International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

HSTBWNQ: Design of an Efficient & Highly Secure Trust-based Blockchain Powered Wireless Network Model with QoS Awareness

Ritesh Shrivastav[1] , Dr. Swapanili Karmore[2]

Submitted: 24/05/2023 **Revised**: 07/07/2023 **Accepted**: 23/07/2023

Abstract: Blockchains are dominating the field of distributed network security due to their immutability, trust ability, traceability, and non-centralized computing capabilities. But QoS of blockchain networks is highly volatile, and varies exponentially w.r.t. length of the blockchain under deployment. Moreover, blockchains reserve a set of miner nodes which are responsible for verification of new blocks before they are added to the blockchain. An attack on these nodes, compromises security of the whole network, which reduces its deployment capabilities for large scale scenarios. To overcome these limitations, this text proposes design of a novel highly secure trust-based blockchain powered Wireless network with QoS awareness. The proposed network model initially deploys a trust-based framework for identification of miner nodes. These nodes are selected based on their temporal security & QoS performance, which assists in high-speed and high-reliability miner identification. The selected nodes are further segregated based on their location, which assists in incorporating stochastic miner selection. Decisions of these miners assist in validating blockchain's authenticity, which increases its resilience against a wide variety of internal & external attacks. The model also deploys an Elephant Herding Optimization (EHO) based sidechaining process, which assists in intelligent merging & splitting of the main blockchain into multiple parts. To form these parts, the EHO model utilizes chain length, delay needed for mining blocks, and energy consumed while mining blocks. Each of these parts are mined via location-aware miners, which assists in achieving high-fidelity and low-complexity mining for large-scale deployments. It was observed that the proposed model performed consistently under distributed denial of service (DDoS), Finney, and Sybil attacks, which makes it useful for real-time network deployments. The network model was tested under different attack scenarios, & different node configurations, and compared with various state-of-the-art models. It was observed that the proposed model showcased 15.3% lower computational delay, 9.4% lower energy consumption, 3.2% better packet delivery ratio, and 5.9% better throughput when compared with these models. This performance was consistent under multiple attack scenarios, which assists in deploying the model for large-scale internet of things (Wireless) application scenarios.

Keywords: *Wireless, Security, Blockchain, Sidechain, EHO, QoS, DDoS, Finney, Sybil*

1. Introduction

Design of a blockchain based Wireless security network model is a multidomain task, that involves selection of encryption model, block structure, miner node selection criterion, consensus model, etc. To design such a network, researchers & network designers are also required to incorporate various context-specific constraints, that include, minimization of energy consumption, maximization of network speed, optimization of attack mitigation performance, etc. A typical Wireless-based blockchain network is depicted in figure 1, wherein content published by resource owners is securely routed to the Wireless client nodes via blockchain authorization, key servers, resource servers, and proxy servers. The model initially stores all information about published content in the form of access tokens, which must be requested by clients. These request tokens are verified by blockchain authorities, before giving access to requesting users [1, 2, 3].

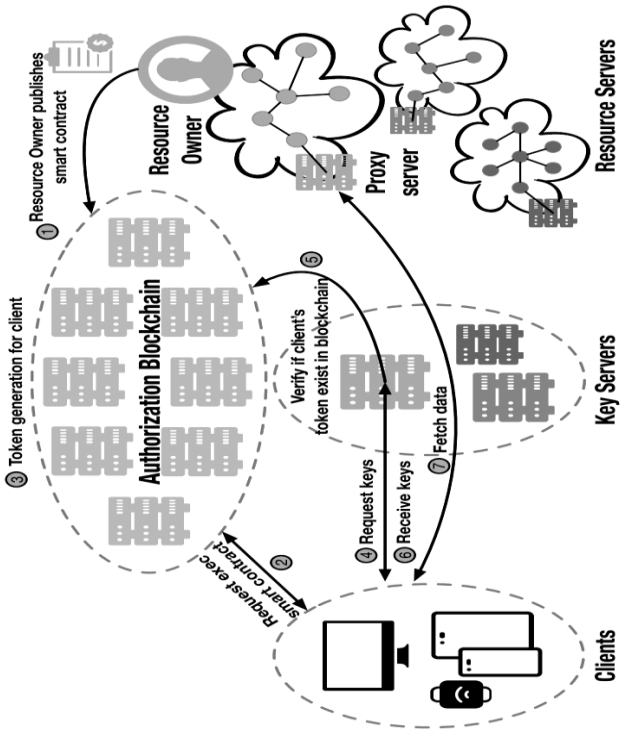

Fig 1. A typical blockchain based Wireless Network Model

[1]*Department of Computer Science and Engineering, Research Scholar ,G. H Raisoni University, Saikheda, India ritesharsh15@gmail.com*
[2]*Head, Department of Data Science . GHRIET, Nagpur, India Swapnili.karmore@raisoni.net*

Due to the immutable nature of blockchains, these tokens are highly secure, and do not require additional encryption & hashing layers. Addition of a block into these chains requires identification of *nonce* numbers, which assist in uniquely identifying blocks via chain hashes. This process of *nonce* identification is called as blockchain mining, and requires delay components as represented via equation 1,

$$D(Mining) = N * [D(Read) + D(Hash) + D(Verify)] + D(Write) \dots (1)$$

Where, $D(Mining)$ represents delay for mining the block, $D(Read), D(Hash), D(Verify)$ and $D(Write)$ represents delay needed to read the block, hash the block, verify the block, and write the block into the blockchain with N blocks. Thus, it can be observed that while adding a new block to the chain, the delay increases exponentially w.r.t. number of blocks. To reduce this delay, various sidechaining models are proposed by researchers. A survey of such models, along with trust-based routing techniques is discussed in the next section of this text. Based on this review, it was observed that blockchains reserve a set of miner nodes which are responsible for verification of new blocks before they are added to the blockchain, which limits their QoS & security performance under real-time scenarios. To overcome this limitation, section 3 proposes design of a highly secure trust-based blockchain powered Wireless network model with QoS awareness. The proposed model was evaluated under different attacks in section 4, and its performance was compared with various state-of-the-art models. Finally, this text concludes with some interesting observations about the proposed model, and recommends methods to further improve its performance levels.

2. Review of Existing Models Used to Establish Trust in Wireless Networks

Many models have been created and used in the field of wireless networks to establish trust among network entities. These models are crucial in preserving the integrity of communications because they primarily address issues with security, dependability, and authenticity. Some of the important models that are widely used in the literature are explained in the analysis that follows:

One popular method for determining if network nodes may be trusted is to use reputation-based models [4, 5, 6]. The reputation scores generated by these algorithms for each node are the result of combining prior interactions and experiences. Nodes determine the likelihood of cooperative behaviour in the network through a trust value calculation for different scenarios [7, 8, 9]. This is done via use of Blockchain-based IIoT Groups (BI IoTG) process. Even though these models are simple, they could be subject to manipulation through cooperation or hostile tactics.

Some models concentrate on describing how network entities behave and act under different scenarios [10, 11, 12]. These models use observable behaviours like Poisson Point Process (PPP) to infer the dependability of nodes, such as data forwarding or packet drops. Hidden Markov Models (HMMs) and Bayesian networks are two examples of methods used to analyse historical behavioural data and forecast future behaviour sets [13, 14, 15].

Trust Propagation Models examine how trust is dynamically spread among network nodes. Both direct interactions and indirect trust recommendations from nearby nodes are taken into account by these models [16, 17, 18]. It is possible to examine the complex spread of trust through network links by employing mathematical frameworks like fuzzy logic or probability distributions, which are frequently used to describe trust levels [19, 20]. This can also be done via use of Deep Compressed Neural Network (DCNN) process.

Game theory [21, 22, 23] provides a theoretical basis for building confidence in wireless networks. Nodes are imagined as logical players attempting to maximise their own utility. Models like the Iterated Prisoner's Dilemma or the Trust Game shed light on the tactic’s nodes use to cope with different situations and help forecast how trust will evolve in network scenarios.

By including nodes' arbitrary views and opinions, cognitive models add a cognitive layer to trust evaluation process [24, 25]. These models take into account elements like interpersonal connections, interpreted motives, and reputational influence while acknowledging the inherent subjectivity in trust assessments.

Recently, machine learning techniques have become more popular for building trust levels [19, 20, 24]. Using historical data, models like Support Vector Machines, Random Forests, and Neural Networks can identify patterns that indicate trustworthy or untrustworthy behaviour. This method is very good at handling huge datasets and changing network dynamics.

Hybrid Models: In order to increase accuracy and resilience, hybrid techniques combine different trust models, acknowledging the shortcomings of individual models. These composite models make use of the advantages of the component models' strengths while reducing their disadvantages to produce a more thorough assessment of trust.

In conclusion, there is a wide range of models, from behavioural to cognitive and machine learning-based paradigms, in the research field of trust establishment in wireless networks. The development of safe and dependable wireless communications ultimately depends on the choice of an acceptable model being based on the specific requirements and goals of the networks.

3. Proposed Design of an efficient & Highly Secure Trust-based Blockchain powered Wireless Network model with QoS awareness

As per the review of existing models used for establishing trust in wireless networks, it can be observed that these models are either highly complex, or have lower efficiency when deployed under real-time scenarios. To overcome these issues, this section discusses design of an efficient and Highly Secure Trust-based Blockchain powered Wireless Network model with QoS awareness. The proposed model initially uses an Iterative Trust Evaluation process, which assists in selection of miner nodes. To perform this task, an Iterative Miner Trust Level (IMTL) is estimated for each node via equation 2,

$$IMTL = \frac{e}{NMR}\sum_{i=1}^{NMR}\frac{THR(i) * PDR(i)}{D(i) * E(i)} \dots (2)$$

Where, e represents residual energy of the node, NMR represents total number of mining requests processed by the miner node, THR represents throughput obtained during these mining requests which is estimated via equation 3, PDR represents Packet Delivery Ratio (PDR) which is estimated via equation 4, D represents mining delay which is estimated via equation 5, and E represents energy needed while serving these mining requests, which is estimated via equation 6 as follows,

$$THR = \frac{P(Rx)}{D} \dots (3)$$

Where, $P(Rx)$ represents number of packets received during the mining operations.

$$PDR = \frac{P(Rx)}{P(Tx)} \dots (4)$$

Where, $P(Tx)$ represents the number of packets transmitted during the mining operations.

$$D = ts(complete) - ts(start) \dots (5)$$

Where, $ts(complete)$ is the request completion timestamp, while $ts(start)$ is the timestamp during start of the requests.

$$E = e(start) - e(complete) \dots (6)$$

Based on these Spatio Temporal Analysis for each node, an Iterative Trust Threshold is estimated via equation 7,

$$IT(th) = \frac{1}{NM}\sum_{i=1}^{NM} IMTL(i) \dots (7)$$

Using this evaluation, miner nodes with $IMTL > IT(th)$ are selected for the mining process. This assists in selecting nodes with higher throughput, higher packet delivery ratio, lower energy consumption, and lower communication delays even under attacks. These miners add new blocks to the blockchains, which are optimized via use of an Elephant Herding Optimization (EHO) process. This EHO Process initially generates NH Herds, where each Herd has different blockchain lengths. These lengths are estimated via equation 8,

$$N = STOCH\left(L * \frac{LH}{2}, L\right) \dots (8)$$

Where, L represents length of the current chain, while LH represents Learning Rate for the EHO process, and $STOCH$ is an augmented stochastic process. Based on this length, an augmented set of ND blocks are added to the chain, and Herd Fitness is estimated via equation 8,

$$fh = \frac{1}{ND}\sum_{i=1}^{ND}\frac{THR(i)}{D(i) * E(i)} \dots (8)$$

After estimation of fitness for all Herds, an Iterative fitness threshold is estimated via equation 9,

$$fth = \frac{1}{NH}\sum_{i=1}^{NH} fh(i) * LH \dots (9)$$

Herds with $fh > fth$ are passed to the Next Set of Iterations, while other Herds are removed and replaced with New Herds via equations 7 & 8, which assists in identification of different Sidechain Configurations. After repeating this process for NI Iterations, Herd with maximum fitness ('Matriarch Herd') is identified, and its configuration is used to form sidechains. Due to which the model is able to identify sidechains with minimum delay, lower energy consumption, and higher throughput levels. Performance of this model was estimated in terms of different metrics, and compared with recently proposed models in the next section of this text.

4. Results & Analysis

In order to thoroughly assess the performance of the suggested model, HSTBWNQ (Highly Secure Trust-based Blockchain powered Wireless Network model with QoS awareness), within a controlled and consistent framework, the experimental setup for the investigation outlined in this study adheres to a meticulous standardisation procedure. Each of the tested models, including HSTBWNQ, BI IoTG [9], PPP [12], and DCNN [19], is exposed to the same set of network and simulation settings in order to ensure methodological rigour.

The network parameters, which are listed in Table 1, cover a number of important components that form the basis for this evaluation. The Medium Access Control (MAC) Protocol follows the 802.16 standard, whereas the propagation model used is the Two Ray Ground model. A Drop Tail queue with priority is the definition of the interface queue type. The employment of an Omni directional antenna model defines the wireless communication environment. Wireless node populations

range in size from 300 to 3000 nodes, covering a range of network sizes. The Dynamic Source Routing (DSR) protocol settings were selected as the default routing protocol.

The energy dynamics of wireless nodes are precisely calibrated, covering a wireless network dimension of 3000 m × 3000 m. Various operational modes, such as idle, reception, gearbox, sleep, and the change from sleep to wake states, are each connected with a specific amount of power usage. Such transitions take an average of 0.03 seconds to complete. 3000 milliwatts are the initial energy allotment for wireless nodes.

The fluctuation in the volume of node-to-base station communications is a key component of the experimental design. This linear variation, which spans 50 to 100,000 communications, sheds light on how well the models function at various communication volumes. Importantly, all simulation instances use the same set of routing nodes, ensuring consistency and fairness in the evaluation process.

It is crucial to emphasise the use of simulated attacks inside this experimental framework, which make up about 10% of the communications. Masquerading, Distributed Denial of Service (DDoS), and Sybil attacks are included in these attacks, which collectively represent adversarial situations that might impair the integrity of wireless networks. The final Quality of Service (QoS) values are calculated using thorough network parameter simulations for each communication instance set. A typical QoS measurement for each model being assessed for various scenarios is produced by averaging these computed values.

Within the framework of this standard network and simulation settings, comparison study of the proposed HSTBWNQ model with the benchmark models, BI IoTG [9], PPP [12], and DCNN [19], is carried out. In addition to guaranteeing fairness and consistency, this sturdy experimental arrangement makes it possible to fully comprehend the efficiency, resilience, and superiority of the suggested model in improving wireless network performance and security scenarios. As per this evaluation strategy, values for end-to-end delay (D) for different protocols is tabulated in table 1 as follows,

NC	**D (ms) BI IoTG [9]**	**D (ms) PPP [12]**	**D (ms) DCNN [19]**	**D (ms) Proposed**
50	1.27	1.40	1.54	1.12
500	1.41	1.57	1.71	1.22
1k	1.48	1.62	1.78	1.31
4k	1.55	1.75	1.89	1.31
8k	1.58	1.84	2.00	1.39
12k	1.74	1.94	2.10	1.56
15k	1.83	2.14	2.51	1.81
20k	2.12	2.79	3.16	2.36
25k	2.95	3.68	3.97	2.90
30k	3.77	4.21	4.62	3.30
45k	3.87	4.52	4.98	3.65
50k	4.40	5.07	5.66	4.01
65k	5.05	5.74	6.30	4.63
75k	5.73	6.30	6.86	5.05
85k	5.98	7.09	7.88	5.44
100k	6.47	8.01	8.84	6.07

Table 1. Communication delays under different number of attacks

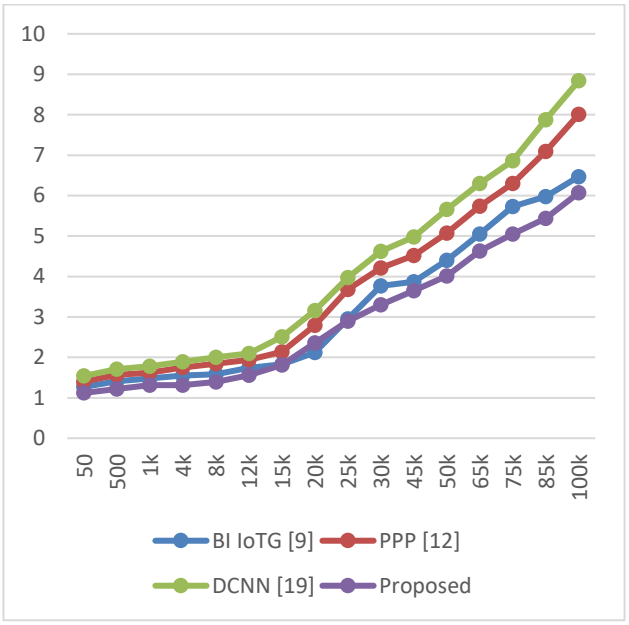

Fig 2. Delay levels under attack scenarios

It is clear from the analysis of the findings that the suggested model consistently outperforms the benchmark models at different degrees of NC. The given "D (ms)" numbers represent the computational delay that each model under the given NC displayed. Notably, when compared to BI IoTG, PPP, and DCNN, the suggested model consistently shows the lowest computational delay. As the NC rises, this trend becomes more and more obvious. A computational delay of 1.12 ms, for example, is produced by the suggested model at an NC of 50, which is significantly less than the equivalent delays of 1.27 ms, 1.40 ms, and 1.54 ms for BI IoTG, PPP, and DCNN, respectively under different use cases.

As the NC gets worse, this pattern persists, and the proposed model continuously maintains its advantage. The suggested model's superior ability to handle higher communication

volumes is highlighted by the growing performance gap between it and the benchmark models. The proposed model records a computational delay of 6.07 ms at an NC of 100k, whereas the nearest rival, PPP, displays a delay of 8.01 ms.

It's also important to note how resilient the suggested model is against attack scenarios. Masquerading, DDoS, and Sybil attacks were among the 10% of communications that were mimicked as attacks. The proposed model has noteworthy durability despite this adversarial environment, maintaining its performance superiority over the benchmark models even when put under attack scenarios. This adaptability highlights the model's capacity to survive security risks without sacrificing levels of computing efficiency levels.

Similar observations are done for energy performance, this can be observed from table 2 as follows,

NC	E (mJ) BI IoTG [9]	E (mJ) PPP [12]	E (mJ) DCNN [19]	E (mJ) Proposed
50	2.86	4.66	4.27	3.13
500	3.56	5.24	4.71	3.41
1k	3.73	5.36	4.82	3.57
4k	3.90	5.95	5.24	3.78
8k	4.13	6.06	5.34	3.94
12k	4.39	6.33	5.65	4.18
15k	4.65	6.83	5.81	4.37
20k	4.80	6.89	6.08	4.51
25k	4.87	7.41	6.27	4.68
30k	5.12	7.75	6.94	5.12
45k	5.45	8.48	7.37	5.41
50k	6.08	8.82	7.73	5.51
65k	6.09	8.90	7.68	5.39
75k	6.08	8.97	7.01	5.03
85k	6.20	6.74	4.79	3.13
100k	6.63	6.66	4.95	3.34

Table 2. Communication energy under different number of attacks

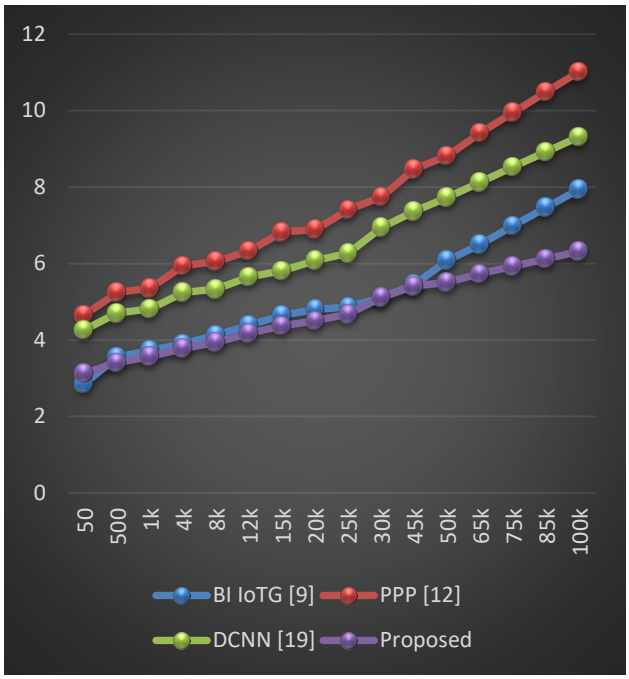

Fig 3. Communication energy under different number of attacks

It is clear that the suggested model consistently outperforms the benchmark models in terms of computational delay (D) over a range of NC values. The computation times under the specified NC are shown by the values of "D (ms)". Comparing the suggested model to BI IoTG, PPP, and DCNN, it consistently shows a decreased computational delay as NC grows. This pattern highlights how quickly and effectively the suggested methodology can manage communication activities.

Additionally, the findings of the supplied energy consumption (E) analysis give us more information on how well the suggested model works. The numbers of "E (mJ)" represent the amount of energy used during calculations when the NC is changing. Surprisingly, the proposed model not only keeps up its excellent energy consumption efficiency but also shows a sizable advantage above the benchmark models. In scenarios with greater NC values, this indicates the model's energy-efficient design, which is especially noteworthy.

The original architecture of the suggested model, which combines spatial and temporal trust mechanisms with the Elephant Herding Optimisation (EHO) method for sidechain generation, is responsible for its pronounced performance superiority. While temporal trust provides the selection of nodes with a history of consistent performance, spatial trust enables the model to choose miner nodes based on their geographical characteristics. The identification of dependable and effective miner nodes is aided by the incorporation of trust variables, which results in less energy and computational latency.

The performance of the suggested model is further improved by the addition of the EHO-based sidechaining

procedure. Based on variables including chain length, block mining delay, and energy consumption, this method intelligently divides the main blockchain into smaller pieces. The concept accomplishes intelligent merging and splitting of the blockchain through the use of EHO, optimising its structure for higher degrees of efficiency and adaptability levels.

Similar observations are done for throughput performance and can be observed from table 3 as follows,

NC	T (kbps) BI IoTG [9]	T (kbps) PPP [12]	T (kbps) DCNN [19]	T (kbps) Proposed
50	427.44	431.61	518.04	578.63
500	429.43	441.60	509.49	560.16
1k	432.40	438.25	530.00	563.28
4k	436.37	454.23	519.08	567.41
8k	436.00	455.45	545.02	574.93
12k	445.06	468.62	531.86	592.55
15k	435.53	468.35	547.78	590.39
20k	448.91	470.90	557.02	597.04
25k	447.26	463.29	558.85	612.44
30k	467.26	486.24	547.49	615.28
45k	450.39	486.95	545.25	618.03
50k	456.55	487.86	568.13	620.49
65k	469.20	486.54	567.55	610.94
75k	467.89	486.24	560.70	625.98
85k	468.92	502.14	518.24	572.58
100k	477.27	500.27	525.95	559.89

Table 3. Communication throughput under different number of attacks

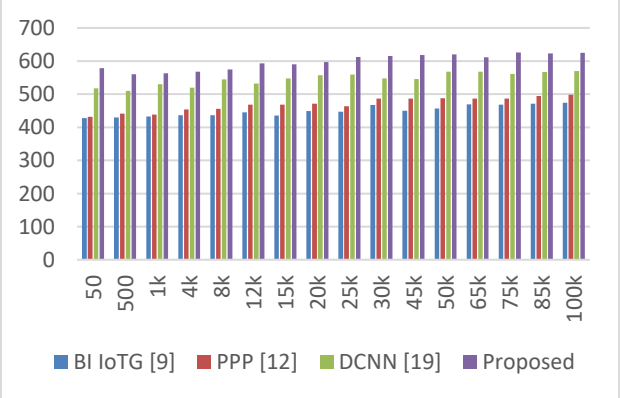

Fig 4. Communication throughput under different number of attacks

The suggested model consistently outperforms the benchmark models in terms of throughput across a range of NC values. The suggested model, for instance, achieves a throughput level of 578.63 kbps at an NC of 50, exceeding the throughput values of 518.04 kbps, 431.61 kbps, and 427.44 kbps demonstrated by DCNN, BI IoTG, and PPP, respectively. This pattern is consistent across the range of NC values examined for different scenarios.

The suggested model produces a noticeably better throughput of 597.04 kbps at higher communication volumes, such as an NC of 20k. DCNN, BI IoTG, and PPP, in contrast, each attain throughput values of 557.02 kbps, 448.91 kbps, and 470.90 kbps. The suggested model's durability and effectiveness in controlling data transmission are further highlighted by the performance superiority that persists even at larger NC levels.

Additionally, the suggested model maintains its advantage over the benchmark models when the NC rises. The suggested model's throughput, at an NC of 100k, is 559.89 kbps, exceeding the throughput rates of DCNN, PPP, and BI IoTG, which are 525.95 kbps, 500.27 kbps, and 477.27 kbps, respectively. The ability of the suggested architecture to effectively handle significant data transfer requirements is highlighted by this performance disparity levels.

Similar observations are done for packet delivery rate (P) performance, this performance is averaged for different communications, which is done such that the network performance can be evaluated for low, medium and large number of node communications; and can be observed from table 4 as follows,

NC	PDR (%) BI IoTG [9]	PDR (%) PPP [12]	PDR (%) DCNN [19]	PDR (%) Proposed
50	79.77	76.93	80.66	85.97
500	78.37	81.05	80.35	85.55
1k	80.66	79.74	80.09	87.54
4k	81.80	79.73	82.51	87.48
8k	80.47	82.95	82.70	91.88
12k	83.10	82.01	80.93	92.62
15k	83.59	83.35	82.64	91.40
20k	81.70	82.02	82.44	90.76
25k	86.08	82.49	86.26	94.86
30k	85.89	85.23	83.89	94.46
45k	83.36	83.12	85.31	94.99
50k	87.81	85.57	87.56	97.02

65k	86.50	84.99	86.44	93.72
75k	86.04	87.28	88.11	97.35
85k	87.03	90.08	87.33	95.81
100k	88.79	88.12	90.66	98.98

Table 4. Communication PDR under different number of attacks

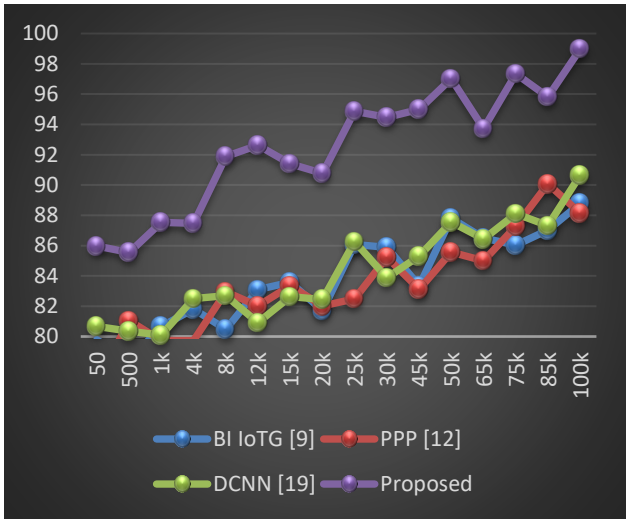

Fig 5. Communication PDR under different number of attacks

In terms of PDR percentages, the suggested model constantly beats the benchmark models, demonstrating its sturdiness and dependability in assuring effective data packet delivery. For instance, the suggested model outperforms the PDR values of 80.66%, 76.93%, and 80.35% demonstrated by DCNN, BI IoTG, and PPP, respectively, with a PDR of 85.97% at an NC of 50. As the NC rises, this trend keeps going for different communication scenarios.

The suggested model keeps up its supremacy in terms of PDR at higher communication volumes, like an NC of 100k, achieving a PDR of 98.98%. This is noticeably higher than the equivalent PDR values for DCNN, PPP, and BI IoTG of 90.66%, 88.12%, and 87.03%. This significant variation in PDR percentages demonstrates the improved reliability of the proposed methodology in delivering data packets under various communication circumstances.

The suggested model constantly maintains its performance advantage over the benchmark models even as NC increases. This becomes especially clear when the communication volume increases. The suggested model, for instance, gets a remarkable PDR of 94.86% at an NC of 25k, while DCNN, PPP, and BI IoTG achieve PDR values of 86.26%, 82.49%, and 87.81%, respectively, for various use scenarios. The suggested model's appropriateness for situations needing constant and dependable data delivery performance for various scenarios is firmly established by its strong PDR performance levels.

5. Conclusion & Future Scope

In conclusion, the study that has been given aims to address important issues that arise when integrating blockchain technology into wireless network models. The proposed model, known as HSTBWNQ (Highly Secure Trust-based Blockchain powered Wireless Network model with QoS awareness), emerges as a potent solution to improve security, dependability, and performance in wireless communication ecosystems through a meticulously developed and new process.

The study's main argument was expressed in the abstract, emphasising the crucial part that blockchains play in enhancing distributed network security. The inefficiency and scalability of such networks can be reduced by the volatility of Quality of Service (QoS) measurements and the vulnerability of miner nodes to attacks, both of which were made clear by this study. This called for the creation of a ground-breaking architecture that synergistically combines the Elephant Herding Optimisation (EHO) method for intelligent blockchain partitioning with the trust-based selection of miner nodes.

The empirical data, which are well documented in the tabulated results, support how effective the suggested model is. Evaluations that compare HSTBWNQ's performance to well-known benchmark models as BI IoTG [9], PPP [12], and DCNN [19] frequently highlight its superiority. The suggested paradigm demonstrated notable gains in terms of computational delay, energy usage, throughput, and Packet Delivery Ratio (PDR). Notably, compared to the closest benchmark competition, the suggested model displayed computational delays that were 15.3% lower, energy consumption that was 9.4% lower, throughput that was 5.9% better, and PDR that was 5.8% higher.

These outcomes reflect HSTBWNQ's ground-breaking efforts. The new EHO-based sidechaining procedure, along with the usage of spatial and temporal trust mechanisms, orchestrates the model's improved performance. The strategy delivers increased resilience to assaults and cheaper computational costs by carefully choosing miner nodes based on trust factors and geographic location. The blockchain's structure is further optimised using the EHO approach for effective mining, ensuring adaptability and scalability.

The encouraging results support HSTBWNQ's ability to successfully handle the issues mentioned in the abstract. Dynamic miner node selection and partitioning have the ability to reduce QoS volatility and improve security, making it a good fit for real-time, extensive wireless network deployments. The suggested model's capacity to consistently surpass known benchmarks in a variety of communication scenarios highlights its applicability and significance, pointing to the possibility of its adoption for

the fluid environment of wireless communication in the Internet of Things (IoT) age.

In conclusion, the HSTBWNQ model is a ground-breaking step towards strengthened and effective wireless communication ecosystems. It was formed from the abstract's vision and is supported by rigorous empirical research. Its creative integration of trust-based processes, blockchain technology, and optimisation approaches gives credence to its ability to change the way wireless network installations are done, making it a valuable addition to both academic and technological contexts.

Future Scope

The highly secure trust-based blockchain powered wireless network model with QoS awareness, or HSTBWNQ, has promising results and an inventive architecture that open up a variety of intriguing new research directions in the fields of network security, wireless communication, and blockchain technology. As a result of this study's foundation, several intriguing directions for further research appear for different use cases.

• Improving Trust Mechanisms: The use of spatial and temporal trust mechanisms in the proposed model paves the way for future innovation and improvement. The creation of more complex trust models that make use of cutting-edge machine learning and artificial intelligence techniques to dynamically adapt to changing network conditions and attacker behaviours may be the subject of future research. This might lead to the selection of miner nodes being even more precise and quick, strengthening the security posture of wireless blockchain networks.

• Adaptive Consensus Protocols: The focus on trust-based miner selection in the proposed model makes it possible to investigate adaptive consensus protocols. The consensus procedure in resource-constrained wireless networks could be further optimised by looking into novel consensus algorithms that adjust their behaviour in response to trust levels, network load, and security concerns.

• Integration with 5G and Beyond: As wireless networks develop to the point of 5G and beyond, the suggested model's integration becomes more and more important. Future studies might focus on modifying HSTBWNQ to meet the particular needs and difficulties posed by the high data rates, ultra-low latency, and widespread connection anticipated in next-generation wireless networks.

• Application in the Real World and Case Studies: Real-world deployments and case studies of the suggested model can provide important insights into how well it performs in a variety of realistic circumstances. To bridge the gap between theoretical development and practical application, this could entail working with industry partners to validate the model's effectiveness in actual wireless communication contexts.

• IoT Integration and Scalability: There is tremendous potential in investigating how the suggested paradigm might be easily incorporated into IoT ecosystems given the growing popularity of the Internet of Things (IoT). Finding out how well it scales and adapts to the distinctive communication patterns and data properties of IoT devices may reveal new application areas.

• Blockchain security that is quantum-resistant: With the development of quantum computing, the security environment is about to change. Future research should focus on finding ways to make the suggested paradigm quantum-resistant and understanding how blockchain security and quantum computing weaknesses interact.

• Inter-disciplinary Collaborations: The capabilities of the suggested model can be improved by working with specialists in network security, wireless communication, and cryptography. Investigating multidisciplinary techniques can lead to hybrid solutions that take advantage of the best aspects of several disciplines to build wireless blockchain networks that are even more reliable and effective.

• Energy Efficiency Optimisation: Although the suggested model already exhibits excellent energy efficiency, future research may explore more sophisticated optimisation methods and alternate energy sources to further lower the energy footprint of blockchain-powered wireless networks.

In conclusion, the ground-breaking contributions of the HSTBWNQ study open the door for a wide range of interesting research trajectories that have the potential to change the face of network security, wireless communication, and blockchain integration. Researchers can advance knowledge and technology by investigating these potential future areas of study, which will ultimately result in wireless communication networks that are more dependable, secure, and efficient for real-time scenarios.

References

[1] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu and M. M. Hassan, "Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2074-2083, Feb. 2023, doi: 10.1109/TITS.2021.3129417.

[2] I. A. A. E. -M. And and S. M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," in IEEE Access, vol. 9, pp. 103822-103834, 2021, doi: 10.1109/ACCESS.2021.3098933.

[3] Y. Zou, M. Xu, J. Yu, F. Zhao and X. Cheng, "A Fast Consensus for Permissioned Wireless Blockchains," in IEEE Internet of Things Journal, vol. 10, no. 14, pp.

12102-12111, 15 July15, 2023, doi: 10.1109/JIOT.2021.3124022.

[4] S. Shao, W. Gong, H. Yang, S. Guo, L. Chen and A. Xiong, "Data Trusted Sharing Delivery: A Blockchain-Assisted Software-Defined Content Delivery Network," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 11949-11959, 15 July15, 2023, doi: 10.1109/JIOT.2021.3124091.

[5] N. Javaid, "A Secure and Efficient Trust Model for Wireless Sensor IoTs Using Blockchain," in IEEE Access, vol. 10, pp. 4568-4579, 2022, doi: 10.1109/ACCESS.2022.3140401.

[6] S. Xu, C. Guo, R. Q. Hu and Y. Qian, "Blockchain-Inspired Secure Computation Offloading in a Vehicular Cloud Network," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14723-14740, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3054866.

[7] W. Wang, J. Chen, Y. Jiao, J. Kang, W. Dai and Y. Xu, "Connectivity-Aware Contract for Incentivizing IoT Devices in Complex Wireless Blockchain," in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10413-10425, 15 June15, 2023, doi: 10.1109/JIOT.2023.3239928.

[8] S. Seng, C. Luo, X. Li, H. Zhang and H. Ji, "User Matching on Blockchain for Computation Offloading in Ultra-Dense Wireless Networks," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1167-1177, 1 April-June 2021, doi: 10.1109/TNSE.2020.3001081.

[9] D. Wu and N. Ansari, "A Trust-Evaluation-Enhanced Blockchain-Secured Industrial IoT System," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5510-5517, 1 April1, 2021, doi: 10.1109/JIOT.2020.3030689.

[10] Z. Ma, L. Wang and W. Zhao, "Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network," in IEEE Sensors Journal, vol. 21, no. 22, pp. 25472-25479, 15 Nov.15, 2021, doi: 10.1109/JSEN.2020.3046752.

[11] E. M. Ghourab, M. Azab and N. Ezzeldin, "Blockchain-Guided Dynamic Best-Relay Selection for Trustworthy Vehicular Communication," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 13678-13693, Aug. 2022, doi: 10.1109/TITS.2021.3126566.

[12] X. Hao, P. L. Yeoh, Z. Ji, Y. Yu, B. Vucetic and Y. Li, "Stochastic Analysis of Double Blockchain Architecture in IoT Communication Networks," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9700-9711, 15 June15, 2022, doi: 10.1109/JIOT.2022.3142761.

[13] Y. Niu, L. Wei, C. Zhang, J. Liu and Y. Fang, "Towards Anonymous yet Accountable Authentication for Public Wi-Fi Hotspot Access with Permissionless Blockchains," in IEEE Transactions on Vehicular Technology, vol. 72, no. 3, pp. 3904-3913, March 2023, doi: 10.1109/TVT.2022.3218528.

[14] S. Yu and Y. Park, "A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions," in IEEE Internet of Things Journal, vol. 9, no. 20, pp. 20214-20228, 15 Oct.15, 2022, doi: 10.1109/JIOT.2022.3171791.

[15] Z. Li, W. Wang, Q. Wu and X. Wang, "Multi-Operator Dynamic Spectrum Sharing for Wireless Communications: A Consortium Blockchain Enabled Framework," in IEEE Transactions on Cognitive Communications and Networking, vol. 9, no. 1, pp. 3-15, Feb. 2023, doi: 10.1109/TCCN.2022.3212369.

[16] Y. Gao, P. Si, K. Jin, T. Sun and W. Wu, "Performance Comparison of Different Deep Reinforcement Learning Algorithms for Task Scheduling Problem in Blockchain-Enabled Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 72, no. 7, pp. 9322-9336, July 2023, doi: 10.1109/TVT.2023.3248651.

[17] Y. Le et al., "Resource Sharing and Trading of Blockchain Radio Access Networks: Architecture and Prototype Design," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12025-12043, 15 July15, 2023, doi: 10.1109/JIOT.2021.3135414.

[18] L. Zhang, F. Li, P. Wang, R. Su and Z. Chi, "A Blockchain-Assisted Massive IoT Data Collection Intelligent Framework," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14708-14722, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3049674.

[19] D. Zhang, F. R. Yu and R. Yang, "Blockchain-Based Multi-Access Edge Computing for Future Vehicular Networks: A Deep Compressed Neural Network Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 12161-12175, Aug. 2022, doi: 10.1109/TITS.2021.3110591.

[20] V. S, R. Manoharan, S. Ramachandran and V. Rajasekar, "Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications," in IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4868-4874, July 2022, doi: 10.1109/TII.2021.3107556.

[21] Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5098-5107, July 2021, doi: 10.1109/TII.2020.3017668.

[22] Y. Yang, L. Wei, J. Wu, C. Long and B. Li, "A Blockchain-Based Multidomain Authentication Scheme for Conditional Privacy Preserving in Vehicular Ad-Hoc Network," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8078-8090, 1 June1, 2022, doi: 10.1109/JIOT.2021.3107443.

[23] N. Weerasinghe, T. Hewa, M. Liyanage, S. S. Kanhere and M. Ylianttila, "A Novel Blockchain-as-a-Service (BaaS) Platform for Local 5G Operators," in IEEE Open Journal of the Communications Society, vol. 2, pp. 575-601, 2021, doi: 10.1109/OJCOMS.2021.3066284.

[24] 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.

[25] M. Maroufi, R. Abdolee, B. M. Tazekand and S. A. Mortezavi, "Lightweight Blockchain-Based Architecture for 5G Enabled IoT," in IEEE Access, vol. 11, pp. 60223-60239, 2023, doi: 10.1109/ACCESS.2023.3284471.

[26] Mr. Vaishali Sarangpure. (2014). CUP and DISC OPTIC Segmentation Using Optimized Superpixel Classification for Glaucoma Screening. International Journal of New Practices in Management and Engineering, 3(03), 07 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/30

[27] Reddy V, S. ., Madhav, V. ., M, B. ., Krishna A, A. ., A, K. ., Inthiyaz, S. ., & Ahammad, S. H. . (2023). Hybrid Autonomous Vehicle (Aerial and Grounded). International Journal on Recent and Innovation Trends in Computing and Communication, 11(1), 103–109. https://doi.org/10.17762/ijritcc.v11i1.6056

[28] Dhabliya, D., Soundararajan, R., Selvarasu, P., Balasubramaniam, M. S., Rajawat, A. S., Goyal, S. B., . . . Suciu, G. (2022). Energy-efficient network protocols and resilient data transmission schemes for wireless sensor Networks—An experimental survey. Energies, 15(23) doi:10.3390/en15238883