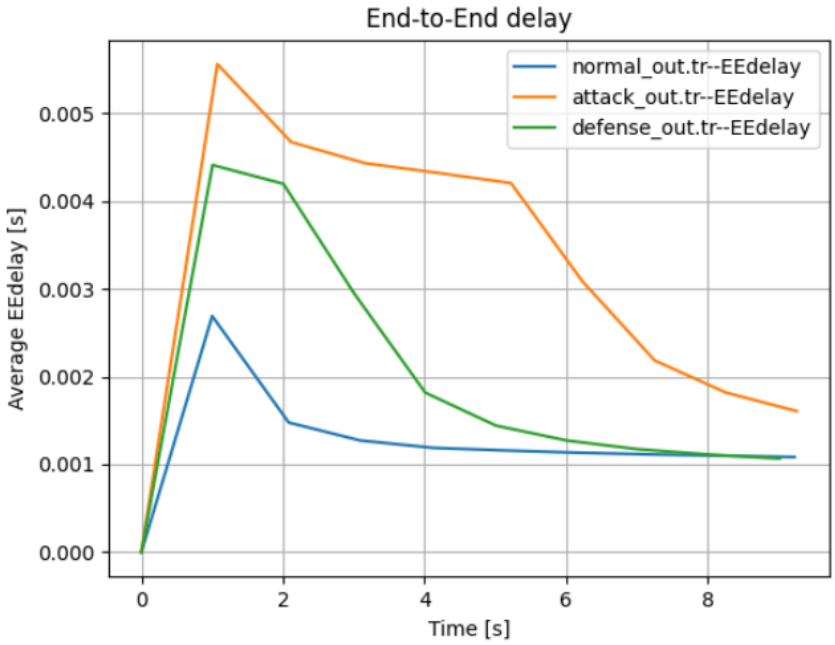

Figure 4: Average End-to-End Delay

- In Case 3: The malicious node is connected to Cluster 1 Node 3 as shown in figure 5 and the traffic properties of the malicious node are increased by 2 folds. The proposed defense algorithm was able to determine the node and reduce the traffic rate thereby stabilizing the network.
  - The average End-to-End under attack generated in this case is as follows:

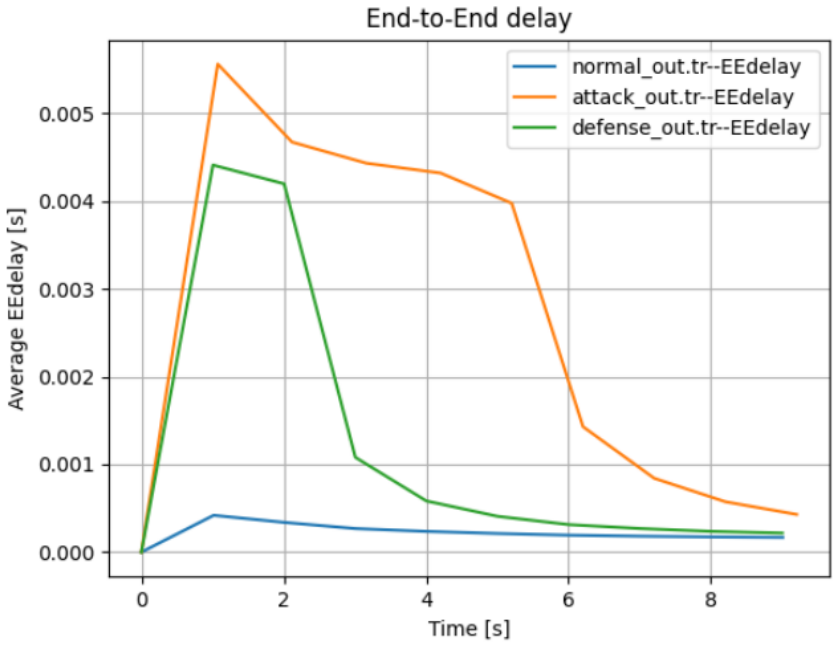

Figure 5: Average End-to-End Delay

7.2. Scenario - 2

In order to maintain the working concept of the proposed algorithm for a larger network, the number of nodes or endpoint devices attached per cluster was increased by 5, therefore each cluster is now determined to have 15 nodes, and the 5 added nodes in each cluster follow the same topological formal as their parent cluster. The nodes run different applications on them and have a busy traffic flow amongst them. Therefore a single malicious node introduced in the network would greatly disrupt the network activity thereby causing network failure or a significant increase in the End-to-End Delay of the network.

The results and observations on the new network are added below:

1. Case 1: Malicious Node is attached to Cluster 1 - Node 3
2. Case 2: Malicious Node is attached to Cluster 3 - Node 6

3. Case 3: Malicious Node is attached to Cluster 4 - Node 3

- In Case 1: The malicious node is connected to cluster 3 node 6 as shown in figure 6 which would cause a disruption in the traffic flow through Switch 3 and Router 1. The defense algorithm here, instead of reducing the traffic flow, reduced the rate of packet transfer thereby maintaining the network stability and reducing End-to-End Delay.
  - The average End-to-End Delay under attack generated in this case is as follows:

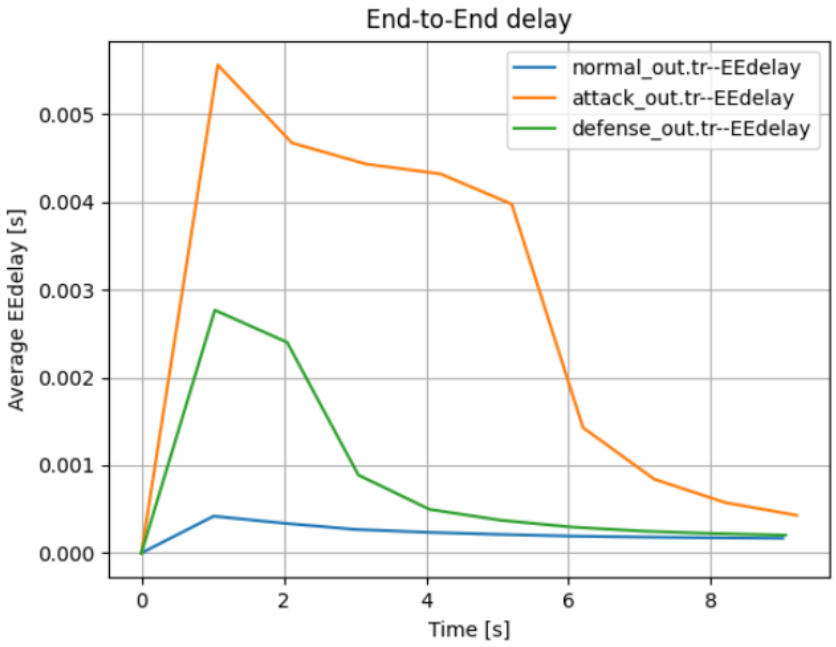

Figure 6: Average End-to-End Delay

- In Case 2: The malicious node is connected to Cluster 3 Node 6 as shown in figure 7 which increases the traffic flow through Switch 3 thus causing an increase in End-to-End Delay in the attack scenario which is managed and reduced by the proposed defense algorithm.

– The average End-to-End under attack generated in this case is as follows:

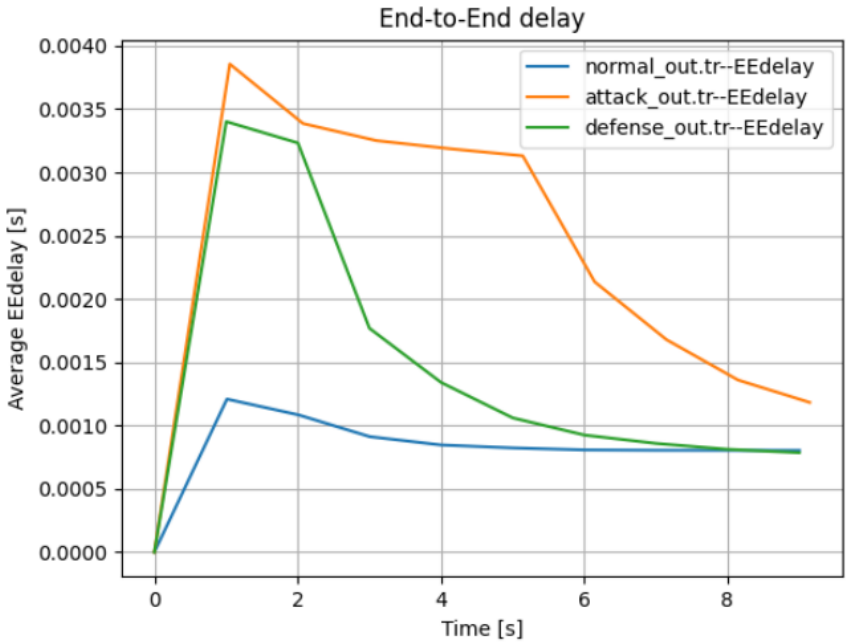

Figure 7: Average End-to-End Delay

- In Case 3: The malicious node is connected to Cluster 4 Node 3 as shown in figure 8 which disturbs traffic flow through Switch 4, therefore reducing network stability which is managed and the End-to-End is reduced as compared to the Attack Scenario.
  – The average End-to-End under attack generated in this case is as follows:

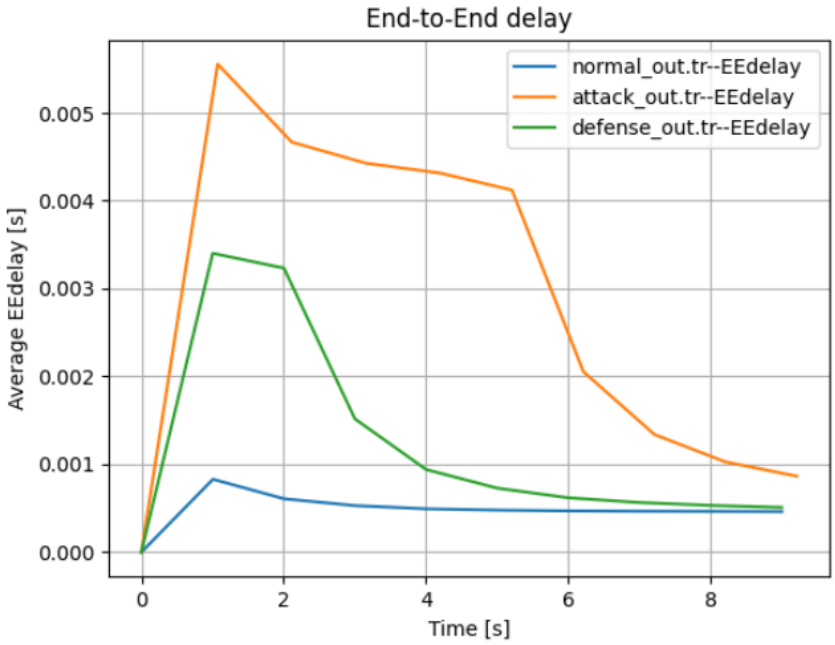

Figure 8: Average End-to-End Delay

It is therefore conclusive that using Adaptive Defense Approach to solve complex network issues like intrusions and malicious activity can be done with a higher efficiency as compared to native algorithms.

This statement is substantiated by testing 6 random test cases implemented on a simulated network retrieved from a network adaptive defense testbed [3].

The potential limitations of the proposed Adaptive defense approach include its complexity and require better understanding during the implementation process. It is dependent on the network connectivity for continuous monitoring of the endpoints connected to a network. There can be compatibility concerns based on the type of on-site infrastructure used by the businesses. These limitations are however taken into consideration while defining the proposed algorithm which defines a unified approach to monitoring using the

least amount of on-site resources and the complex approach is reduced by performing meta-heuristic search procedure of Nature Inspired Algorithms.

8. Contributions

This paper devises a defensive algorithm that monitors the state of the nodes present in the network recursively such that any malicious activity defined by a change in the network parameters such as Throughput, End-to-End Delay, and Packet Delivery Ratio could be flagged into the solution set prepared by the algorithm and the properties of the nodes can be altered to give a defined set of the packet transfer, therefore, preventing attacks involving hammering the network with loads of data such as Denial-of-Service attacks. The base paper [3] provides a testbed to determine the performance comparison of a network under normal and attack conditions.

This paper has enhanced the methodology of [3] by not just determining the throughput difference but also using other network parameters to determine the set of malicious nodes and modifying their packet delivery properties to prevent an attack at an earlier state before they are detected by native Intrusion Detection and Prevention System in the Modern Day firewalls.

The workflow and mechanism stated in the paper are to add a pre-detection phase to the normal modern-day firewalls. Single or multi-layer firewalls have the capability of determining traffic properties based on preset signatures that are used for validation purposes but with the implementation of an additional early-detection algorithm as defined in this paper, the traffic properties can be determined based on the advanced Machine Learning approach. Also, modern-day firewalls have the capability to detect malicious traffic into the network which does not guarantee the network to remain available during an attack whereas, the proposed algorithm keeps the network active even under an attack condition.

For instance, during a massive attack like Distributed Denial of Service, the network services may become unavailable to the public thereby causing a business loss and also a disruption in the Availability constraint in the Confidentiality-Integrity-Availability (CIA) Triad. To prevent this, the proposed algorithm has the capability to shift unwanted load between the other

network intermediaries and make an attacked node non-functional in order to keep the network functional at a reduced load but still it remains available to the public. This provides extra time for network security engineers to assess the network and detach the attacked node from the network, replacing it with a different node while patching the vulnerability that was used to gain access to the nodes in the network. This enables Business Continuity in times of attack and helps recover the network while allowing some extra time, without the network getting shut down due to load caused by the said attack.

The proposed algorithm can provide a granular approach to maintaining the security of the endpoints present in the network. This algorithm enables businesses to operate under sustained load even during an attack condition because of the early detection approach introduced in it. This enables improved protection against malware activities in a critical network and detects infected systems present in it by matching the network properties on each of them in a continuous manner.

9. Conclusions

This paper proposes an algorithmic approach that connects Nature Inspired Cyber Security with the Adaptive Defense Concept to detect and manage malicious nodes attached to a network of any topology thereby reducing the attack surface and pre-determining an attack scenario to future-proof the concept of safer computing. Nature Inspired Cyber Security algorithm such as Artificial Bees Colony Algorithm is implemented in this paper which includes the employed bees being linked with a defined food source, the onlooker bees following the employed bees to define an optimal food source location, and the scout bees to define food source solution set in random order.

The proposed method is able to detect and respond to attacks or threats imposed on a network before the traffic is checked by the firewall. This introduces the process of early detection that gives rise to adaptive defense such that when a malicious node is introduced in a large network, the proposed algorithm can create a set of probable malicious nodes instead of shutting them down which could cause disruption in the network and therefore a threat to business continuity, it reduces the packet transfer rate from source

to destination or defines a specified rate of traffic flow based on the Artificial Intelligence driven defense mechanism.

10. Future Work

This work is a combination of Intrusion Detection and Prevention Systems that work at an earlier stage as opposed to Native algorithms that work after the traffic reaches the clusters and routers where the firewall is implemented. This early detection mechanism can be enhanced by defining different parameters as opposed to the proposed two methods of traffic control and packet management such that the capacity of the network under load can be improved and the stability of the network can be increased. The proposed algorithm can be further improved by devising other Nature Inspired Cyber Security Algorithms as opposed to Artificial Bees Colony Algorithm which might provide better experimental results and therefore a more stable network.

The proposed algorithm can be further extended to other types of cyber attacks by managing and defining the network properties based on the difference in the case studies for attack and normal scenarios. For example, the major difference in the case of Distributed Denial of Service attack is found in the End-to-End Delay property of a network. Similar defining properties can be established for other cyber attacks and applied to the algorithm for handling such attacks.

References

[1] H. Balakrishnan, M. Stemm, S. Seshan, R. H. Katz, Analyzing stability in wide-area network performance (1997) 2–12doi:10.1145/258612.258631.
URL https://doi.org/10.1145/258612.258631

[2] C.-W. Ten, G. Manimaran, C.-C. Liu, Cybersecurity for critical infrastructures: Attack and defense modeling, IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 40 (4) (2010) 853–865. doi:10.1109/TSMCA.2010.2048028.

[3] S. K. Shandilya, S. Upadhyay, A. Kumar, A. Nagar, Ai-assisted computer network operations testbed for nature-inspired cyber security

based adaptive defense simulation and analysis, Future Generation Computer Systems 127 (09 2021). doi:10.1016/j.future.2021.09.018.

[4] H. Alrezaamiri, A. Ebrahimnejad, H. Motameni, Parallel multi-objective artificial bee colony algorithm for software requirement optimization, Requirements Engineering 25 (09 2020). doi:10.1007/s00766-020-00328-y.

[5] A. Ebrahimnejad, M. Tavana, H. Alrezaamiri, A novel artificial bee colony algorithm for shortest path problems with fuzzy arc weights, Measurement 78 (2016) 322–333. doi:10.1016/j.measurement.2016.06.050.

[6] D. Di Caprio, A. Ebrahimnejad, H. Alrezaamiri, F. J. Santos Arteaga, A novel ant colony algorithm for solving shortest path problems with fuzzy arc weights, AEJ - Alexandria Engineering Journal 61 (08 2021). doi:10.1016/j.aej.2021.08.058.

[7] A. Abbaszadeh Sori, A. Ebrahimnejad, H. Motameni, Elite artificial bees' colony algorithm to solve robot's fuzzy constrained routing problem, Computational Intelligence 36 (11 2019). doi:10.1111/coin.12258.

[8] J. Liu, Z.-G. Wu, D. Yue, J. Park, Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks, IEEE Transactions on Systems, Man, and Cybernetics: Systems PP (2019) 1–11. doi:10.1109/TSMC.2018.2888633.

[9] R. Fu, X. Huang, J. Sun, Z. Zhou, D. Chen, Y. Wu, Stability analysis of the cyber physical microgrid system under the intermittent dos attacks, Energies 10 (5) (2017). doi:10.3390/en10050680.
URL https://www.mdpi.com/1996-1073/10/5/680

[10] C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control 60 (11) (2015) 2930–2944. doi:10.1109/TAC.2015.2416924.

[11] R. E. Abbadi, H. Jamouli, Stabilization of cyber physical system with data packet dropout and replay attack via switching system approach (2019) 325–329doi:10.1109/SYSTOL.2019.8864787.

[12] N. Zhao, P. Shi, W. Xing, C. Lim, Event-triggered control for networked systems under denial of service attacks and applications, IEEE Transactions on Circuits and Systems I: Regular Papers PP (2021) 1–10. doi:10.1109/TCSI.2021.3116278.

[13] S. Hu, D. Yue, X. Xie, X. Chen, X. Yin, Resilient event-triggered controller synthesis of networked control systems under periodic dos jamming attacks, IEEE Transactions on Cybernetics 49 (12) (2019) 4271–4281. doi:10.1109/TCYB.2018.2861834.

[14] J. Bansal, H. Sharma, S. Jadon, Artificial bee colony algorithm: A survey, International Journal of Advanced Intelligence Paradigms 5 (2013) 123–159. doi:10.1504/IJAIP.2013.054681.

[15] S. Kumar, V. K. Sharma, R. Kumari, Memetic search in artificial bee colony algorithm with fitness based position update (2014) 1–6doi:10.1109/ICRAIE.2014.6909301.

[16] D. Karaboga, An idea based on honey bee swarm for numerical optimization, technical report tr06, Technical Report, Erciyes University (01 2005).

[17] D. Karaboga, B. Akay, Artificial bee colony algorithm on training artificial neural networks (2007) 1–4doi:10.1109/SIU.2007.4298679.

[18] D. Karaboga, B. Akay, C. Ozturk, Artificial bee colony (abc) optimization algorithm for training feed forward neural networks (2007) 318–329doi:10.1007/978-3-540-73729-2-30.
URL https://doi.org/10.1007/978-3-540-73729-2-30

[19] A. Bolaji, A. T. Khader, M. Al-Betar, M. Awadallah, Artificial bee colony algorithm, its variants and applications: A survey, Journal of Theoretical and Applied Information Technology 47 (2013) 434–459.

[20] F. Gibb, S. Buchanan, A framework for business continuity management, International Journal of Information Management 26 (2) (2006) 128–141. doi:https://doi.org/10.1016/j.ijinfomgt.2005.11.008.
URL https://www.sciencedirect.com/science/article/pii/S0268401205001179

[21] S. V. Aleksandrova, M. N. Aleksandrov, V. A. Vasiliev, Business continuity management system (2018) 14–17doi:10.1109/ITMQIS.2018.8525111.

[22] R. Sahay, W. Meng, C. D. Jensen, The application of software defined networking on securing computer networks: A survey, Journal of Network and Computer Applications 131 (2019) 89–108. doi:https://doi.org/10.1016/j.jnca.2019.01.019.
URL https://www.sciencedirect.com/science/article/pii/S108480451930027X

NICS_ABC_Defense_J2 (9).pdf

ORIGINALITY REPORT

12%
SIMILARITY INDEX

PRIMARY SOURCES

1	www2.mdpi.com Internet	289 words — 5%
2	www.mdpi.com Internet	67 words — 1%
3	www.hindawi.com Internet	45 words — 1%
4	www.researchgate.net Internet	37 words — 1%
5	domainwhoisdb.appspot.com Internet	33 words — 1%
6	www.scilit.net Internet	28 words — < 1%
7	sedici.unlp.edu.ar Internet	19 words — < 1%
8	www.passeidireto.com Internet	18 words — < 1%
9	dokumen.pub Internet	15 words — < 1%
10	gitlab.math.univ-paris-diderot.fr Internet	

		14 words — < 1%
11	jglobal.jst.go.jp Internet	14 words — < 1%
12	jce.shahed.ac.ir Internet	13 words — < 1%
13	doaj.org Internet	11 words — < 1%
14	Engineering Computations, Volume 31, Issue 2 (2014-03-28) Publications	10 words — < 1%
15	docs.di.fc.ul.pt Internet	10 words — < 1%
16	pjm.ppu.edu Internet	10 words — < 1%
17	research.rug.nl Internet	10 words — < 1%
18	downloads.hindawi.com Internet	9 words — < 1%
19	dspace.library.uvic.ca Internet	9 words — < 1%
20	mafiadoc.com Internet	9 words — < 1%
21	old.nnc.kz Internet	9 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	< 3 WORDS
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	< 9 WORDS