Fusion Processing Techniques and Bio-inspired Algorithm for E-Communication and Knowledge Transfer

Omar Saad Ahmed[1], Fay Fadhil[2], Laith H. Jasim Alzubaidi[3], Riyadh Al-Obaidi[4]

[1] Al-Turath University College, Baghdad, 10021, Iraq
[2] Department of Computer Techniques Engineering, Al-Rafidain University College, Baghdad 10064, Iraq
[3] Department of Medical device technology Engineering, Alfarahidi University, Baghdad, Iraq
[4]Department of Business Administration, Al- Mustaqbal University College, Babylon 51001, Iraq
Emails: omar.saad@turath.edu.iq; rana.abbas@ruc.edu.iq; fay.fadhil@alfarahidiuc.edu.iq; raidh.h.salman@uomus.edu.iq

Abstract

This study suggests employing a dynamic natural and bio-inspired algorithm (DNBIA) to strengthen the confidentiality, integrity, and availability of digital information exchanges. You may think of the suggested method as a clever approach to Fusion Processing. Fusion Processing is the practice of combining and analyzing information from many databases. The efficiency and reaction time of e-communication systems may be increased by the use of the suggested DNBIA algorithm, which processes and integrates data from different sources. It is also possible to see the multi-objective optimization study presented in this work as a type of Fusion Processing. Cyberattacks and other types of computer security risks are the focus of this study, which seeks to optimize numerous objectives concurrently in order to eliminate them. The study can give a complete solution to improve the security of e-communication systems by combining different goals. The suggested method of enhancing e-communication and information transmission using DNBIA and multi-objective optimization analysis can be seen as a type of Fusion Processing. Efficient e-communication systems may be achieved by collecting data from a variety of sources and analyzing the results.

Keywords: E-Communication; Knowledge Transfer; Natural; Fusion Processing; Bio-Inspired Algorithms.

1. Introduction

E-communications security faces a number of issues and worries due to the dynamic and ever-changing nature of electronic communication technology. Integrating and processing data from numerous sources to draw relevant insights and enhance security measures, Fusion Processing can play an important role in resolving these security challenges [1,2]. For instance, Fusion Processing's ability to unify disparate data and communication networks can provide rapid access to extensive resources and boost security. The interconnected and networked nature of e-communications systems also makes Fusion Processing a useful tool for spotting and countering the resulting weaknesses and threats [3-5]. Therefore, the use of Fusion Processing methods can aid in the development of a security culture that raises both the profile and the level of knowledge of security issues within the context of electronic communication networks. Fusion Processing allows electronic communication systems to adapt to the demands of rapid technological advancements and shifting security concerns [6, 7].
Knowledge transfer (KT) is utilized to comprehend a pervasive range of actions to support mutually valuable collaborations among businesses, the public, and universities [8,9]. Knowledge transfer, known as knowledge sharing, can be reflected in a process in which an organizational unit, like a department, group, individual, or division, can use the knowledge acquired from another unit and apply this knowledge to another situation [10]. The personalization strategy refers to transferring knowledge through personal communication [11,12]. There are numerous points to consider when utilizing e-communication in organizational contexts. These involve transmission and response to messages, generation speed, the cost of distribution messages, and accessibility; there is an issue with sending too much correspondence, privacy and security by unauthorized people, and sender authenticity [13].

Doi: https://doi.org/10.54216/FPA.100109
Received: June 18, 2022 Accepted: November 12, 2022

A wireless sensor network contains interconnected nodes linked, utilizing the air medium to achieve distributed sensing tasks [14]. Wireless sensor networks are measured as the most suitable selection in different disciplines for sensing, monitoring, and cooperative decision-making. Incorporating signal processing, detection systems [15], and data communication functions alter the wireless sensor network into a powerful platform to progress the environment's data[25]. Nature and bio-inspired protocols and algorithms for these networks must allow network operations during the usual process, initialization, and emergency circumstances [16].

Natural or Bio-inspired computing algorithms are an emerging method based on nature's biological development ideologies and inspiration to progress new and robust competing techniques. Current cybersecurity device limitations include a lack of self-awareness and self-correction methods, impairment of configuration flaws, and settling disputes due to multiparty security infrastructure management[24][26]. The biological method, nature-inspired, has the desirable built-in quality to adjust to different environmental conditions and intrinsic flexibility for failures and damages in electronic communication and networking [17,18]. The system utilizes a hybrid approach that incorporates natural optimization strategies with modeling for simulation to build and analyze candidate architecture and adapt to changing threats. A Bio-Inspired based attack detection [19] addresses an emergent attack pattern termed the transmissive attacks in which an assailant influences diverse electronic communication paths to method the target and achieves malicious behaviors. This outlines normally utilized prevalent models for an electronic communication system and then relates transmissive attacks to these wide-ranging models.

Fayez et al. [20] introduced trust-based monitoring (TBM) to improve cloud-assisted IoT environments' security features. This security framework uses middleware and smart agents to handle user and communication security. Three security steps of TBM are conducted: spoof identification, trust, and message authentication. The smart agents are responsible for guaranteeing safe contact with the middleware by sharing the faith and signal powers. The agents help to track, process, and adjust activities to minimize coordination costs. Through detailed simulations, TBM was tested. The findings show its coherence in minimizing reaction and detection cycles, improper detection probabilities, and false-positive rates. Furthermore, reduced energy consumption has been found to boost network life.

Shaila Sharmeen et al. [21] suggested a Novel Adaptive Framework (NAF) that includes deep learning and semi-supervised approaches (DL-SSA) to predict android privilege escalation threats. The suggested detection models would derive know-how from unscored apps to recognize the latest malicious activity through unregulated training and incorporating deep learning and clustering methods with the supervised detection engine. Therefore, their adaptive architecture knows about malicious applications and their actions without manual professional supervision and can guarantee zero-day security. The detection models were tested on an actual mobile malware testbed and dataset. Experimental findings indicate that the DL and SSA achieve 99 % precision, are better for zero-day security, and surpass other already controlled sensing engines.

Abhishek Verma and Virender Ranga [22] proposed machine learning classification algorithms (MLCA) for Intrusion Detection Systems for the Internet of Things Applications. In this study, abnormality-based Intrusion Detection Systems suitable for securing the Internet of Things against DoS attacks are carried out. The performance evaluation of seven ML classification algorithms involving AdaBoost, random forests, extremely randomized trees, gradient boosted machine, regression trees, classification, and multi-layer perceptron, is completed. The optimal constraints of classifiers are determined by utilizing random search algorithms. Every classifier's performance is calculated in terms of specificity, false-positive rate, accuracy, sensitivity, and AUROC curve. From the performance outcomes and statistical test, it is established that classification and regression trees and extreme gradient boosting classifiers show the best trade-off among response time and prominent metrics; therefore, both are the appropriate choice for constructing Internet of Things-specific abnormality-based Intrusion Detection Systems.

Ismaeel et al. [23] initialized the Mobile Edge Computing (MEC) solution that allows node collaboration between IoT devices to deliver secure and reliable communication among the fog layer and devices and the cloud and the fog layer. Using node-by-node communication Protocols proposed solution eliminates the unwanted traffic flows to and from the edge. The cloud and Fog layers are utilized to provide external data and extensive computing applications to ensure stable cloud communications protocols. Preliminary simulations would show whether the proposed architecture is effectively adapted to attain smart city environmental sustainability via efficiency and service reliability. The findings showed that, in terms of effective service distribution and composition time, hit ratios, and offender node detection, the proposed approach would significantly exceed other non-cooperative and semi-cooperative service composition methods.

There are several challenges to existing methods for E-communication and knowledge transfer. In this paper, the DNBIA model has been suggested to overcome these issues. The paper concentrates on the process of organizational knowledge transfer and the probable of Electronic Communication models. The evolution of nature and bio-inspired algorithms and their applications in e-communication and knowledge transfer are presented. Different security mechanism has been employed based on biological behavior in a wireless sensor network for electronic communication and knowledge transfer. The remainder of the article is structured as

Doi: https://doi.org/10.54216/FPA.100109

Received: June 18, 2022 Accepted: November 12, 2022

follows: Section 1 discusses the overview of e-communication and knowledge transfer. Section 2 deliberates the suggested DNBIA model. Section 3 discusses the numerical analysis, and section 4 concludes the research article.

2. Dynamic Natural and Bio-inspired algorithm (DNBIA)

This paper introduced the DNBIA model for effective electronic communication systems and knowledge transfer in different sectors. The Wireless Sensor Network (WSN) based communication solves major security concerns with wireless networking between nodes and open node distribution. The attacker disrupts protection criteria by beginning attacks on multiple WSN layers. A trust-based intrusion scheme for the protocol layer to protect the WSN by detecting the attackers in different layers is suggested in this paper. With the growing trust of nodes in the network, a wireless sensor network's security is considerably improved. A variety of confidence models are proposed using different approaches for determining trust. This paper categorizes trust assessment approaches into natural-inspired, bio-inspired, and computational methods for wireless sensor networks. Compared to the empirical techniques, biologically driven processes and social frameworks are frequently used to design trust mechanisms. This paper examines current bio-inspired trust structures and socially inspired trust schemes based on their contributions, the trust assessment methodology, and the drawback of the trusts, for wireless sensor networks and trust models (such as analysis, biology, and socio-inspired). The advantages and disadvantages of analysis, sociological and biologically influenced computational algorithms, are listed to quickly determine the utility of biological or socio-inspired methods for resolving trust problems on wireless sensor networks.

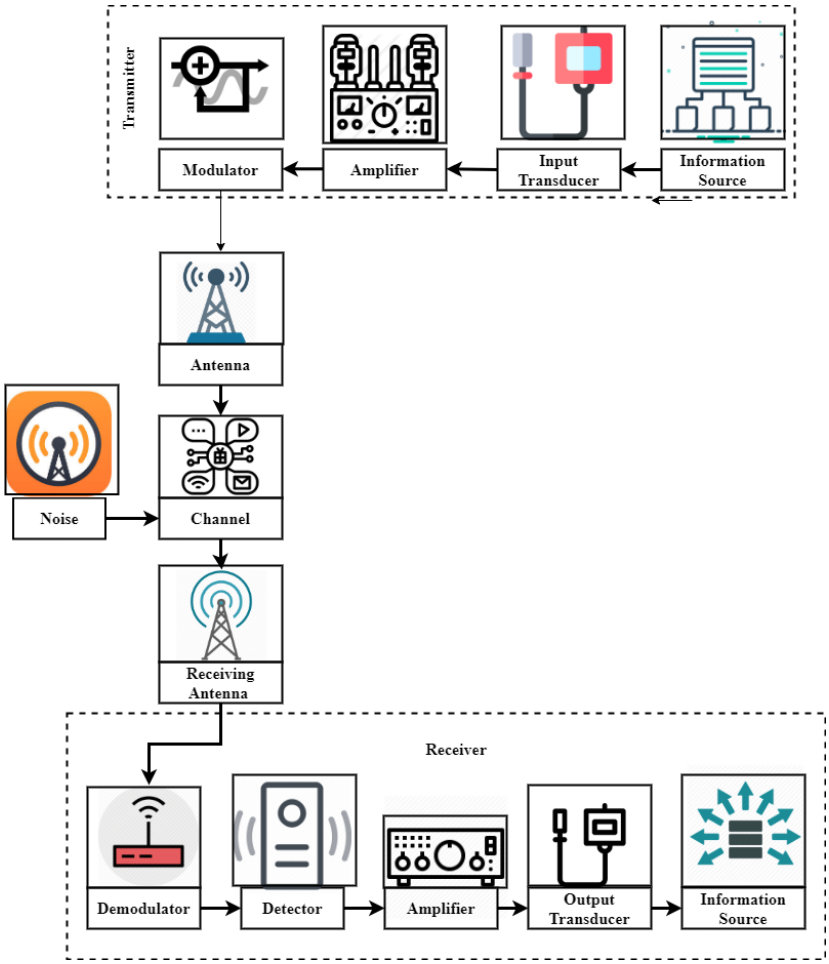

Figure 1: Electronic Communication System

Figure 1 shows the Electronic Communication System. The method of communication is a system representing the sharing of information in two areas. Communication is called the method of sending and receiving information. The core communication components are the information sender, the communication source or medium, and the receiver. The individual to be conveyed is the message or the information. The format can be audio, film, temperature, image, strain, etc. The time that holds the information is the significant outcome. This information is translated into a transmitting electrical form. A computer or a system that converts one sort of energy into another. An electric transition into the resulting electrical signal alters physical variables, including pressure, energy, and temperature.

Doi: https://doi.org/10.54216/FPA.100109

Received: June 18, 2022 Accepted: November 12, 2022

For example, a Microphone transforms audio into power signals. The sensor converts light signals into electrical signals. An amplifier, which increases signal amplitude or strength, is called an electronic circuit or device. The signal amplitude is less than the correct magnitude, and amplification may occur between the transmitter and the receiver. The amplification is provided with a DC power supply. Low frequency and amplitude mean that the original pulse cannot be transmitted over a wide distance. A vibration substitutes for the wave of the receivers. Modulation by the carrier wave is this overlaying phenomenon of the message signal. The wave results in a modulated relay wave. This approach is called amplitude modulation by impressing or overlaying the signal wave's amplitude on a high-frequency carrier wave. Frequency modulation is a method where a transmitter pulse modulates the frequency of a signal. It is better than amplitude modulation because it eliminates noise from multiple sources. The wave phase of the carrier transfers the wave phase of the signal. The transition in phase after modulation often depends on the carrier wave frequency. The modulated phase waves are more likely to be resistant to noise. That is the structure in which the communicating signal will be sent and received in an appropriate form. An antenna is an electromagnetic wave structure or unit that radiates. A metallic object, mostly a set of wires, is essentially an antenna. The antenna position polarises the electromagnetic waves.

A channel is a medium from a transmitter to the receiver, such as wire, cables, and space. Any channel deficiencies are markedly adverse to the channel output: noise, mitigation, and overall listing of major deficiencies. The signal noise obtained at the target is an imperfection or fault in the channel. External and internal sources produce noise. External causes include local television interferences (cross-speaking), interaction with natural sources such as lightning, solar and cosmic rays, inducing vehicle radiation, etc. The external noise can be reduced and avoided with proper channel configuration and cable shielding. External noise can be significantly minimized by wireless transmission. Noise from spontaneous movement and electron colliding in conductors, thermal noise attributable to diffusion, and the charging carriers' recombination into other electrical equipment include internal sources. Cooling and using digital transmission technologies will reduce internal noise. Attenuation is a medium-related concern. The original energy reduces as the signal is distributed over a greater distance across a medium based on length. The initial power losses are directly proportional to the medium range.

The signal power is increased or amplified to minimize attenuation using amplifiers. In contrast to analog signals, optical signals are relatively lower resistant to mitigation. It is another kind of issue with the channel. The distorted signal can vary with the distorted signal, both in frequency and bandwidth. The difference in signal frequency can be linear or nonlinear. A system that extracts and plays a correct copy of the message or information on the channel's output end from the message or signal, as the initial message signal is a recipient. It's the reverse modulation thing. The transmitter is isolated from the transmitter wave by the demodulator. The wave is moduled to restore knowledge. Repeaters are placed in separate locations between the transmitter and the receiver. A repeater catches, amplifies, and transfers the signal to the next replayer without distorting the signal.

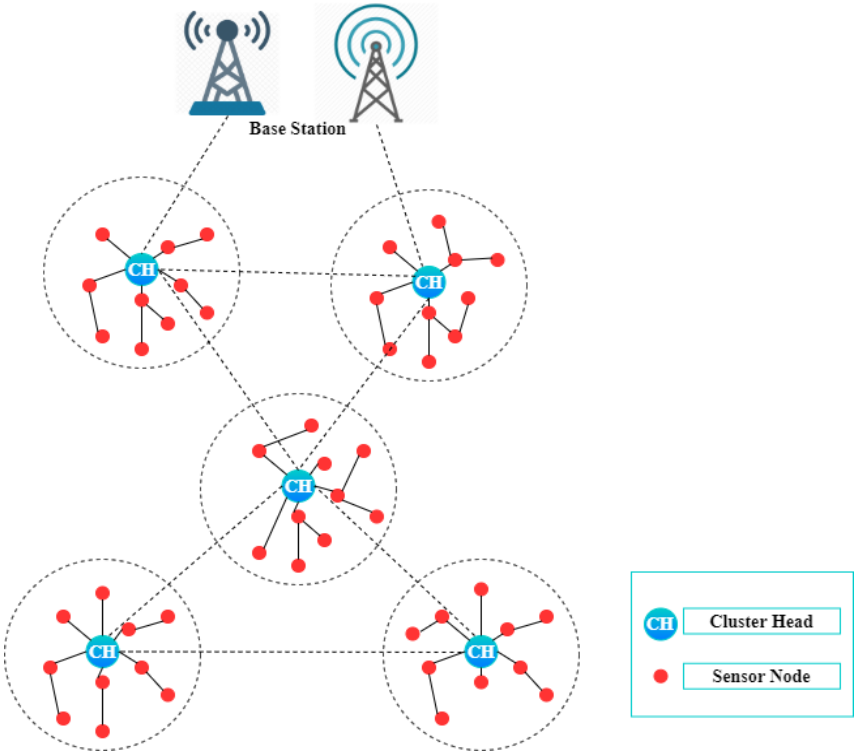

Figure 2: Wireless Communication with Cluster Head and Sensor Node

Doi: https://doi.org/10.54216/FPA.100109

Received: June 18, 2022 Accepted: November 12, 2022

Figure 2 shows the Wireless Communication with Cluster Head and Sensor Node. The model of the system describes the topology, coordination, and attack models used. A WSN architecture that is clustered consists of a network model. The cluster head (CH) and sensor node (SNs) are part of a network cluster. Using wireless networking, the SNs connect. SNs can communicate directly via wireless or indirectly with the base station (BS) via other SNs. With wireless networking, CHs can contact each other. The CH is finely processed and computer-friendly. The battery capacity of the CH is presumed to be high. This algorithm uses a DNBIA model to test an SN for its neighbor.

In this case, every node uses the monitoring mechanism, where a node constantly views the next nodes by updating its trust value. The clustered wireless sensor network structure is shown in Figure 1. The trust for each layer is determined, and the cumulative trust of an SN is eventually integrated. The measures of faith are seen as the motion of the nodes in every layer. These criteria are used on each sheet to determine trust. An SN monitors this node again in the model to calculate the physical layer's trust value for each layer, network layer, and MAC layer. The substance of attacks occurs on the network layer, so they are primarily used to route network data. Firstly, for each layer, trust calculations are chosen. The physical layer's trust measurements are the sensor node's energy consumption and the number of SN texts. Time off and other transmitting quality are measures of trust in the MAC layer. The number of hops marketed on the network layer is the trust indicator. To measure individual confidence levels on each layer and have justified in the following sections those parameters. The total trust of the SN is determined by adding each layer's trust. The SN's cumulative confidence value is conveyed to the CH.

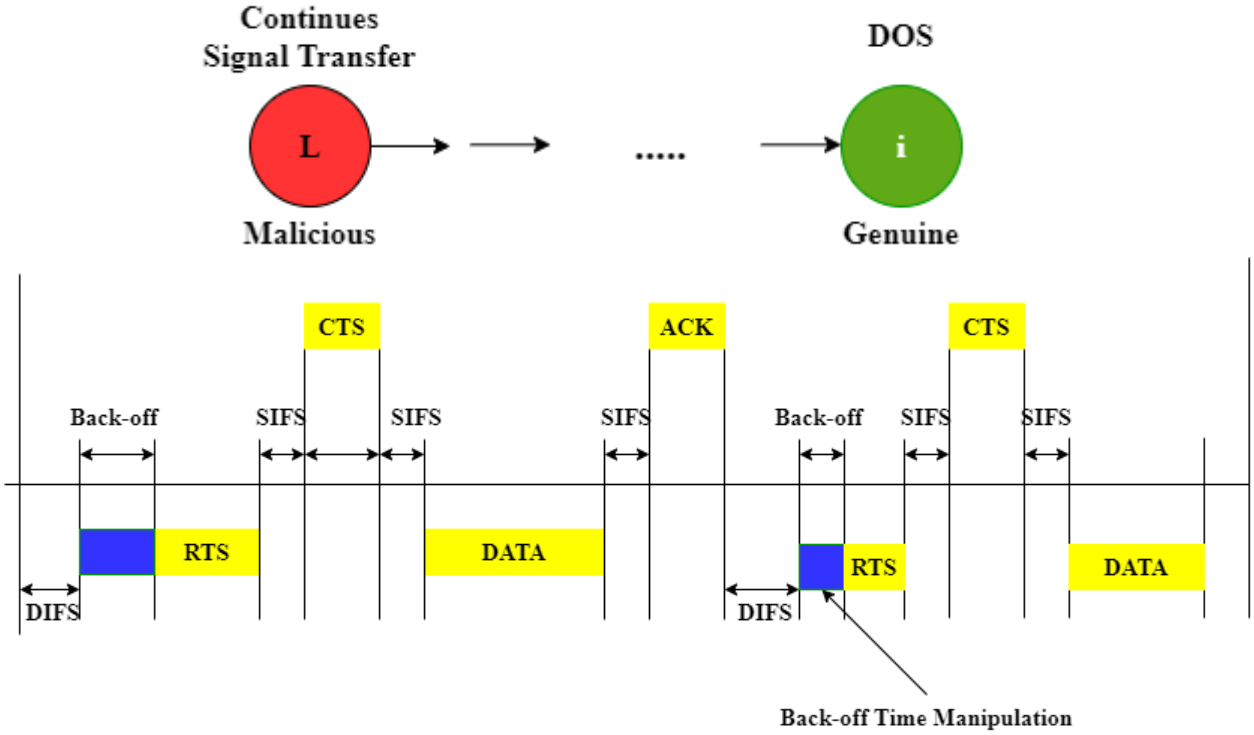

Figure 3: Attack Manipulation in the physical layer and MAC layer.

Figure 3 shows the Attack Manipulation in the physical layer and MAC layer. In this method, RTS represents the request to send, DIFS Distributed coordination function Interframe Spacing, Short Inter-frame Spacing is denoted the (SIFS), CTS is referred to as (request to send/ clear to send), and ACK represents the acknowledgment. The proposed DNBIA Attack model addressed the attacks used to evaluate efficiency. Jamming is a common safety hazard at the physical level, where malicious nodes repeatedly transmit for a short period. Attacks on the physical, MAC, and network layers are defined with each layer. This propagation of the signal generates network traffic. Owing to this traffic, unwanted signals continue to receive a real node, and other applications reject them. This is classified as an access denial of service (DoS). Mathematically as follows, the model of attack can be represented in equation (1):

$$i = e + m \qquad (1)$$

As shown in equation (1), denial of service (DoS) has been represented. Where i is the right or incorrect information, e shows the intended information, depending on the IDS, and m refers to the malicious content information. In this layer, energy consumption is known to predict malicious network nodes and the number of received messages (Nmr). The congestion attack is when the malicious L node begins to transmit a signal to the new j node, as seen in figure 3. This model assumes fewer messages generated (nm) on a mobile terminal in a

Doi: https://doi.org/10.54216/FPA.100109
Received: June 18, 2022 Accepted: November 12, 2022

given time interval than the malicious node (nm). A channel priority is an important consideration in the MAC layer. Thus the back-off modification attack where the malicious node targets the device by manipulating the back-off time has been considered. Random time of existence is back-off here. It reduces entry priority on the channel by reducing the backup time. This improves the efficiency of transmissions (Nst). The layer of malicious nodes and multiple active message (Nst) parameters are considered to detect back-off (Bt) time. The reverse attack of intimidation where the L node sends the signal constantly to the real j nodes, granting the channel priority in less time. The assailants often impact routing information at the network layer by publicizing wrong network information, such as the minimum number of hops. The sinkhole attack is taken into account in this work. The malicious node routinely sends information such as low-hop numbers through bogus advertising routing.

This is when second-hand records and first-hand information are used together as indices of output and reputation. There is uncertainty regarding the reliability of second-hand information surrounding first-hand information. As a result, much further processing is needed before the credibility metric computing feature can be allocated. The reputation of nodes with fake feedback data for other nodes is tested in proven ways. The credibility of these secondary messages can be tracked using variability tests and using statistical formulas such as Beta distribution in equation (2):

$$\left|F\left(beta\ (\beta,\alpha)\right) - F(beta(\beta_e,\alpha_e))\right| \geq C \tag{2}$$

As deliberated in equation (2), the Beta distribution has been checked. In Equation 2,C is a heuristic value, $\beta\ and\ \alpha$ are beta distribution parameters. In settings where some risk factor occurs, $\beta\ and\ \alpha$ are utilized to describe positive and negative behavior. The calculation of the actual confidence information on one Node B on another Node A is $F\left(beta\ (\beta,\alpha)\right)$, reflecting the predicted value. On the other hand, $F(beta(\beta_e,\alpha_e))$ reflects new confidence data generated with node D to node A of node B. Node C is deemed trustworthy, provided that the left-hand expression of 1 yields a value below threshold C. The Gamma function is used for the possible distribution function of the beta distribution:

$$Q(y) = beta\ (\beta,\alpha) = \frac{\Gamma(\beta+\alpha)}{\Gamma(\beta)\Gamma(\alpha)} y^{\beta-1}(1-y)^{\alpha-1}, \forall 0 \leq y \leq 1, \beta \geq 0, \alpha \geq 0 \tag{3}$$

As inferred in equation (3), the gamma function has been calculated. Equation 3 is another way to test data accuracy from the node. If $Q(y)$, the probability that the message is coherent in the next observation, calculates to 1, then ported information is expected to be consistent. The knowledge is deemed authentic for any value of $Q(y)$ other than 1. The Poisson, Binomial, and Gaussian distributions are used as statistical distributions.

The protocol with the ant-colony optimization (ACO) methodology incorporates certificate and quality of service (QoS) dependent security implementations in WSN. The malicious node routinely sends information such as low-hop numbers through bogus advertising routing. In ACO, there are stochastic houses, which create solutions when walking on a building graph. ACO is the best choice for combinatorial problems due to its constructive search behavior. ACO uses the heuristic pheromone and domain sensitivity search understanding to speed up the search process. For ACO-based routing algorithms, connectivity (unicasting and broadcasting) efficiencies and data aggregation have been improved, and the lives of homogeneous and heterogeneous WSNs have been maximized. In WSN, the reliability and credibility of the respective sensor node are closely correlated with a contact. Protocol security is provided by identifying malicious nodes that drop out messages received from them and reject them. The credibility of a node is modeled on a communication pathway dependent on the pheromone material. In this respect, the route with more deposits of pheromones Γ_{ji} is believed to be better than one with small deposits of pheromones in equation (4):

$$\emptyset(s) = \frac{\sum_{L=1}^{m_j} SL_i}{m_j} \tag{4}$$

As explored in equation (4), misbehavior has been calculated. Whereby Γ_{Li} is the pheromone trace from L to i nodes and m_j is the number of nodes in j's vicinity. A safety breach or wrongdoing occurs when $\emptyset_{ji} < \Gamma_{min}$ indicates the node j cannot forward the packets or does not trust.

The QoS formula is used to measure the percentage of uncovered traffic as in equation (5):

$$\theta_{ji}(s) = \frac{\sum N_h(s) + \sum N_p(s) - \sum N_c(s)}{\sum N_h(s) + \sum N_p(s)} \tag{5}$$

As shown in equation (5), the percentage of uncovered traffic has been measured. The number of received and dropped packets generated is presented as $\sum N_h(s) + \sum N_p(s)$and $\sum N_c(s)$, respectively. The QoS parameter indicates the form and existence of the service. This indicates the depth of operation offered by a node in the future. The following words indicate the QSec, a weighted creditworthiness sum, and QoS in equation (6):

$$z_m(s) = z_1 \emptyset_{ji}(s) + z_2 \emptyset_{ji}(s) \tag{6}$$

As discussed in equation (6), the weighted sum of credibility has been evaluated. Where z_1 and z_2 are the respective credibility and QoS and $z_1 + z_2 = 1$ weight parameters. QSec is the key factor to determine which node is the following step on the path.

Doi: https://doi.org/10.54216/FPA.100109

Received: June 18, 2022 Accepted: November 12, 2022

Trustee node, to create the trustee node's trustworthiness. In addition to the average pheromone measurements, the consistency of a solution depends on the solution's length and the number of aunts which have the same solution. The efficiency of the route is measured within equation (7):

$$P(T_L) = \frac{\overline{S_L}}{length\ (S_L)^{PLF}} \%B_L \quad (7)$$

As shown in equation (7), the efficiency of the route has been measured. If the path leads to the chosen sensor, $PLF \in [0,1]$ represents the path factor and percentage S_L represents the averaged pheromone T_L of path detected by ant L, $P(T_L)$ corresponds to the path T_L, B_L represents the percentage of ants selected with the same solution as the ant L. Where T_L represents the path leading back to the selected sensor. Determined by the equation is the confidence value

$$S(V) = \sum_{j=1}^{J(V)} \frac{T(V,J)}{J(V)} \quad (8)$$

As explored in equation (8), the trusted value has been calculated. If $J(V)$ is the overall amount of transactions, the peer V has been engaged with all the other peers, and $T(V,J)$ reflects the satisfaction of the peer V in its ith relationship.

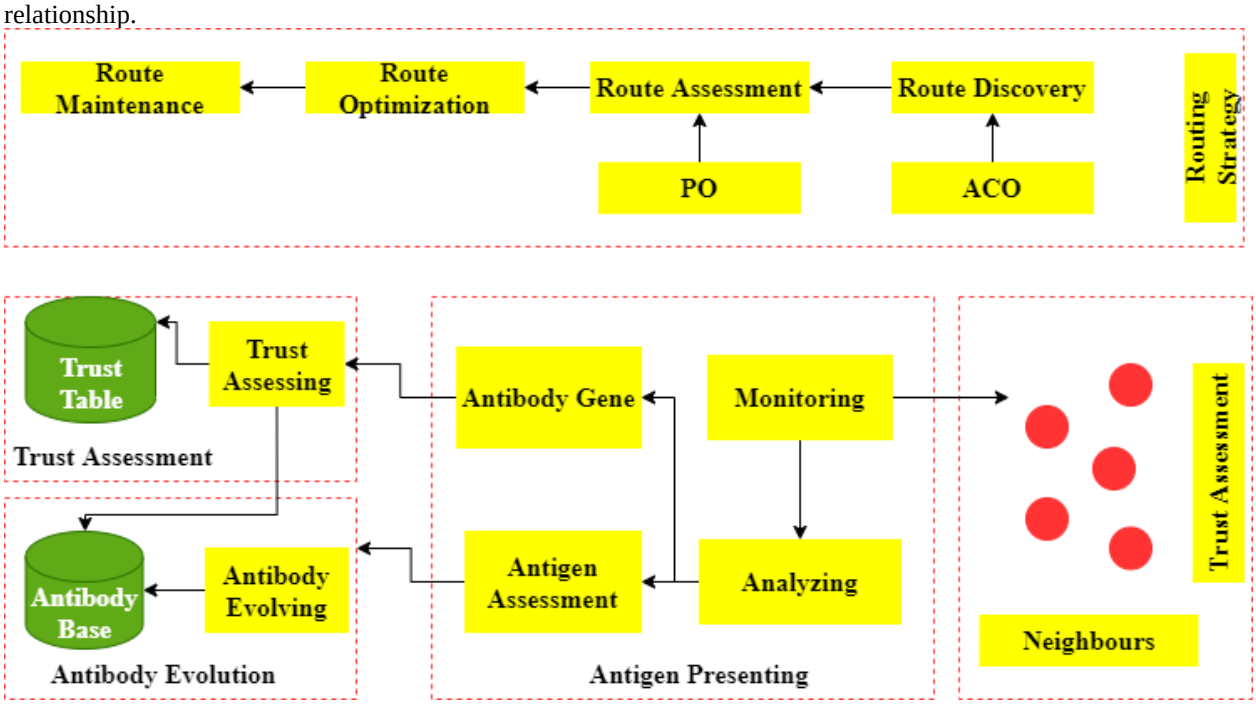

Figure 4: proposed DNBIA

Figure 4 shows the proposed DNBIA. DNBIA is designed specifically for mobile sensor networks focused on Ant Colony Optimization (ACO), Physarum Optimization (PO), and Artificial Immune Systems (AIS). It is specially designed for mobile wireless sensor networks (MWSNs). Figure 4 shows that the DNBIA model's design reveals two major aspects: trust evaluation and routing policy. ACO and PO are used to search and evaluate neighboring nodes using AIS. The evaluation for the trust of neighboring nodes is carried out.

An antigen is an immunologically active material that can induce the response of organisms to immune problems. Given MWSN, antigenes are node activities; an antigen gene is a node's behavior (for example, distributing, transmitting, and generating packets). The antigen collection is $Ba = \{y | y\ is\ node'sbehaviour\ in\ MWSN\}$ in which antigen is a permissible, unlawful, or unknown activity in equation (9):

$$Ba = \{< gene, weight, age, count > | gene \in B_h H(age, weight, count)\}$$

$$E(y,x) = \begin{cases} y, weight, if\ y, gene = \emptyset(x) \\ o, \qquad otherwise \end{cases} \quad (9)$$

As elaborated in equation (9), antigen has been found. The gene of antigen is the age of the antigen, the number of times the antigens match, and weight is the weight of the antigen. The id is the neighbor's address, and the gene is the antigen. The confidence assessment protocol using$L$ node provides an example: first, it tests each entity in an antibody set L node ab when it receives < id, gene >, the algorithm will add the weight to the value of element j in equation (10):

$$V_i = \frac{1}{n} \sum_{j=1}^{n} y_i^j \quad (10)$$

As described in equation (10), trust value transmission has been derived. This mechanism lasts some time before the gateway produces confidence values in the third block for the nodes. The rating of confidence is an important element in disabling fraudulent nodes on the network regardless of the nodes' fraudulent rating that

Doi: https://doi.org/10.54216/FPA.100109
Received: June 18, 2022 Accepted: November 12, 2022

drops below a certain level. To perform the disabled, the fraudulent node's radio is disabled using a gateway; contact on the network is isolated. Nature and bio-inspired algorithms reduce communication delay and latency. The socio-psychological study describes a trust which is asymmetric, transitive, relational, and contextually adaptive. The markers for socio-psychology are benevolence (B), ability (A), and integrity (J). Equation ten clarifies that the three measures A, B, and I are the foundation of confidence in equation (11):

$$trust = E(B, A, J) \quad (11)$$

As found in equation (11), trust indicators have been measured. Equation 11 tests the measurement of trust (T) as the product of the ability, benevolence, and integrity of benevolence and integrity. In equations 12, 13, and 14, respectively, equations for capacity and benevolence are further explained in equation (12):

$$S_m = B_m(\beta A_m + \alpha J_m) wher, \beta + \alpha = 1$$
$$B_m = \begin{cases} 1, if\ functional \\ 0, \quad otherwise \end{cases}$$
$$A_m = f^{-(\|s_m - s_{m'}\|)}$$
$$J_m = \frac{q_m}{q_m + m_m} \quad (12)$$

As shown in equation (12), capacity and benevolence have been explained. If S_m is the current node Ysensor reading, t_{n_0} is the mean readings of all adjacent Ynodes, p_n is the positive response number, and m_m is the negative outcome number. The immune module is instantiated below the appropriate threshold as soon as the social-psychological module's morale level is measured. The module canceled the problem node's impact by deleting the node from the grid and reducing the sampling time interval. The model insists on the right dimensions for the base station.

The data structure, known as the PS_j reputation table has other nodes on a given sensor node j reputations. The credibility table is seen in equation (13):

$$PS_j = \{P_{ji}\} \quad (13)$$

As explored in equation (13) creditability table has been calculated.P_{ji} node j credibility is held by node j. The entries, P_{ji} are designed using the word "watchdog in equation (14):

$$P_{ji} = E(C_{ji}, P_{ji}) \quad (14)$$

As found in equation (14) watchdog mechanism has been evaluated. C_{ji} is the watchdog performance that is used remedially to change the i node credibility at node j. There are two separate subcomponents of the prestige for an RFSN-determined node, respectively, $(P_{ji})_C$ direct and $(P_{ji})_{iD}$indirect. The P_{ji}shall be $(P_{ji})_C$ and $(P_{ji})_{iD}$ as calculated and expressed in equation (15)

$$P_{ji} = (P_{ji})_C + (P_{ji})_{iD}$$
$$(P_{ji})_C = (C_{ji}, P_{ji})_c, \forall_i \in M_j$$
$$(P_{ji})_{iD} = (P_{ji})_{iD} + Z_{jL} \times P_{Li}, \forall_L \in M_j \quad (15)$$

As inferred in equation (15), creditability distribution has been expressed. The weight is extracted from the prestige of I and k nodes, $Z_{jL} = h(P_{jL})$. The proposed DNBIA model enhances the efficiency and response ratio and reduces the signal-to-noise ratio, delay rate, and latency ratio compared to other existing models.

3. Simulation Analysis

The proposed DNBIA model's simulation analysis has been performed based on the performance metrics such as efficiency, signal-to-noise ratio, delay, latency, and response ratio.

(i) Signal-to-Noise Ratio

Noise can be stated as any unwanted, deterministic or random signals that interfere with the system's desired signal's realistic imitation. The noise produced by e-devices differs importantly, as numerous diverse possessions generate it. In an electronic communication system, noise is an error or unwanted random disruption of a user data signal. The noise is a summation of disturbing or unwanted energy from natural and occasionally human-made sources. If the noise level in microvolts is V_n, and inward signal strength in microvolts is V_s, the signal-to-noise ratio, S/N, in decibels is provided by the expression: $S/N = 20\ log10\left(\frac{V_s}{V_n}\right)$. The suggested natural and bio-inspired model reduces the electronic communication noise rate when compared to other existing models. Figure 5 shows the DNBIA model's SNR ratio.

Doi: https://doi.org/10.54216/FPA.100109
Received: June 18, 2022 Accepted: November 12, 2022

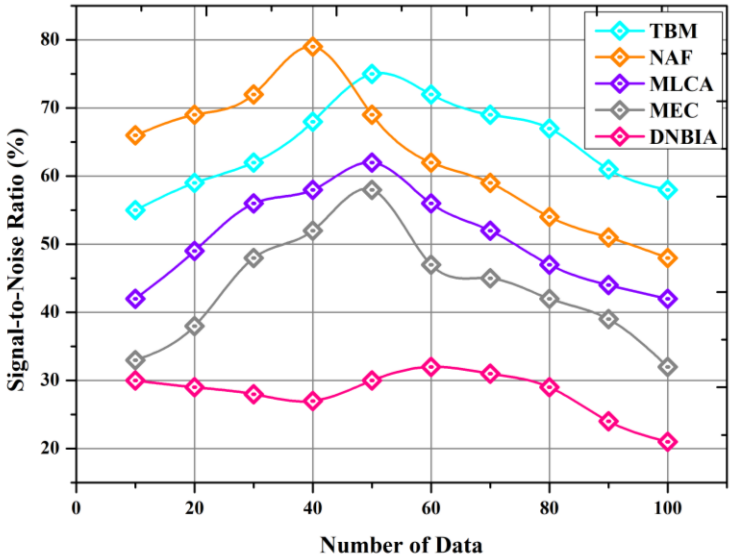

Figure 5: Signal-to-Noise Ratio

(ii) Efficiency Ratio

Globalization and the improvement of information technology are forcing many organizations to reconsider their business policies to be more productive and efficient in their operations. Digital communication systems often have built-in automation, analytics, and data management implements, permitting higher efficiency and productivity across the organizational teams. Recently, Bluetooth and WiFi chip sets are expressively lower power than their antecedents and are progressively competitive for certain classes of energy-efficient Internet of Thing-type applications, predominantly in the consumer electronics market. Factors like collision avoidance, ultra-low power operation, robustness, efficient channel utilization to time-varying channel and scalability, network conditions, and efficiency in terms of employment and memory requirements need to be addressed by designing natural bio-inspired algorithm-based knowledge transfer and electronic communications. Figure 6 shows the efficiency ratio.

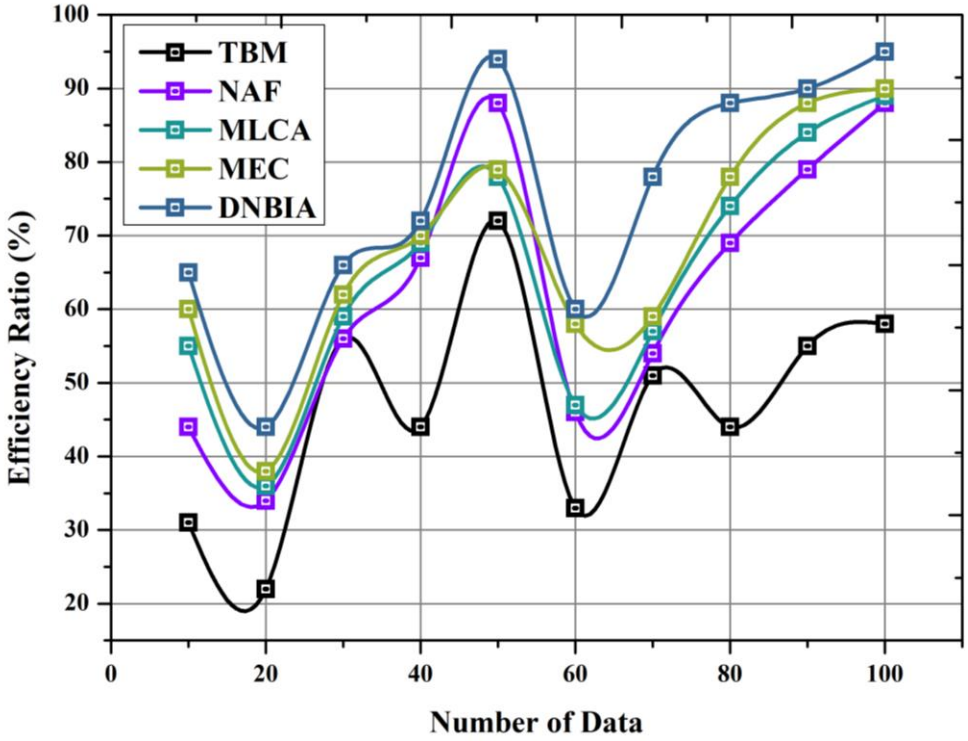

Figure 6: Efficiency Ratio

(iii) Delay Rate

Data transmission with extended-distance upturns the transmission delay, which does not encounter the necessity of low latency, high quality of service (QoS), and real-time in the network of thousands of interconnected devices and distresses the total efficiency of the system. This paper proposed a collaborative

Doi: https://doi.org/10.54216/FPA.100109
Received: June 18, 2022 Accepted: November 12, 2022

platform solution, which greatly simplified the collaborative application development mechanism and decreased delay and energy consumption because mobile users are far away from the cloud server and produce great transmission delay. This study analyzes the trade-offs between load balance and average network delay. The proposed natural and bio-inspired model reduces the delay rate in electronic communication compared to other existing approaches. Figure 7 shows the Delay rate.

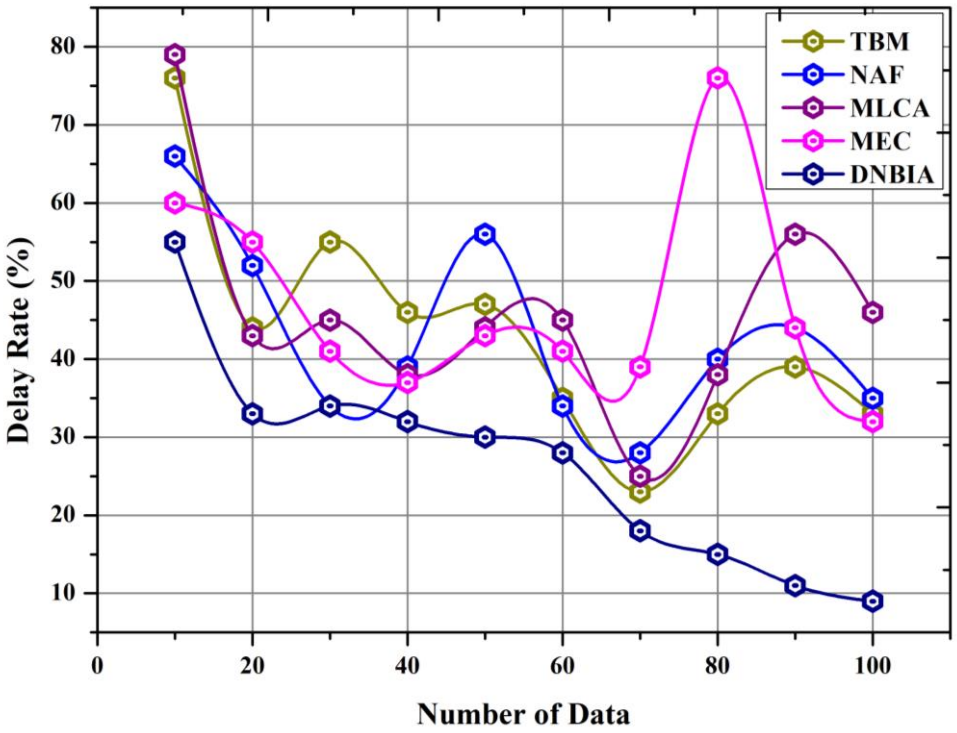

Figure 7: Delay Rate

(iv) Latency Rate

Latency is the delay in a web application's response to a user action, often mentioned in networking terms as the overall round trip time it takes for an information packet to travel. In an electronic communication network, latency processes the time it takes for data to get to its endpoint across the networks. The performance outcomes show that the DNBIA model reaches a greater packet delivery ratio, low packet loss, fault tolerance, reliability, and small latency. It overtakes congestion-aware multi-path routing methods in terms of packet delivery ratio. Considering low data-rate applications and effort, a tractable analytical method based on natural and bio-inspired algorithms modeling latency and energy efficiency as functions of protocol constraints involving slot duration, duty cycle, and total slots, seeking to identify optimal settings for given workloads stated by application-level constraints. Figure 8 shows the latency rate.

Doi: https://doi.org/10.54216/FPA.100109

Received: June 18, 2022 Accepted: November 12, 2022

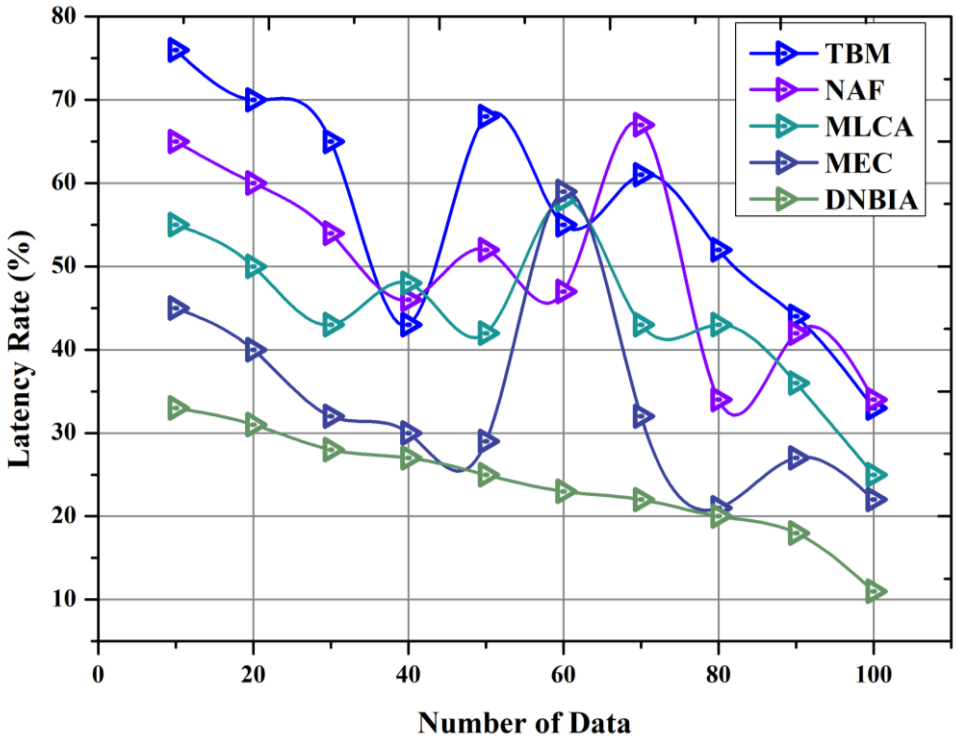

Figure 8: Latency Rate

(v) Response Time

Response times to authentication of communication sources and electronic communication involve inherent uncertainties. This proposed analysis indicates a need for policy regarding response times and suitable online behavior and recommends further training in the effective and appropriate use of electronic communication. Utilization of e-communication technology allows for new productivity options and includes additional time spent dealing with quick response time expectations. The suggested model enhances the response time based on natural and bio-inspired algorithms. Figure 9 demonstrates the response time.

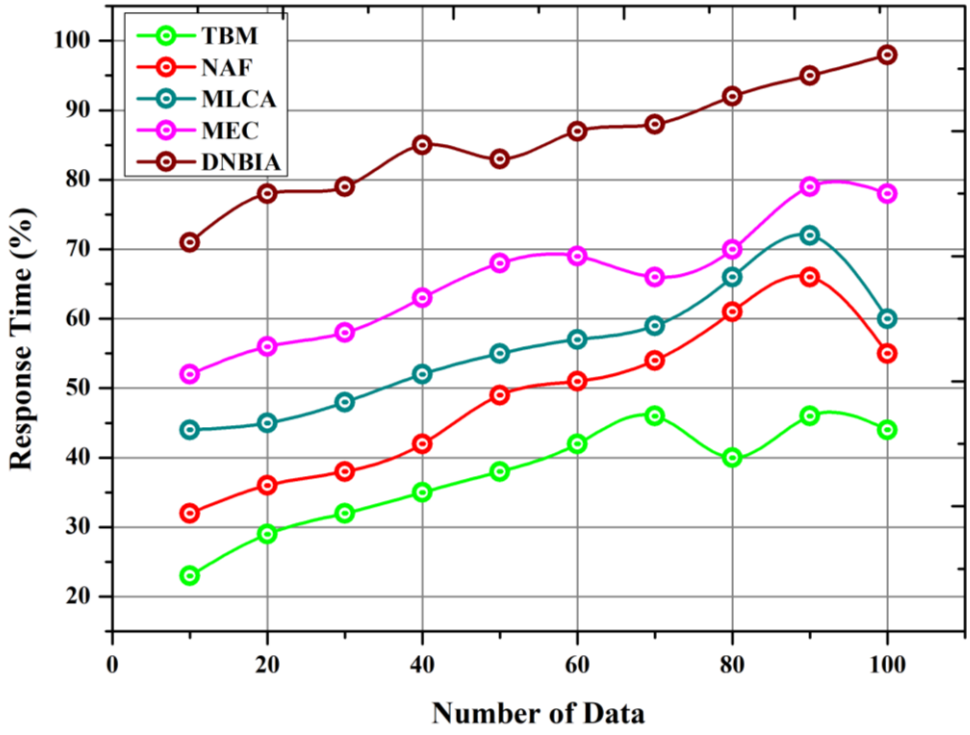

Figure 9: Response Time

The suggested DNBIA model enhances the efficiency, and response ratio and reduces the signal-to-noise ratio, delay rate, and latency ratio when compared to other existing trust-based monitoring (TBM), Novel Adaptive

Doi: https://doi.org/10.54216/FPA.100109
Received: June 18, 2022 Accepted: November 12, 2022

Framework (NAF), machine learning classification algorithms (MLCA), Mobile Edge Computing (MEC) methods.

4. Conclusion

This paper presents the DNBIA model for improving security and privacy in E-Communication systems and knowledge transfer. The influence of electronic handling and communication goes beyond management and security. Understanding human information processing's role in assessing privacy and security risks in electronic communications is significant. As the electronic communications network gets broader and the interconnectivity rises, security becomes international. Nature and bio-inspired computing is a computing paradigm stimulated by the attractive behavior of nature. The facets of natural and biological processes signify the behavior of the corresponding inspired algorithm. With the quickly varying scenario of the technological world, communication network values keep getting upgraded, and the natural and bio-inspired algorithms can adapt to any nature of networks. The experimental results show that the suggested DNBIA model enhances the efficiency ratio of 97.8% and response ratio of 98.3% and reduces the signal-to-noise ratio of 19.2%, delay rate of 9.2%, and latency ratio of 11.5% compared to other existing approaches.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Byrne, J., & Kirwan, G. (2019). Relationship-based social work and electronic communication technologies: anticipation, adaptation and achievement. *Journal of Social Work Practice*, *33*(2), 217-232.

[2] Mijwil, M., Youssef Filali, Mohammad Aljanabi, Mariem Bounabi, Humam Al-Shahwani, & ChatGPT. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. Mesopotamian Journal of CyberSecurity, 2023, 1–6. https://doi.org/10.58496/MJCS/2023/001

[3] Navarro-Millán, I., Zinski, A., Shurbaji, S., Johnson, B., Fraenkel, L., Willig, J., ... & Safford, M. M. (2019). Perspectives of rheumatoid arthritis patients on electronic communication and patient-reported outcome data collection: a qualitative study. *Arthritis care & research*, *71*(1), 80-87.

[4] Khan, F., Jan, M. A., Rehman, A. U., Mastorakis, S., Alazab, M., & Watters, P. (2020). A Secured and Intelligent Communication Scheme for IIoT-enabled Pervasive Edge Computing. IEEE Transactions on Industrial Informatics.

[5] Brundin-Mather, R., Zjadewicz, K., Soo, A., & Stelfox, H. T. (2020). Improving transitions in care from intensive care units: Development and pilot testing of an electronic communication tool for healthcare providers. *Journal of critical care*, *56*, 265-272.

[6] Kadry, S., & Barbar, A. (2009). Design of secure mobile communication using fingerprint. European Journal of Scientific Research, 30(1), 138-145.

[7] Krynski, L., Ghersin, S., Del Valle, M., & Cardigni, G. (2019). Communication through electronic media in pediatrics. Use recommendations. *Archivos argentinos de pediatria*, *117*(4), S175-S179.

[8] Ahmad, I. S., Kalakech, A., & Kadry, S. (2014). Modified Binary Exponential Backoff Algorithm to Minimize Mobiles Communication Time. IJ Information Technology and Computer Science, 3, 20-29.

[9] Liu, J., Wan, J., Jia, D., Zeng, B., Li, D., Hsu, C. H., & Chen, H. (2017). High-efficiency urban traffic management in context-aware computing and 5G communication. IEEE Communications Magazine, 55(1), 34-40.

[10] Hsu, C. H., Slagter, K. D., & Chung, Y. C. (2015). Locality and loading aware virtual machine mapping techniques for optimizing communications in MapReduce applications. Future Generation Computer Systems, 53, 43-54.

[11] Ali, A. H., Mohanad G. Yaseen, Mohammad Aljanabi, Saad Abbas Abed, & ChatGPT. (2023). Transfer Learning: A New Promising Techniques. Mesopotamian Journal of Big Data, 2023, 31–32. https://doi.org/10.58496/MJBD/2023/004

[12] Hasnat, M.A., Akbar, M., Iqbal, Z., Khan, Z.A., Qasim, U. and Javaid, N., 2015, February. Bio inspired distributed energy efficient clustering for Wireless Sensor Networks. In *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)* (pp. 1-7). IEEE.

[13] Chituc, C.M. and de Oliveira Restivo, F.J., 2009. Challenges and Trends in Distributed Manufacturing Systems: Are wise engineering systems the ultimate answer?. In *Second MIT International Symposium on Engineering Systems*.

[14] Kumar, N., & Lee, J. H. (2013). Peer-to-peer cooperative caching for data dissemination in urban vehicular communications. IEEE Systems Journal, 8(4), 1136-1144.

[15] Chaudhary, R., Aujla, G. S., Garg, S., Kumar, N., & Rodrigues, J. J. (2018). SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment. IEEE Transactions on Industrial Informatics, 14(6), 2629-2640.

[16] Dua, A., Kumar, N., Das, A. K., & Susilo, W. (2017). Secure message communication protocol among vehicles in smart city. IEEE Transactions on Vehicular Technology, 67(5), 4359-4373.

[17] Mahmoud, E. E., & AL-Harthi, B. H. (2019). Secure communications via modified complex phase synchronization of two hyperchaotic complex models with identical linear structure and adjusting in nonlinear terms. Journal of Intelligent & Fuzzy Systems, 37(1), 17-25.

[18] Li, J., Zhao, H., Hafid, A.S., Wei, J., Yin, H. and Ren, B., 2019. A bio-inspired solution to cluster-based distributed spectrum allocation in high-density cognitive Internet of Things. *IEEE Internet of Things Journal*, *6*(6), pp.9294-9307.

[19] Gaona-García, P., Mendoza, D., Vargas, F., & Montenegro-Marin, C. (2019). Evaluation of a Medical Alert Communication Infrastructure Based on Fuzzy Logic and IoT Devices. Advanced Science Letters, 25(1), 21-24.

[20] Alqahtani, F., Al-Makhadmeh, Z., Tolba, A., & Said, O. (2020). TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications. *Computer Communications*, *150*, 216-225.

[21] Sharmeen, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). An adaptive framework against android privilege escalation threats using deep learning and semi-supervised approaches. *Applied Soft Computing*, *89*, 106089.

[22] Jaber, M.M., Ali, M.H., Abd, S.K., Jassim, M.M., Alkhayyat, A., Alreda, B.A., Alkhuwaylidee, A.R. and Alyousif, S., 2022. A Machine Learning-Based Semantic Pattern Matching Model for Remote Sensing Data Registration. Journal of the Indian Society of Remote Sensing, pp.1-14.

[23] Al Ridhawi, I., Otoum, S., Aloqaily, M., Jararweh, Y., & Baker, T. (2020). Providing secure and reliable communication for next generation networks in smart cities. *Sustainable Cities and Society*, *56*, 102080.

Doi: https://doi.org/10.54216/FPA.100109

Received: June 18, 2022 Accepted: November 12, 2022