ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

DESIGN OF AN EFFICIENT HIGH-TRUST MODEL FOR IMPROVING NETWORK COMMUNICATION CONSISTENCY VIA INCREMENTAL BIOINSPIRED OPTIMIZATIONS: HTMNCB

Pragati Narayan Patil*, Dr Atul D Raut
Research scholar, Department of Computer Science, Sant Gadge Baba Amravati University, Amravati, pragatimit@gmail.com
Associate Professor, Department of CSE, P R Pote College of Engineering and Management

Abstract: Node failure in Wireless Sensor Networks (WSNs) is common, which might occur due to internal or external faults. But existing fault tolerance models are either highly complex, or showcase lower efficiency when applied to real-time scenarios. To overcome these issues, this paper proposes an efficient high-trust model for improving network communication consistency through incremental bio-inspired optimizations. The model is designed to address the challenges of maintaining consistent and reliable network communication in the presence of network failures, malicious attacks, and other unforeseen events that can disrupt network operations. The proposed model utilizes Grey Wolf Optimization (GWO) & Antlion Optimization (ALO) techniques to incrementally optimize network communication parameters and configurations in response to changing network conditions. The model's effectiveness is evaluated through simulations that demonstrate its ability to maintain consistent network communication and mitigate the impact of network failures and malicious attacks. The results of the simulations show that the proposed model improves network communication consistency while reducing the overall network downtime and increasing its trustworthiness. The high-trust model presented in this paper has significant implications for network communication in critical infrastructure systems, such as healthcare, transportation, and energy, where reliable and consistent network communication is essential under real-time scenarios.

Keywords: Trust, Fault, Bioinspired, Grey, Wolf, Antlion, Optimizations

Introduction

Maintaining a consistent level of network communication is essential to ensuring that today's communication systems continue to function in a dependable and effective manner. On the other hand, keeping network communication continuous is becoming more difficult as a result of the increasing complexity of network infrastructures, the increase in the number of cyber dangers and assaults, and the unpredictability of network events [1, 2, 3]. Traditional methods of network optimization and management are frequently insufficient to adequately address these challenges because they have a restricted capacity to adapt to shifting network conditions and are vulnerable to malicious attacks. More advanced methods of network optimization and management have the potential to overcome these limitations via use of Trust Aware Network Slices (TANS) [4, 5, 6]. In recent years, bio-inspired optimization approaches have surfaced as an intriguing new strategy that carries the potential to improve the consistency of network communications via use of Multifaceted Trust Management (MTM) [7, 8, 9]. In order to maximise network characteristics and configurations, these methods take their cues from natural occurrences such as ant colonies, genetic algorithms, and particle swarms. Techniques of optimization that are inspired by biological processes are particularly well-suited for the task of addressing the challenges associated with maintaining consistent network communication because of their ability to adapt to shifting network conditions and provide solutions that are both robust and resistant to attacks [10, 11, 12].

The purpose of this article is to suggest an effective high-trust model for the purpose of increasing the consistency of network communication through progressive bio-inspired optimizations. In order to maximise network communication parameters and configurations in reaction to shifting network circumstances, the model makes use of optimization techniques that are influenced by biological systems. Simulations are used to evaluate the suggested model. These simulations demonstrate the model's capacity to maintain continuous network communication as well as minimise the effect of malevolent assaults and breakdowns in the network scenarios.

The remaining parts of the document are organised as described below. In Section 2, a synopsis of related work is presented, focusing on bio-inspired optimization approaches and network optimization. In Section 3, we will discuss the high-trust paradigm that has been suggested for the purpose of making network communication more consistent. The findings of the experiment are presented in Section 4 for different use cases. The last part of the article, Section 5, provides a conclusion and addresses prospective recommendations for further improvements.

Literature Review

The development of trust models is an essential component in achieving greater consistency in network communications [13, 14, 15]. They make it possible to evaluate and build confidence between the various organisations that are part of a network by providing a mechanism for doing so. In this overview of the relevant literature, we are going to talk about the various trust models that have been suggested to enhance the consistency of network communications [16, 17, 18].

In the realm of network communication, one of the trust models that sees the most widespread application is the reputation-based trust models &Deep Reinforcement Learning (DRL) [19, 20]. In order to build confidence between the various organisations that make up a network, it uses the idea of reputation as its foundation. In this paradigm, every object keeps a number that is dependent on its reputation relative to its previous actions [21, 22, 23]. After that, the reputation number is used to establish the trustworthiness of the person in subsequent interactions with other people. This approach has been implemented in a variety of different applications, such as peer-to-peer networks, social networking, and online shopping scenarios [24, 25, 26].

Establishing confidence between organisations in a network can also be done with the help of another well-known trust model, which is called the Web of confidence models [27, 28, 29]. This paradigm is predicated on the idea of a web of confidence, in which every entity in the network is connected to a network of other entities that can be trusted. When two entities communicate with one another, they have the opportunity to establish confidence by independently confirming the identities of the other entity through their respective networks of trustworthy entities. This paradigm is utilised in the majority of email correspondence systems in addition to certain peer-to-peer networking systems [30, 31, 32].

The certificate-based trust model is a model of confidence that is utilised frequently in the context of ensuring the safety of communications conducted via the internet. Under this configuration, each entity in the network is given a digital certificate that includes a copy of its public keys [33].

The digital certificate is then used to establish the identification of the organization, guarantee the communication's integrity, and keep the content of the conversation confidential. This approach is widely utilised in a wide variety of applications, including private email correspondence, online shopping, and online banking scenarios.

The Trust Propagation model is a trust model that is founded on the idea of spreading confidence throughout a network. It is also known as the confidence Chain models [30, 31, 32]. In this paradigm, confidence is transferred along a network of intermediary entities, beginning with entities that are already considered trustworthy and ending with entities that are not yet considered trustworthy. This paradigm is frequently utilised in peer-to-peer networks, which are characterised by the transmission of confidence from trustworthy nodes to unverified nodes via a series of intermediary nodes [28, 29, 30].

It is possible to enhance the consistency of network communication by using a trust model known as the Hybrid Trust model, which incorporates several different trust models. This approach establishes confidence between organisations in the network through a combination of reputation-based trust, certificate-based trust, and a web of trust. This model is frequently used in applications where it is necessary to establish confidence using a combination of different trust models, such as when conducting private correspondence over the internet for different scenarios [31, 32].

The development of trust models is an essential component in achieving greater consistency in network communication. When it comes to establishing confidence between organisations in a network, numerous trust models have been suggested, and each one has seen use in a specific application. There are many different types of trust models, but some of the most common ones are reputation-based trust, web of trust, certificate-based trust, trust transmission, and blended trust models [24, 25, 26]. The particular specifications of the application and the characteristics of the network should both be taken into consideration when choosing a confidence model for real-time scenarios. Work in [34, 35] further propose use of bioinspired models for optimization of different networks under multiple attack types.

Design of the proposed dual-Bioinspired Low-complexity data Mining engine for automatic Cluster analysis via Ensemble learning operations

After referring to the review of existing trust-based models used to secure network communications under faults, it can be observed that these models are either highly complex, or showcase lower efficiency when applied to real-time scenarios.

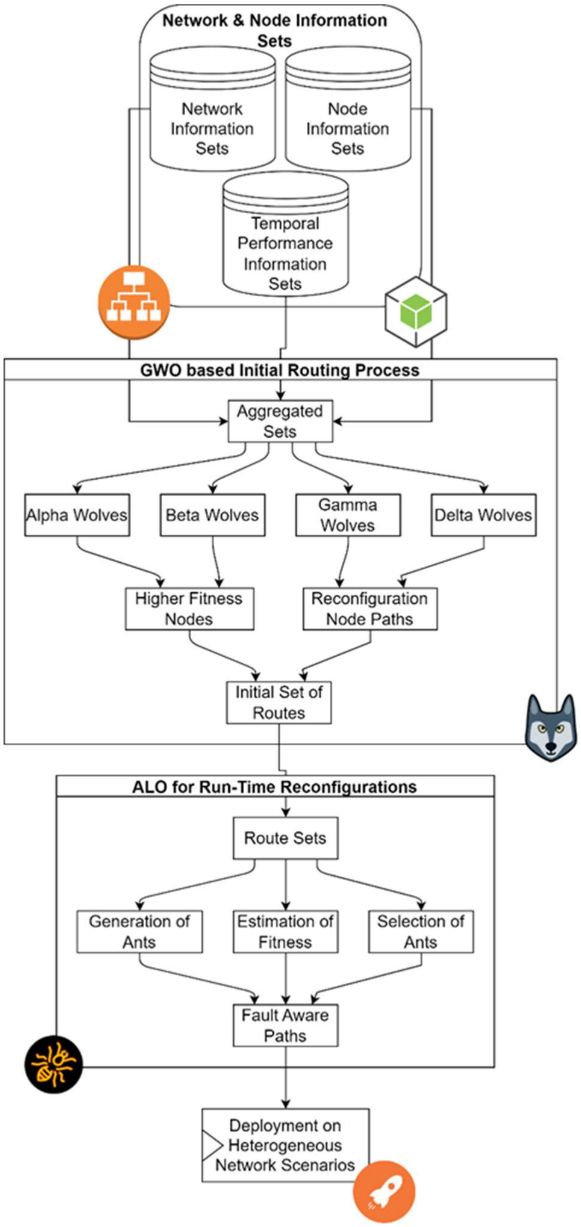


Figure 1. Design of the proposed trust-model for improving network performance under faults

To overcome these issues, this section proposes design of an efficient high-trust model for improving network communication consistency through incremental bio-inspired optimizations. From figure 1, it can be observed that the model is designed to address the challenges of maintaining consistent and reliable network communication in the presence of network failures, malicious attacks, and other unforeseen events that can disrupt network operations. The proposed model utilizes Grey Wolf Optimization (GWO) & Antlion Optimization (ALO) techniques to incrementally optimize network communication parameters and configurations in response to changing network conditions.

Based on the flow of proposed model, it can be observed that the model initially collects network information sets including bandwidth, received signal strength indicator, previous communication information, etc. And fuses it with node-level information sets including node

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

locations, temporal Packet Delivery Ratio (PDR), throughput, residual & consumed energy, etc. This data is collected for each node under normal & fault conditions. After collection of these data samples, a Trust Score (TS) is estimated for each node via equation 1,

$$TL(N,F) = \frac{\frac{D(N)}{D(F)} + \frac{E(N)}{E(F)} + \frac{T(F)}{T(N)} + \frac{PDR(F)}{PDR(N)}}{4} \dots (1)$$

Where, D,E T & PDR are the temporal communication delays, communication energy levels, temporal throughput levels, and temporal packet delivery ratios for previous N normal communications, and F faulty communications. The delay is estimated via equation 2,

$$D(N) = \frac{\sum_{i=1}^{N} t_{complet\ i} - t_{start_i}}{N} \dots (2)$$

Where, t_start&t_complete represents the start & completion timestamps of communications. Similarly, the energy, throughput and PDR levels are estimated via equations 3, 4 & 5 as follows,

$$E(N) = \frac{\sum_{i=1}^{N} E_{star\ i} - E_{complete_i}}{N} \dots (3)$$

$$T(N) = \sum_{i=1}^{N} \frac{Rx(P)_i}{N * D(N)} \dots (4)$$

$$PDR(N) = \sum_{i=1}^{N} \frac{Rx(P)_i}{Tx(P)_i * N} \dots (5)$$

Where, E_start&E_complete are initial and completion residual energy levels for the nodes during different communications, while Tx & Rx represents total number of transmitted & received packets during these communications. Based on these evaluations, a trust threshold is estimated via equation 6 as follows,

$$T_{th} = \sum_{i=1}^{N} \sum_{j=1}^{F} \frac{TL(i,j)}{N * F} \dots (6)$$

Nodes with TL(N,F)>T_th are used for further routing operations, while other nodes are discarded for the current routing process. To further assist in selection of nodes for routing data between a given pair of src & dest nodes, a Grey Wolf Optimization (GWO) based model is used, which works as per the following process,

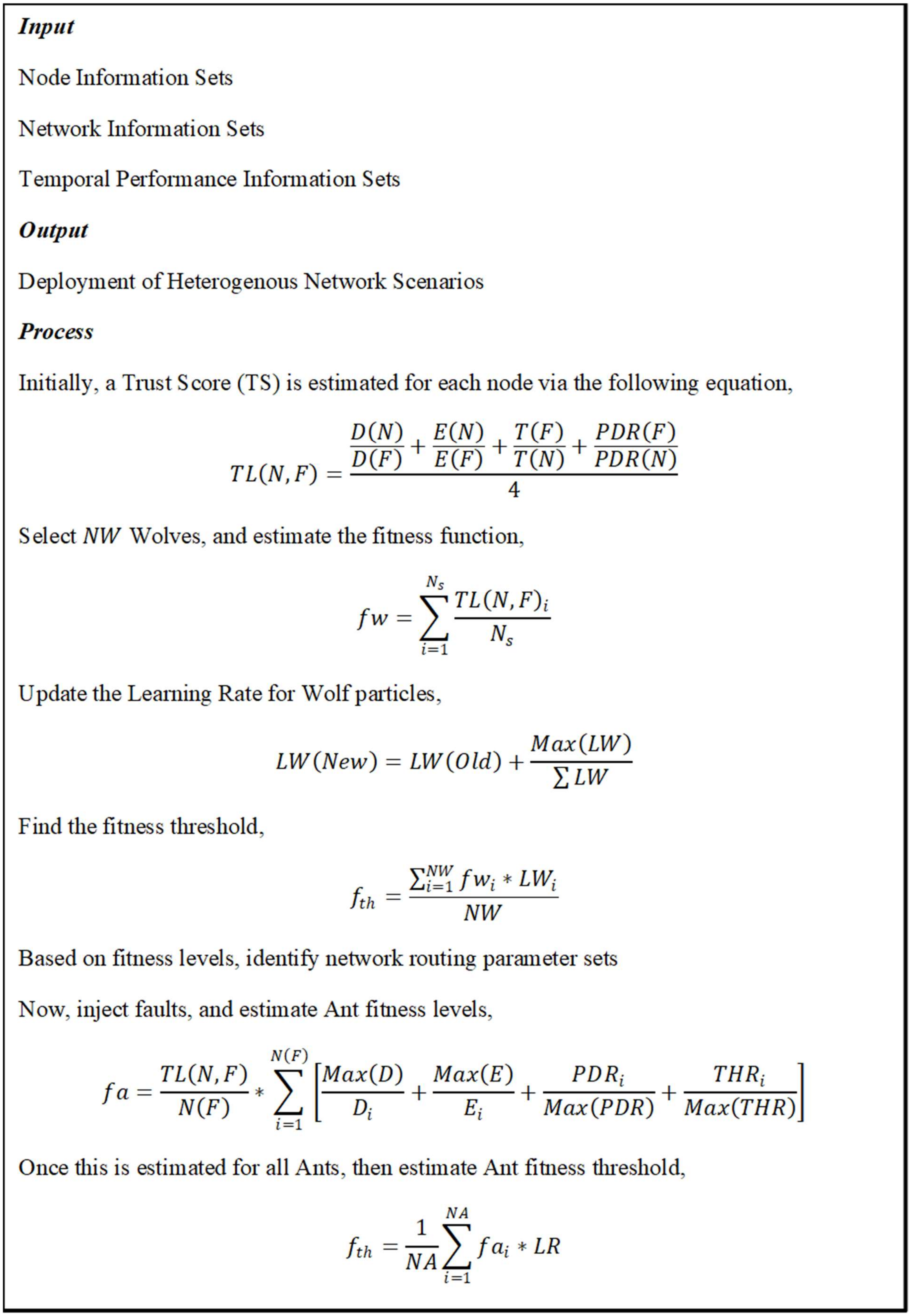
Initially, a set of NW different Wolves are generated by selecting multiple nodes between source & destination nodes via equation 7,

$$N = STOCH\big(1, N(T)\big) \dots (7)$$

Where, N(T) represents number of trusted nodes, while STOCH represents a stochastic process for generation of number sets.

A set of nodes that satisfy equation 8 are continuously selected till destination node is reached, which generates one set of Wolf configurations.

$$d(src,N) < d(src,dest) \& \ d(N,dest) < d(src,dest) \dots (8)$$



Input

Node Information Sets

Network Information Sets

Temporal Performance Information Sets

Output

Deployment of Heterogenous Network Scenarios

Process

Initially, a Trust Score (TS) is estimated for each node via the following equation,

$$TL(N,F)=\frac{\frac{D(N)}{D(F)}+\frac{E(N)}{E(F)}+\frac{T(F)}{T(N)}+\frac{PDR(F)}{PDR(N)}}{4}$$

Select NW Wolves, and estimate the fitness function,

$$fw=\sum_{i=1}^{N_s}\frac{TL(N,F)_i}{N_s}$$

Update the Learning Rate for Wolf particles,

$$LW(New)=LW(Old)+\frac{Max(LW)}{\sum LW}$$

Find the fitness threshold,

$$f_{th}=\frac{\sum_{i=1}^{NW} fw_i * LW_i}{NW}$$

Based on fitness levels, identify network routing parameter sets

Now, inject faults, and estimate Ant fitness levels,

$$fa=\frac{TL(N,F)}{N(F)}*\sum_{i=1}^{N(F)}\left[\frac{Max(D)}{D_i}+\frac{Max(E)}{E_i}+\frac{PDR_i}{Max(PDR)}+\frac{THR_i}{Max(THR)}\right]$$

Once this is estimated for all Ants, then estimate Ant fitness threshold,

$$f_{th}=\frac{1}{NA}\sum_{i=1}^{NA} fa_i * LR$$

Where, $d(i,j)$ is distance between nodes i & j, and is estimated via equation 9,

$$d(i,j) = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \dots (9)$$

- Similarly, a set of NW such Wolves are generated, and their fitness is estimated via equation 10 as follows,

$$fw = \sum_{i=1}^{N_s} \frac{TL(N,F)_i}{N_s} \dots (10)$$

Where, N_s represents total number of nodes selected during the routing process.

- After generation of NW different Wolf configurations, a fitness threshold is calculated via equation 11,

$$f_{th} = \frac{\sum_{i=1}^{NW} fw_i * LW_i}{NW} \dots (11)$$

Where, LW_i represents learning rate for the i^{th} Wolf, and is updated in each set of iterations.

- Wolves with $fw > 2f_{th}$ are marked as 'Alpha', and their configurations are kept unchanged during current set of iterations.

- Wolves with $fw > f_{th}$ are marked as 'Beta', and their learning rate is modified as per equation 12,

$$LW(New) = LW(Old) + \frac{Max(LW)}{\sum LW} \dots (12)$$

- Wolves with $fw < \frac{f_{th}}{2}$ are marked as 'Gamma', and their learning rate is modified as per equation 13,

$$LW(New) = LW(Old) + \frac{LW(Beta)}{\sum LW} \dots (13)$$

- All other Wolves are marked as 'Delta', and their learning rate is modified as per equation 14,

$$LW(New) = LW(Old) + \frac{LW(Gamma)}{\sum LW} \dots (14)$$

- For each pair of source & destination, this process is continued for NI iterations.

After completion of all iterations, node configurations that satisfy equation 15 are marked as initial routing configurations.

$$RC = \bigcup_{i=1}^{fw>2f_{th}} RC_i \dots (15)$$

Where, RC represents the routing configuration which was stochastically generated by different Wolf particles. These routes are further optimized via an Ant Lion Optimizer (ALO), which assists in identification of fault-tolerant routes. The ALO Model works as per the following process,

- From the set of GWO routes, stochastically select a route via equation 16,

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

$$SR = STOCH\big(1, N(RC)\big) \ldots (16)$$

Where, SR is the selected route, while $N(RC)$ are the number of routing configurations selected by the GWO process.

- For the selected routes, inject $N(F)$dummy node-level faults, and estimate Ant Fitness (fa) via equation 17,

$$fa = \frac{TL(N,F)}{N(F)} * \sum_{i=1}^{N(F)} \left[\frac{Max(D)}{D_i} + \frac{Max(E)}{E_i} + \frac{PDR_i}{Max(PDR)} + \frac{THR_i}{Max(THR)}\right] \ldots (17)$$

- A set of NA such Ants are generated, and a fitness threshold is estimated via equation 18,

$$f_{th} = \frac{1}{NA}\sum_{i=1}^{NA} fa_i * LR \ldots (18)$$

Where, LR represents Learning Rate of the Ants.

- After generation of NA such particles, Ants with $fa > f_{th}$ are passed directly to the next iteration, while other Ants are discarded and new Ants are generated via equations 16 & 17 for the next set of iterations.
- This process is repeated for NI iterations, and new Ants are generated & configured for each of these iterations.

After completion of all iterations, Ants with highest fitness levels are selected, and their node configurations are used for the routing process. Due to these operations the model is capable of selecting routes with high trust levels. To validate the performance of this model, it was simulated under different fault conditions in the next section of this text.

1. Result evaluation and comparative analysis with existing techniques

The proposed model utilizes Grey Wolf Optimization (GWO) & Antlion Optimization (ALO) techniques to incrementally optimize network communication parameters and configurations in response to changing network conditions.These network conditions can be observed as follows,

Total Communication Nodes: 10k

Communication Size: 1k bytes per set of communications

Energy Model: $TE = 2\ mJ, RE = 1mJ, IdleE = 0.0005\ mJ$

Where, $TE, RE\ \&\ IdleE$ represents the energy needed for transmission, energy needed for reception and idle energy of the communicationnodes. These setups were used to create a collection of 1.25 million block addition requests, 20% of which were stochastically transformed into fault requests. These flaws include communication, source, and destination defects. The average communication delay (D), average energy required for communication (E), speed received during communication (T), and packet delivery ratio (PDR) were assessed while carrying out these defects for various numbers of communication requests. (NC). This performance was contrasted with three newly suggested optimization models for wireless installations, TANS [4], MTM [8], and DRL [22]. Table 1 provides the following information about the transmission latency based on these strategies,

NC	**D (s)** **TANS [4]**	**D (s)** **MTM [8]**	**D (s)** **DRL [22]**	**D (s)** **HTM NCB**
125k	4.02	4.43	4.62	1.83
187k	4.76	5.24	5.47	2.16
250k	5.50	6.05	6.32	2.50
375k	6.22	6.84	7.14	2.82
500k	6.91	7.60	7.93	3.14
625k	7.60	8.37	8.72	3.45
750k	8.30	9.15	9.53	3.78
1M	9.02	9.94	10.35	4.10
1.25M	9.75	10.73	11.18	4.43

Table 1. Average communication delay under 20% faults

According to this assessment and figure 2, it was found that the suggested model can increase communication speed under heavy communication demand by 15.4% compared to TANS [4], 16.4% compared to MTM [8], and 18.5% compared to DRL [22]. The use of temporal communication delay through GWO improvements and the use of delay measures during node selection through ALO operations both contribute to an increase in communication performance. Because of this, the model can be used in situations involving high-speed cellular networks.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

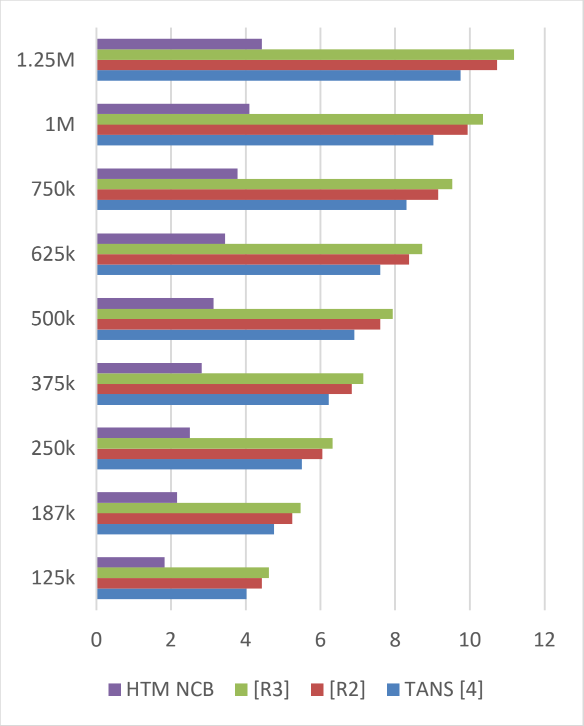


Figure 2. Average communication delay under different faults

Similarly, the energy needed for these communication operations can be observed from table 2 as follows,

NC	**E (mJ)** **TANS [4]**	**E (mJ)** **MTM [8]**	**E (mJ)** **DRL [22]**	**E (mJ)** **HTM NCB**
125k	50.33	47.90	44.51	22.84
187k	52.78	50.24	46.68	23.95
250k	55.40	52.73	48.99	25.14
375k	58.17	55.37	51.43	26.40
500k	60.92	57.98	53.85	27.64
625k	63.59	60.51	56.21	28.85
750k	66.18	62.98	58.50	30.03

1M	68.73	65.40	60.76	31.19
1.25M	71.32	67.86	63.05	32.36

Table 2. Average communication energy under 20% faults

Based on this evaluation and Figure 3, it was determined that the proposed model can increase the communication lifetime by 29.5% compared to TANS [4], 24.9% compared to MTM [8], and 24.5% compared to DRL [22] for a significant number of communication requests. This energy consumption is optimised by utilising temporal communication energy during GWO optimizations and residual energy metrics during node selection via ALO operations. Due to this, the model is deployable in scenarios involving high-lifetime wireless networks.

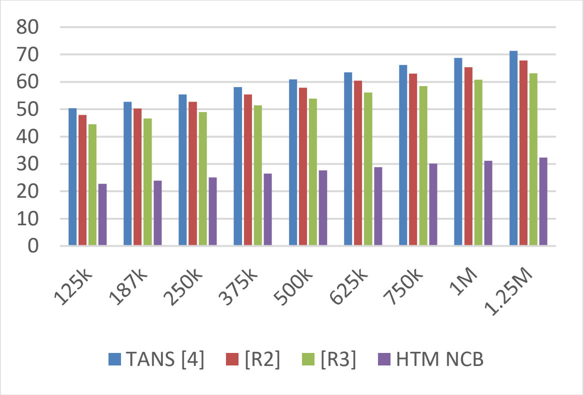


Figure 3. Average communication energy under different faults

Similarly, the throughput needed for these communications is tabulated in table 3 as follows,

NC	Thr. (kbps) TANS [4]	Thr. (kbps) MTM [8]	Thr. (kbps) DRL [22]	Thr. (kbps) HTM NCB
125k	2594.3	1866.9	2861.8	4850.2
187k	2618.1	1884.1	2888.0	4894.7
250k	2641.0	1900.6	2913.3	4937.5
375k	2665.8	1918.4	2940.7	4983.9
500k	2691.7	1937.1	2969.3	5032.4

625k	2717.7	1955.8	2997.9	5080.9
750k	2742.8	1973.9	3025.7	5127.9
1M	2767.4	1991.6	3052.8	5174.0
1.25M	2791.6	2009.1	3079.6	5219.3

Table 3. Average throughput under 20% faults

Based on the results of the assessment and the data presented in Figure 4, it was determined that the suggested model increases communication speed by 18.5% compared to TANS [4], 23.4% compared to MTM [8], and 16.5% compared to DRL [22] when dealing with a high number of communication requests. The utilisation of temporal data rate via GWO improvements and the utilisation of throughput measures while selecting nodes via ALO operations both contribute to the enhancement of communication throughput. This allows the model to be used in real-world situations where cellular transmission rates are extremely high for different scenarios.

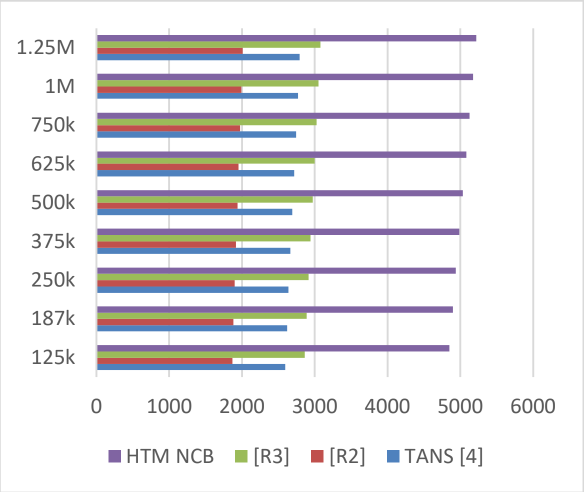


Figure 4. Average throughput under different faults

Similarly, the PDR can be observed from table 4 as follows,

NC	**PDR (%)** **TANS [4]**	**PDR (%)** **MTM [8]**	**PDR (%)** **DRL [22]**	**PDR (%)** **HTM NCB**
125k	94.4	91.0	82.9	97.9

187k	94.5	91.1	83.0	98.0
250k	94.6	91.2	83.1	98.1
375k	94.7	91.3	83.1	98.2
500k	94.8	91.4	83.2	98.3
625k	94.9	91.5	83.3	98.4
750k	95.0	91.6	83.4	98.5
1M	95.1	91.7	83.5	98.6
1.25M	95.1	91.8	83.5	98.7

Table 4. Average PDR under 20% faults

According to this assessment and figure 5, it was discovered that the suggested model is able to enhance the communication PDR by 3.5% when compared with TANS [4], 5.9% when compared with MTM [8], and 15.4% when compared with DRL [22] under conditions involving a large number of communication requests. The effectiveness of this communication has been enhanced as a result of the utilisation of temporal PDR through GWO optimizations and the utilisation of PDR measures during the selection of nodes through ALO operations. Because of this, the device is suitable for use in high packet delivery ratio (PDR) cellular network situations.

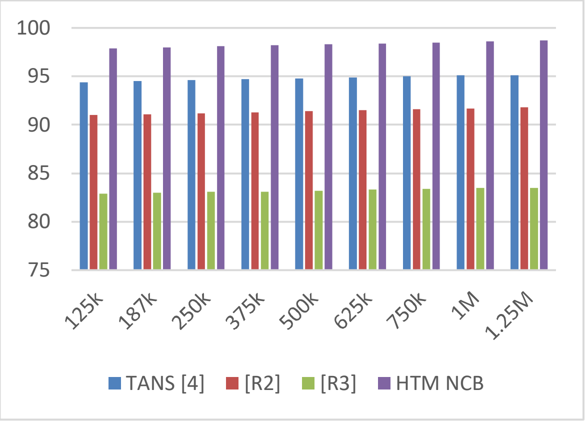


Figure 5. Average PDR under different faults

Based on these analyses, it can be seen that the suggested model, when compared to current models, was able to increase communication speed, decrease communication energy, while increasing capacity and packet distribution effectiveness. Because of this, a variety of wireless rollout situations can use the suggested GWO-based QoS-aware operations & ALO-based fault-aware node selection process.

2. Conclusions & Future Scopes

The proposed model utilizes Grey Wolf Optimization (GWO) & Antlion Optimization (ALO) techniques to incrementally optimize network communication parameters and configurations in response to changing network conditions. According to evaluation of delay, it was found that the suggested model can increase communication speed under heavy communication demand by 15.4% compared to TANS [4], 16.4% compared to MTM [8], and 18.5% compared to DRL [22]. The use of temporal communication delay through GWO improvements and the use of delay measures during node selection through ALO operations both contribute to an increase in communication performance. Because of this, the model can be used in situations involving high-speed cellular networks.Based on evaluation of energy levels, it was determined that the proposed model can increase the communication lifetime by 29.5% compared to TANS [4], 24.9% compared to MTM [8], and 24.5% compared to DRL [22] for a significant number of communication requests. This energy consumption is optimised by utilising temporal communication energy during GWO optimizations and residual energy metrics during node selection via ALO operations. Due to this, the model is deployable in scenarios involving high-lifetime wireless networks.

Upon assessment of throughput levels, it was determined that the suggested model increases communication speed by 18.5% compared to TANS [4], 23.4% compared to MTM [8], and 16.5% compared to DRL [22] when dealing with a high number of communication requests. The utilisation of temporal data rate via GWO improvements and the utilisation of throughput measures while selecting nodes via ALO operations both contribute to the enhancement of communication throughput. This allows the model to be used in real-world situations where cellular transmission rates are extremely high for different scenarios. In terms of packet delivery performance, it was discovered that the suggested model is able to enhance the communication PDR by 3.5% when compared with TANS [4], 5.9% when compared with MTM [8], and 15.4% when compared with DRL [22] under conditions involving a large number of communication requests. The effectiveness of this communication has been enhanced as a result of the utilisation of temporal PDR through GWO optimizations and the utilisation of PDR measures during the selection of nodes through ALO operations. Because of this, the device is suitable for use in high packet delivery ratio (PDR) cellular network situations. Based on these analyses, it can be seen that the suggested model, when compared to current models, was able to increase communication speed, decrease communication energy, while increasing capacity and packet distribution effectiveness. Because of this, a variety of wireless rollout situations can use the suggested GWO-based QoS-aware operations & ALO-based fault-aware node selection process.

In future, the model must be evaluated for larger number of fault scenarios, and can be extended via use of Q-Learning, and Auto Encoders for pre-emptive identification of fault nodes. This performance can also be improved via use of low complexity autoregressive models that can assist in enhancing fault detection performance under large number of nodes & network configurations.

References

[1] T. Wu, X. Liu, J. Qin and F. Herrera, "Trust-Consensus Multiplex Networks by Combining Trust Social Network Analysis and Consensus Evolution Methods in Group Decision-Making," in IEEE Transactions on Fuzzy Systems, vol. 30, no. 11, pp. 4741-4753, Nov. 2022, doi: 10.1109/TFUZZ.2022.3158432.

[2] J. Wang, Z. Yan, H. Wang, T. Li and W. Pedrycz, "A Survey on Trust Models in Heterogeneous Networks," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2127-2162, Fourthquarter 2022, doi: 10.1109/COMST.2022.3192978.

[3] F. Li, Z. Guo, C. Zhang, W. Li and Y. Wang, "ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain," in IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4011-4021, May 2021, doi: 10.1109/TVT.2021.3050007.

[4] V. Varadharajan, K. K. Karmakar, U. Tupakula and M. Hitchens, "Toward a Trust Aware Network Slice-Based Service Provision in Virtualized Infrastructures," in IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 1065-1082, June 2022, doi: 10.1109/TNSM.2021.3128882.

[5] S. S. Desai and M. J. Nene, "Multihop Trust Evaluation Using Memory Integrity in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4092-4100, 2021, doi: 10.1109/TIFS.2021.3101051.

[6] S. S. Desai and M. J. Nene, "Multihop Trust Evaluation Using Memory Integrity in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4092-4100, 2021, doi: 10.1109/TIFS.2021.3101051.

[7] S. Dhelim, N. Aung, M. T. Kechadi, H. Ning, L. Chen and A. Lakas, "Trust2Vec: Large-Scale IoT Trust Management System Based on Signed Network Embeddings," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 553-562, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3201772.

[8] H. El-Sayed, H. Alexander, P. Kulkarni, M. A. Khan, R. M. Noor and Z. Trabelsi, "A Novel Multifaceted Trust Management Framework for Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 11, pp. 20084-20097, Nov. 2022, doi: 10.1109/TITS.2022.3187788.

[9] J. Du, G. Han, C. Lin and M. Martínez-García, "LTrust: An Adaptive Trust Model Based on LSTM for Underwater Acoustic Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 21, no. 9, pp. 7314-7328, Sept. 2022, doi: 10.1109/TWC.2022.3157621.

[10] J. Du, G. Han, C. Lin and M. Martínez-García, "LTrust: An Adaptive Trust Model Based on LSTM for Underwater Acoustic Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 21, no. 9, pp. 7314-7328, Sept. 2022, doi: 10.1109/TWC.2022.3157621.

[11] S. Huang, Z. Zeng, K. Ota, M. Dong, T. Wang and N. N. Xiong, "An Intelligent Collaboration Trust Interconnections System for Mobile Information Control in Ubiquitous

5G Networks," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 1, pp. 347-365, 1 Jan.-March 2021, doi: 10.1109/TNSE.2020.3038454.

[12] Y. Zhao et al., "Entity and Sociality Trust-Aware Model for Content Distribution in Social Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 71, no. 12, pp. 12511-12522, Dec. 2022, doi: 10.1109/TVT.2022.3196671.

[13] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati and D. Simeonidou, "Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks," in Journal of Lightwave Technology, vol. 40, no. 17, pp. 5816-5824, 1 Sept.1, 2022, doi: 10.1109/JLT.2022.3183962.

[14] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati and D. Simeonidou, "Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks," in Journal of Lightwave Technology, vol. 40, no. 17, pp. 5816-5824, 1 Sept.1, 2022, doi: 10.1109/JLT.2022.3183962.

[15] Pragati Narayan Patil, Dr. A. D. Raut, “Study and Analysis of Energy and Time Characteristics of Node in Wireless Sensor Network”, NeuroQuantology , Volume 20, No 9 (2022), DOI: 10.14704/nq.2022.20.9.NQ44213

[16] A. Kumar, K. Singh, T. Khan, A. Ahmadian, M. H. M. Saad and M. Manjul, "ETAS: An Efficient Trust Assessment Scheme for BANs," in IEEE Access, vol. 9, pp. 83214-83233, 2021, doi: 10.1109/ACCESS.2021.3086534.

[17] A. Kumar, K. Singh, T. Khan, A. Ahmadian, M. H. M. Saad and M. Manjul, "ETAS: An Efficient Trust Assessment Scheme for BANs," in IEEE Access, vol. 9, pp. 83214-83233, 2021, doi: 10.1109/ACCESS.2021.3086534.

[18] M. Bin-Yahya, O. Alhussein and X. Shen, "Securing Software-Defined WSNs Communication via Trust Management," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22230-22245, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3102578.

[19] S. -M. Yu, Z. -J. Du, X. -Y. Zhang, H. -Y. Luo and X. -D. Lin, "Trust Cop-Kmeans Clustering Analysis and Minimum-Cost Consensus Model Considering Voluntary Trust Loss in Social Network Large-Scale Decision-Making," in IEEE Transactions on Fuzzy Systems, vol. 30, no. 7, pp. 2634-2648, July 2022, doi: 10.1109/TFUZZ.2021.3089745.

[20] D. Zhang, F. R. Yu, R. Yang and L. Zhu, "Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2, pp. 1400-1414, Feb. 2022, doi: 10.1109/TITS.2020.3025684.

[21] Y. Zhao and G. Srivastava, "A Wireless Mesh Opportunistic Network Routing Algorithm Based on Trust Relationships," in IEEE Access, vol. 10, pp. 4786-4793, 2022, doi: 10.1109/ACCESS.2021.3138370.

[22] H. Huang, J. Zhang, J. Hu, Y. Fu and C. Qin, "Research on Distributed Dynamic Trusted Access Control Based on Security Subsystem," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 3306-3320, 2022, doi: 10.1109/TIFS.2022.3206423.

[23] J. Wu, S. Wang, F. Chiclana and E. Herrera-Viedma, "Two-Fold Personalized Feedback Mechanism for Social Network Consensus by Uninorm Interval Trust Propagation," in IEEE Transactions on Cybernetics, vol. 52, no. 10, pp. 11081-11092, Oct. 2022, doi: 10.1109/TCYB.2021.3076420.

[24] B. Pang, Z. Teng, H. Sun, C. Du, M. Li and W. Zhu, "A Malicious Node Detection Strategy Based on Fuzzy Trust Model and the ABC Algorithm in Wireless Sensor Network," in IEEE Wireless Communications Letters, vol. 10, no. 8, pp. 1613-1617, Aug. 2021, doi: 10.1109/LWC.2021.3070630.

[25] Z. Liu et al., "PPTM: A Privacy-Preserving Trust Management Scheme for Emergency Message Dissemination in Space–Air–Ground-Integrated Vehicular Networks," in IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5943-5956, 15 April15, 2022, doi: 10.1109/JIOT.2021.3060751.

[26] Z. Zhai et al., "Lightweight Secure Detection Service for Malicious Attacks in WSN With Timestamp-Based MAC," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 5299-5311, Dec. 2022, doi: 10.1109/TNSM.2022.3194205.

[27] H. Gao, C. Liu, Y. Yin, Y. Xu and Y. Li, "A Hybrid Approach to Trust Node Assessment and Management for VANETs Cooperative Data Communication: Historical Interaction Perspective," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 16504-16513, Sept. 2022, doi: 10.1109/TITS.2021.3129458.

[28] A. Rehman et al., "CTMF: Context-Aware Trust Management Framework for Internet of Vehicles," in IEEE Access, vol. 10, pp. 73685-73701, 2022, doi: 10.1109/ACCESS.2022.3189349.

[29] S. Liu, X. Hu, S. -H. Wang, Y. -D. Zhang, X. Fang and C. Jiang, "Mixing Patterns in Social Trust Networks: A Social Identity Theory Perspective," in IEEE Transactions on Computational Social Systems, vol. 8, no. 5, pp. 1249-1261, Oct. 2021, doi: 10.1109/TCSS.2020.3021179.

[30] J. Jiang, S. Hua, G. Han, A. Li and C. Lin, "Controversy-Adjudication-Based Trust Management Mechanism in the Internet of Underwater Things," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2603-2614, 1 Feb.1, 2023, doi: 10.1109/JIOT.2022.3215635.

[31] B. Li, R. Liang, W. Zhou, H. Yin, H. Gao and K. Cai, "LBS Meets Blockchain: An Efficient Method With Security Preserving Trust in SAGIN," in IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5932-5942, 15 April15, 2022, doi: 10.1109/JIOT.2021.3064357.

[32] W. Ma, X. Wang, M. Hu and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," in IEEE Access, vol. 9, pp. 65066-65077, 2021, doi: 10.1109/ACCESS.2021.3076118.

[33] P. Nie et al., "Sparse Trust Data Mining," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4559-4573, 2021, doi: 10.1109/TIFS.2021.3109412.

[34] Pragati Patil Bedekar, Atul Raut & Abhimanyu Dutonde , “Energy Conserving Techniques of Data Mining for Wireless Sensor Networks—A Review”, Springer IoT and Analytics for Sensor Networks pp 433–443.

[35] Pragati Narayan Patil, Dr. A. D. Raut, “BLMCE: Design of A Dual-Bioinspired Low-Complexity Data Mining Engine For Automatic Cluster Analysis Via Ensemble Learning Operations”, Webology (ISSN: 1735-188X) Volume 18, Number 5, 2021, Pg. No. 4339-4360.