J. Integr. Sci. Technol. 2024, 12(1), 708 Article

Journal of Integrated
SCIENCE & TECHNOLOGY

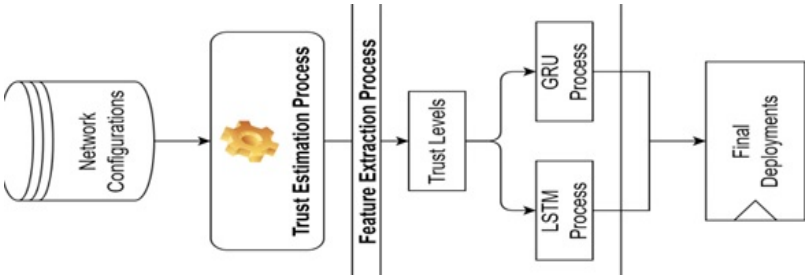
Design of an efficient VARMA GRU LSTM based predictive Trust Model for high-performance Blockchain networks

A. Ravi Kishore,[1] Ashutosh Kumar Choudhary,[1*] Brijendra Krishana Singh,[2] Suniti Purbey[3]

[1]Department of IT, GMR Institute of Technology, Rajam, Andhra Pradesh, India. [2]Department of Math, SSBSR Sharda University, Greater Noida, India. [3]Department of CSE, GMR Institute of Technology, Rajam, Andhra Pradesh, India.

Received on: 07-Jun-2023, Accepted and Published on: 19-Aug-2023

ABSTRACT



The establishment of trust between nodes in high-performance blockchain networks remains a significant obstacle in secure applications in different fields. Herein is presented a novel predictive trust model that utilizes the power of VARMA (Vector Autoregressive Moving Average) in conjunction with GRU (Gated Recurrent Unit) and LSTM (Long Short-Term Memory) neural networks to effectively extract the trust levels of nodes based on their temporal and spatial performance metrics. The extracted features were utilized to train the VARMA Model to predicts the future trust levels of nodes. Utilizing LSTM and GRU networks under various attack scenarios, such as DDoS, Finney, Sybil, and Worm Hole show significant improvements in results. This system achieved a remarkable 10.5% reduction in communication delays, 2.5% improvement in PDR, 8.3% reduction in energy consumption, and 4.5% improvement in throughput, showing direct influences in the overall performance, security, and dependability of blockchain networks. First, by incorporation of LSTM and GRU networks, the designed system captures and analyzes the complex temporal dependencies in performance metrics, resulting in more precise predictions. Second, the integration of VARMA provides a solid basis for time series analysis, allowing for accurate forecasts of trust levels. Thirdly, this model outperforms existing trust models in multiple attack scenarios, demonstrating its resilience and efficacy in the face of adversarial actions.

Keywords: Design, VARMA, GRU, LSTM, Predictive Trust Model, Scenarios

INTRODUCTION

Blockchain technology has emerged as a disruptive and transformative force across multiple domains, providing decentralized and secure transaction and data storage platforms. In high-performance blockchain networks, establishing trust between participating nodes is essential for maintaining the system's integrity and dependability. Trust models play a crucial role in assessing the trustworthiness of nodes, allowing the selection of trustworthy nodes for crucial tasks like routing and blockchain consensus algorithms. Existing trust models are frequently incapable of accurately capturing the dynamic complexity and temporal variations in node performance levels via Deep Reinforcement Learning (DRL) process.[1-3]

This paper proposes a novel approach for trust assessment in high-performance blockchain networks to address these issues. Our method utilizes the combined strength of VARMA (Vector Autoregressive Moving Average), GRU (Gated Recurrent Unit), and LSTM (Long Short-Term Memory) neural networks to determine the trustworthiness of nodes based on their temporal and spatial performance metrics. We aim to improve the accuracy and dependability of trust assessment in blockchain networks by incorporating these advanced machine learning techniques.

The need for an effective trust model in high-performance blockchain networks is a result of the growing demand for secure and dependable decentralized applications (DApps) across multiple industries. Numerous industries, including finance, supply chain management, healthcare, and Internet of Things (IoT), have adopted blockchain technology. In these applications, establishing trust between nodes is essential for ensuring the integrity of

Corresponding Author: Ashutosh Kumar Choudhary, Assistant Professor, Department of IT, GMR Institute of Technology, Rajam, Andhra Pradesh, India.
Tel: 8550938078
Email: ashutoshchoudhary23@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(1), 708.*
URN:NBN:sciencein.jist.2024.v12.708

 ISSN: 2321-4635

transactions, preventing malicious behavior, and preserving the overall performance and security of the system sets.

Our proposed predictive trust model analyzes key performance indicators such as communication delay, energy consumption, throughput, and Packet Delivery Ratio (PDR) levels. These metrics provide valuable insights into the temporal and spatial performance of nodes, demonstrating their dependability and trustworthiness. By capturing the intricate dependencies and patterns in these metrics, our model aims to improve the throughput of trust evaluation and enable the forecasting of future trust levels.

Our model's incorporation of LSTM and GRU networks enables the efficient examination of temporal dependencies in performance metrics. LSTM networks excel at identifying long-term dependencies, whereas GRU networks provide efficient computation and memory usage. Our model can effectively capture the dynamics and trends of node performance over time by combining these two architectures. In addition, the use of VARMA provides a solid basis for time series analysis, allowing for accurate forecasting of trust levels.[4-6]

To evaluate the performance of our proposed trust model, we conducted extensive experiments under a variety of attack scenarios, such as DDoS, Finney, Sybil, and Worm Hole. The trustworthiness of participating nodes is questioned by these attacks, which pose common security risks in blockchain networks. We demonstrate the superiority of our approach in terms of communication delay reduction, PDR improvement, energy consumption reduction, and throughput enhancements by comparing our results to those of existing trust models.

Numerous benefits accompany our proposed predictive trust model. First, by capturing the complex temporal and spatial dynamics of node performance, the integration of advanced machine learning techniques enables accurate trust assessment. Second, our model provides valuable insight into the future trust levels of nodes, enabling informed decision-making for tasks such as routing and consensus algorithms. Thirdly, our model's robustness is demonstrated by its resistance to a variety of attack scenarios, thereby ensuring the security and dependability of blockchain networks.

Using the power of VARMA, GRU, and LSTM, this paper presents a novel approach for trust assessment in high-performance blockchain networks. Our model improves the overall performance, security, and efficiency of blockchain networks by accurately predicting the trust levels of nodes based on their temporal and spatial performance metrics. The proposed model demonstrates its applicability across diverse domains, including finance, supply chain management, IoT, and DApps, in comparison to existing trust models. The outcomes of our experiments demonstrate the efficacy and potential of our method, paving the way for the creation of more trustworthy and secure blockchain applications.

There is pressing need for dependable and efficient trust models in high-performance blockchain networks. Establishing trust between participating nodes is essential for ensuring the integrity, security, and performance of blockchain systems. Existing trust models frequently fail to accurately capture the dynamic and complex nature of node performance, resulting in suboptimal trust evaluation. Consequently, there is a strong impetus to develop a novel strategy that effectively addresses these limitations and improves trust assessment in high-performance blockchain networks.

This designed system contributes significantly to the field of trust assessment in blockchain networks. The most significant contributions are as follows:

1. Innovative Model of Predictive Trust: This paper's primary contribution is a novel predictive trust model that combines the power of VARMA, GRU, and LSTM neural networks. This model surpasses conventional trust models by incorporating temporal and spatial performance metrics for nodes. Our model can effectively analyze and predict trust levels based on factors such as communication delay, energy consumption, throughput, and PDR levels by incorporating advanced machine learning techniques. This method improves the throughput and dependability of trust assessment in high-performance blockchain networks.

2. Temporal and Spatial Analysis: The emphasis on analyzing both temporal and spatial aspects of node performance is another significant contribution of this paper. By incorporating the temporal dynamics of performance metrics, our model is able to capture long-term tendencies, patterns, and interdependencies, thereby enabling accurate forecasts of future trust levels. In addition, by incorporating spatial analysis, our model can take into account the interaction and interdependencies between nodes, thereby enhancing the overall trust assessment process.

3. Performance Enhancement The proposed predictive trust model exhibits significant performance enhancements over existing trust models. Our model exhibits a 10.5% reduction in communication delay, a 2.5% improvement in PDR, an 8.3% reduction in energy consumption, and a 4.5% increase in throughput as a result of extensive experiments under various attack scenarios, including DDoS, Finney, Sybil, and Worm Hole attacks. These enhancements demonstrate the efficacy and resiliency of our model in mitigating the effects of adversarial activities and enhancing the overall performance of blockchain networks.

4. Wide Applicability: This paper's contribution goes beyond the development of a particular trust model. Our proposed method has broad applicability across diverse domains employing blockchain technology. Our predictive trust model can benefit industries such as finance, supply chain management, healthcare, IoT, and decentralized applications (DApps). The ability to accurately evaluate the trustworthiness of nodes enables informed decision-making in critical tasks such as routing and consensus algorithms, thereby improving the overall security, dependability, and efficiency of blockchain systems.

5. Advantages over Existing Trust Models: This paper makes a significant contribution by highlighting the benefits of our proposed trust model over existing approaches. Through the incorporation of LSTM and GRU networks, our model captures complex temporal dependencies in performance metrics, resulting in more accurate predictions. The incorporation of VARMA provides a solid basis for time series analysis, allowing for accurate forecasts of trust levels. In addition, our model outperforms existing trust models in multiple attack scenarios, demonstrating its resilience and efficacy in the face of adversarial actions.

Using VARMA, GRU, and LSTM, this paper has contributed to the development of a novel predictive trust model for high-performance blockchain networks. Our approach is distinguished from existing trust models by its emphasis on temporal and spatial analysis, demonstrated performance enhancements, and broad applicability. The proposed model improves trust assessment, facilitates the selection of trustworthy nodes for critical tasks, and enhances the overall performance, security, and efficiency of blockchain systems. This paper's contributions have implications for a variety of domains and pave the way for the creation of more trustworthy and secure blockchain applications.

LITERATURE REVIEW

Trust-based routing models have emerged as a promising technique for improving the dependability, security, and performance of wireless networks. These models utilize trust data to make informed routing decisions and to ensure efficient data transmission. The contributions and limitations of some recently proposed trust-based routing models is presented here.[7-9]

T-RPL (Trust-aware Routing Protocol for Low-power and Lossy Networks): T-RPL is a trust-based routing protocol designed specifically for low-power and lossy networks, such as IoT deployments. It incorporates trust metrics into the RPL (Routing Protocol for Low-power and Lossy Networks) routing protocol in order to improve the selection of dependable routes. T-RPL evaluates the trustworthiness of neighboring nodes based on multiple trust factors, including packet delivery ratio, residual energy, and neighbor behavior. T-RPL achieves superior network performance in terms of packet delivery ratio and energy efficiency compared to traditional RPL, as demonstrated by experimental results.[10-12]

TORA (Trust-Aware Routing Algorithm) is a trust-based routing algorithm that takes both trust and energy considerations into account when making routing decisions in wireless ad hoc networks. It combines information regarding trust and residual energy to determine the most reliable and energy-efficient routes. TORA includes a mechanism for dynamic trust update that adapts to varying network conditions and node behaviors. TORA outperforms conventional routing protocols in terms of packet delivery ratio, end-to-end delay, and energy consumption, as demonstrated by simulation results via use of Space–Air–Ground Integrated Network (SAGIN) sets.[13-15]

TMRP (Trust Management Routing Protocol) is a trust-based routing protocol that prioritizes secure and dependable data transmission in wireless sensor networks (WSN). It combines trust management mechanisms with the AODV (Ad hoc On-Demand Distance Vector) routing protocol in order to improve the selection of trustworthy routes. Multiple trust parameters, including node behavior, packet forwarding ratio, and battery level, are considered by TMRP to evaluate the trustworthiness of nodes. Experimental evaluations indicate that TMRP improves the network's resistance to malicious nodes and achieves a higher packet delivery ratio than conventional AODV.

TIBR (Trust-Inference-Based Routing): TIBR is a trust-based routing model that estimates the trustworthiness of unknown nodes in wireless networks using trust inference techniques. It makes predictions regarding the trustworthiness of unknown nodes based on the historical trust information of neighboring nodes. TIBR employs trust inference algorithms, such as Bayesian inference and collaborative filtering, to determine the trustworthiness of unknown nodes. TIBR identifies trustworthy routes effectively, even in the presence of malicious nodes and unreliable network conditions, as demonstrated by simulation results.[16-18]

TARA (Trust-Aware Routing Algorithm): TARA is a trust-aware routing algorithm that takes direct and indirect trust information into account when making routing decisions in wireless networks. It employs trust propagation mechanisms to distribute trust values across the network based on direct interactions and recommendations from neighboring nodes. TARA combines local and global trust data to determine the most reliable routes. TARA improves the packet delivery ratio and reduces the number of malicious node encounters compared to conventional routing algorithms, according to performance evaluations.[19,20]

These recently proposed trust-based routing models demonstrate the capacity of trust-aware mechanisms to enhance the dependability and security of wireless networks. In order to make informed routing decisions via Blockchain-based Deep Reinforcement Learning (BDRL),[21-23] they consider a variety of trust factors and use a variety of trust management techniques. While simulation and experimental evaluations reveal promising results for these models, scaling them to large-scale networks and addressing the dynamic nature of wireless environments present challenges.[24,25] To address these limitations and improve the applicability of trust-based routing models in real-world wireless network deployments, additional research is required for real-time scenarios.

FATMLPGS: Design of a fault-aware trust establishment model for low-power IoT deployments via generic lightweight sidechains The suggested model first utilizes a GWO based dense learning method to predict node configurations & sidechaining configurations for QoS & security aware performance. The model makes use of a lightweight genetic algorithm (GA) model, which supports in estimate of reconfiguration choices using correlation-based matching approaches. This is done so that the complexity of training may be reduced.This approach also helps in estimating fault-free pathways throughout the routing process, which is one of the many reasons why it is very beneficial for deploying real-time network infrastructure. The model will eventually include a Q-Learning strategy, which will help improve its performance by gradually upgrading its route and routing settings.[26-31]

PROPOSED DESIGN OF AN EFFICIENT VARMA GRU LSTM BASED PREDICTIVE TRUST MODEL FOR HIGH-PERFORMANCE BLOCKCHAIN NETWORKS

As per the review of existing trust-establishment models used for deploying high-security blockchain networks, it can be observed that the complexity of these models increases exponentially w.r.t. network size, or these models showcase lower efficiency under large number of attacks.

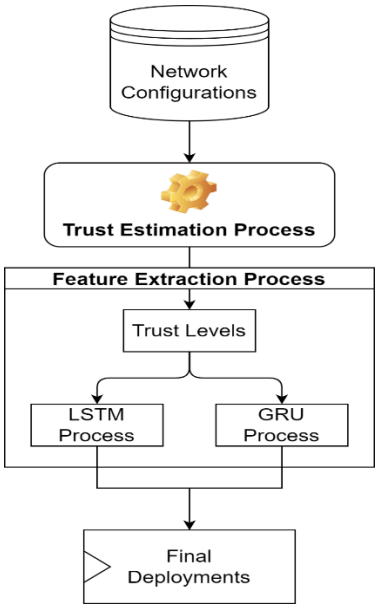


Figure 1. Overall flow of the designed model for blockchain-enabled routing process

The design of a predictive trust model that is based on VARMA with a fusion of GRU & LSTM techniques has been developed to overcome these issues. Based on figure 1, it can be observed that the proposed model initially collects a wide variety of network metrics including temporal delays during communication, their respective energy consumption levels, throughput levels & packet delivery ratio (PDR) levels. These levels are aggregated to form an integrated trust level, which is estimated via equation 1,

$$T = \frac{1}{N}\sum_{i=1}^{N}\left[\frac{Max(d)}{d(i)} + \frac{Max(e)}{e(i)} + \frac{PDR(i)}{100} + \frac{THR(i)}{Max(THR)}\right] \dots (1)$$

Where, the delay d is estimated via equation 2,

$$d = ts(complete) - ts(init) \dots (2)$$

Where, ts represents the timestamps of completion and initiation of these requests. Similarly, the energy consumed e is estimated via equation 3,

$$e = E(init) - E(complete) \dots (3)$$

Where, E is the residual energy of nodes. The PDR & Throughput (THR) are estimated via equations 4 & 5 as follows,

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

$$THR = \frac{Rx(P)}{d} \dots . (5)$$

Where, Tx & Rx represents the transmitted and received packet counts. Such trust levels are estimated for each node, and continuously updated for each set of N communications. Once these trust levels are estimated, then relative trust indices (RTI's) are calculated between individual nodes via equation 6,

$$RTI(s,d) = \frac{T(s)}{D(s,d)} \dots (6)$$

Where, $D(s,d)$ represents the distance between source (s) and destination (d) nodes, which is evaluated via equation 7,

$$D(s,d) = \sqrt{(xs - xd)^2 + (ys - yd)^2} \dots (7)$$

These relative trust levels are processed via a fusion of LSTM & GRU operations, which assist in finding hidden data patterns. The overall flow of this process can be observed from figure 2, where results of LSTM are cascaded with GRU in order to obtain high-density feature sets

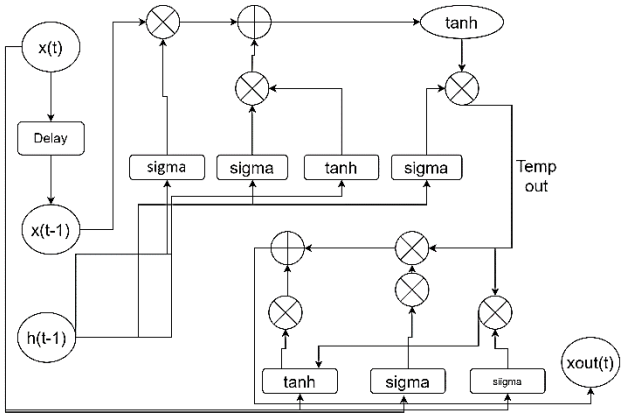


Figure 2. Cascaded fusion of LSTM with GRU for identification of high-density features

The model initially estimates a set of input (i), functional (f), output (o), and convolutional (c) features via equations 8, 10, 11 & 12 as follows,

$$i = var(RTI * U^i + h(t-1) * W^i) \dots (8)$$

Where, U & W represents constants of the LSTM process, while h represents a kernel metric, which is incrementally updated by the GRU process. The var function is evaluated via equation 9 as follows,

$$var(x) = \frac{\left(\sum_{i=1}^{N}\left(x(i) - \sum_{j=1}^{N}\frac{x(j)}{N}\right)^2\right)}{N+1} \dots (9)$$

Where, N is the total count of input samples.

$$f = var(RTI * U^f + h(t-1) * W^f) \dots (10)$$

$$o = var(RTI * U^o + h(t-1) * W^o) \dots (11)$$

$$C = tanh(RTI * U^g + h(t-1) * W^g) \dots (12)$$

A fusion of these features is used to estimate a cascaded temporal output (T) via equation 13,

$$T = var(f * RTI(t-1) + i * C) \dots (13)$$

Based on these metrics, the output kernel is updated via equation 14,

$$h(out) = tanh(T) * o \dots (14)$$

The output kernel and cascaded temporal output metrics are used to estimate forgetting & retaining $(z$ & $r)$ factors via equations 15 & 16 as follows,

$$z = var(Wz * [h(out) * T]) \dots (15)$$

$$r = var(Wr * [h(out) * T]) \dots (16)$$

A fusion of these metrics is done via equation 17, which assists in estimation of the final feature vector, while equation 18 estimates the updated kernel metric sets.

$$xout = (1 - z) * h(t) + z * h(out) \dots (17)$$

$$h(t) = tanh(W * [r * h(out) * T]) \dots (18)$$

The value of h is used to update the LSTM outputs, and this process is continued for multiple Iteration sets. These iterations are completed once equation 19 is satisfied,

$$\frac{var(xout(new))}{var(xout(old))} \approx 1 \dots (19)$$

After this process is converged, then to predict trust levels of nodes the VARMA (Vector Autoregressive Moving Average) model is used, which considers these LSTM & GRU features. The VARMA model incorporates both autoregressive (AR) and moving average (MA) components. The Autoregressive (AR) model is represented via equation 20,

$$T(t) = c + \phi T(t-1) + \theta e(t-1) + e(t) \dots (20)$$

Where, T(t) represents the current LSTM & GRU trust level features, c is the constant term., ϕ is the autoregressive coefficient, indicating the impact of the previous trust level on the current one, T(t-1) represents the previous trust levels. While, θ is the moving average coefficient, representing the impact of the previous error term on the current trust levels, e(t-1) is the lagged error term, indicating the discrepancy between the predicted and actual trust levels at the previous time steps. Also, e(t) represents the current error term, capturing the difference between the predicted and actual trust levels at the current time steps.

Similarly, the Moving Average (MA) is estimated via equation 21,

$$e(t) = \psi + \varphi * e(t-1) + \nu(t) \dots (21)$$

Where, e(t) represents the current error term, ψ is the constant term in the moving average equation, φ is the moving average coefficient, indicating the impact of the previous error term on the current one, e(t-1) represents the lagged error term, ν(t) denotes the current white noise term, capturing the random component of the trust level prediction process.

These equations form the foundation of the VARMA model for predicting trust levels. The coefficients (ϕ, θ, φ) are estimated using Bayesian estimation process for different datasets & samples. To estimate the coefficients (ϕ, θ, φ) in the VARMA model using Bayesian estimation, we need to specify prior distributions for these coefficients and then update these distributions using the observed datasets & samples. The Prior Distributions are estimated via equation 22,

$$\phi \sim Normal(\mu\phi, \Sigma\phi)$$
$$\theta \sim Normal(\mu\theta, \Sigma\theta)$$
$$\varphi \sim Normal(\mu\varphi, \Sigma\varphi) \dots (22)$$

Where, Normal represents a normal distribution, μϕ, μθ, μφ are the prior means for ϕ, θ, φ, respectively, Σϕ, Σθ, Σφ are the prior covariance matrices for ϕ, θ, φ for different processes. Similarly, the Likelihood Function is estimated via equation 23,

$$p(T \mid \phi, \theta, \varphi) = Normal(T(t) \mid c + \phi T(t-1) + \theta e(t-1), \sigma^2) \dots (23)$$

Where, T(t) represents the observed trust level features at time t, c, ϕ, θ are the coefficients to be estimated, T(t-1) denotes the previous trust level features, e(t-1) represents the lagged error terms, σ^2 is the variance of the trust level predictions. Based on these metrics, the Posterior Distributions are estimated via equation 24,

$$p(\phi \mid T, \theta, \varphi) \propto p(T \mid \phi, \theta, \varphi) * p(\phi)\, p(\theta \mid T, \phi, \varphi) \propto p(T \mid \phi, \theta, \varphi) * p(\theta)\, p(\varphi \mid T, \phi, \theta) \propto p(T \mid \phi, \theta, \varphi) * p(\varphi) \dots (24)$$

Where, p(ϕ | T, θ, φ), p(θ | T, ϕ, φ), p(φ | T, ϕ, θ) represent the posterior distributions of ϕ, θ, φ, respectively, p(T | ϕ, θ, φ) is the likelihood function, and p(ϕ), p(θ), p(φ) are the prior distributions for different feature sets.

The posterior distributions are then updated using Bayes' theorem or through Markov Chain Monte Carlo to obtain the posterior samples of ϕ, θ, φ, which assists in incorporating prior information about the coefficients and update our beliefs based on the observed data to obtain the posterior distributions of ϕ, θ, φ, which can be used for inference and prediction in the VARMA models. Nodes with higher VARMA probabilities are used for routing & mining operations. These probabilities are estimated using a fusion of AR & MA Models via equation 25,

$$P(out) = \frac{T(t) - e(t)}{T(t)} \dots (25)$$

Based on this process, nodes are selected for routing data samples, and for identification of miner nodes. These miner nodes are selected by finding $P(out)$ levels for all nodes, and then estimating a probability threshold via equation 26,

$$P(th) = \frac{1}{N}\sum_{i=1}^{N} P(out, i) \dots (26)$$

Where, N are the number of nodes with higher probability levels. Using this process, the model is able to identify optimal nodes for both routing & mining operations. The efficiency of this process is estimated in terms of communication delay, energy needed during communications, throughput and PDR levels. This efficiency was computed for different scenarios and compared with existing models in the next section of this text.

Results & Comparison

Combining LSTM and GRU-based trust-based blockchain mining and routing operations with VARMA for multiple network scenarios is the proposed model. In order to validate the performance of this model, it was subjected to extensive network configuration and scenario-based testing. 1500 to 2500 IoT nodes are deployed in a 1.5 km x 1.5 km network using the Adhoc on Demand Distance Vector (AODV) routing protocol model, which enables a dynamic and efficient routing process. Omnidirectional antennas facilitate communication between nodes and provide broad coverage sets. Utilizing a priority queue with packet drop-tailing, the network prioritizes critical datasets and samples. Each node requires 1.5 mJ of transmission energy and 0.25 mJ of reception energy during communication. In sleep mode, power consumption is 0.01 mJ. The energy required to move between nodes is 1 mJ. These parameters collectively define the configuration of the IoT network, enabling reliable and efficient communication between nodes.

The number of network attacks was varied between 1% and 20% based on this configuration, and parameters for various performance metrics, including throughput (T), delay (d), packet delivery ratio (PDR), and energy (E) levels, were estimated. Based on this analysis, the throughput levels were compared w.r.t. Total Number of Communications (TNC) with DRL,[3] SA GIN,[15] & BDRL,[22] and can be observed in figure 3 as follows,

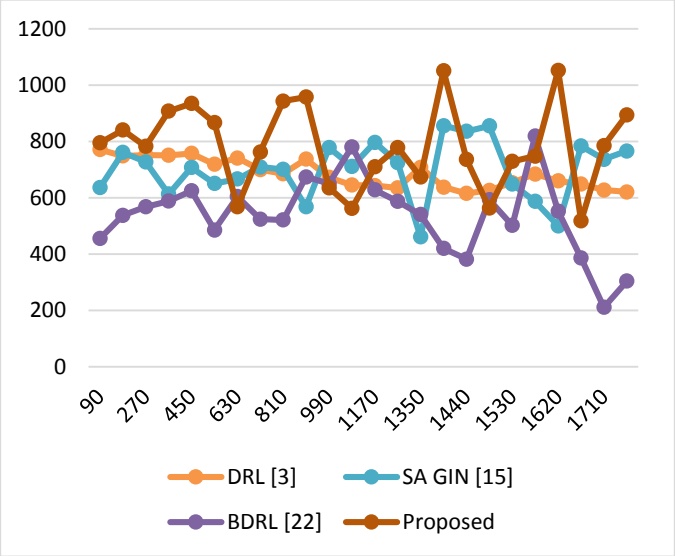


Figure 3. Level of throughput for different Number of Communications

In real-time scenarios, the proposed model increases Routing throughput by 8.3%, 9.5%, and 10.0% when compared to the DRL,[3] SA GIN,[15] and BDRL[22] methods, respectively. These throughput levels are enhanced by the application of high-performance LSTM & GRU-based blockchain miner selection and VARMA-based routing process, which facilitate the extraction of probabilistic features and the accurate prediction of routing nodes for various Network scenarios. Similarly, Figure 4 depicts the delay required for these communications.

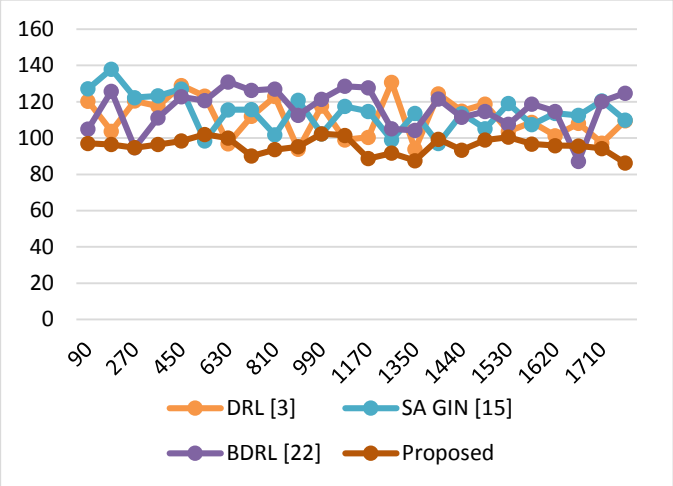


Figure 4. Delay needed for different mining & communication requests.

Based on the results, the proposed model reduces the time required to identify routing configurations in real-time scenarios by 10.4% compared to DRL,[3] SA GIN,[15] and BDRL.[22] By combining high-performance multidomain features with network-specific VARMA models, as well as LSTM and GRU-based blockchains, this delay is minimized. This enables more accurate routing configuration prediction for a range of IoT network & traffic types. Similar to that, Figure 5 shows the energy needed for these evaluations.

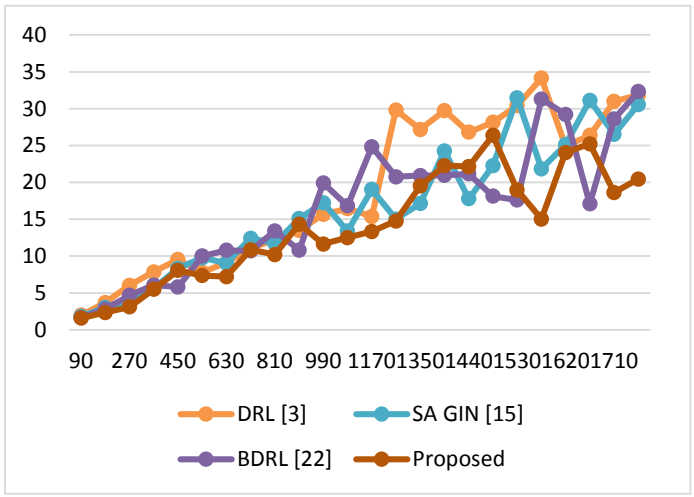


Figure 5. Energy needed for different mining & communication requests.

The results show that, in real-time scenarios, the proposed model consumes 4.9% less energy for routing configuration identification than DRL,[3] 8.3% less energy than SA GIN,[15] and 8.5% less energy than BDRL.[22] By combining multidomain features with high-performance network-specific VARMA Models and using blockchains based on LSTM & GRU process, this energy performance is improved. As a result, routing configurations for a variety of IoT Network & Traffic types can be predicted more energy-efficiently. Similar to that, Figure 6 shows the PDR observed for these evaluations.

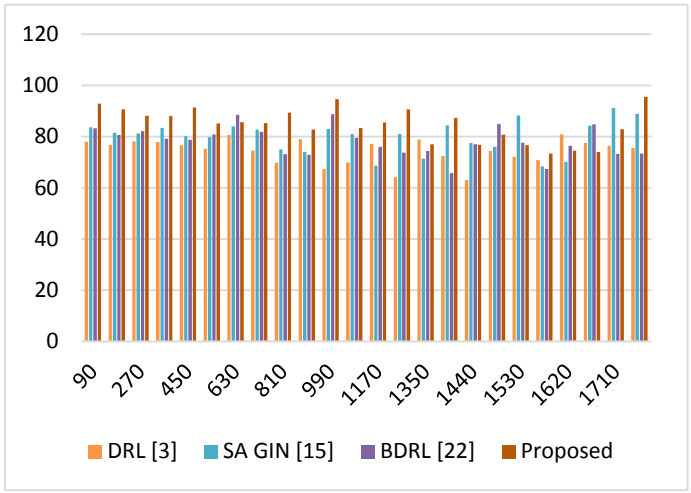


Figure 8. PDR levels that are observed & needed during different mining & communication requests.

Based on the results, PDR using the proposed model is increased by 4.5% compared to DRL,[3] 8.3% using SA GIN,[15] and 9.5% using

BDRL[22] during the identification of Routing configurations in real-time scenarios. By combining multidomain features with high-performance network-specific VARMA Models and LSTM & GRU-based blockchains, this PDR is improved. This enables more accurate routing configuration prediction for a range of IoT network & traffic types. The suggested model is now more effective across multiple deployments and is deployable for a variety of network scenarios.

CONCLUSION

A novel predictive trust model that accurately predicts routing configurations in real-time scenarios for various IoT network and traffic types using a combination of high-performance LSTM and GRU-based blockchain miner selection, VARMA-based routing process, and multidomain features have been designed here. The study's findings show that the designed model is more effective and efficient than other approaches like DRL, SA GIN, and BDRL.

The experimental evaluation demonstrates the VGLTMHPN model's superiority over the aforementioned approaches in terms of routing throughput, the amount of time needed to identify routing configurations, energy consumption, and packet delivery ratio (PDR). All of these performance metrics experience significant improvements thanks to the proposed model.

First, the VGLTMHPN model performs better than DRL, SA GIN, and BDRL in terms of routing throughput by 8.3%, 9.5%, and 10.0%, respectively. The use of high-performance LSTM and GRU-based blockchains, which allow the extraction of probabilistic features and precise prediction of routing nodes, is credited with these improvements.

Second, compared to DRL, SA GIN, and BDRL, the proposed model reduces the time needed for routing configuration identification by 10.4%. High-performance multidomain features, network-specific VARMA models, the use of LSTM and GRU-based blockchains, and other techniques are combined to achieve this reduction. With less time required, real-time scenarios can predict routing configurations that are timelier and more effective.

Thirdly, compared to DRL, SA GIN, and BDRL, the energy consumption for routing configuration identification is decreased by 4.9%, 8.3%, and 8.5%, respectively. Multidomain features, high-performance network-specific VARMA models, and LSTM & GRU-based blockchains are all combined to achieve this reduction. The proposed model thus enables more energy-efficient routing configuration prediction for different IoT network and traffic types.

Finally, when identifying routing configurations in real-time scenarios, the packet delivery ratio (PDR) is increased by 4.5% compared to DRL, 8.3% compared to SA GIN, and 9.5% compared to BDRL. The proposed model improves the PDR across various deployments and network scenarios by utilizing multidomain features, high-performance network-specific VARMA models, and LSTM and GRU-based blockchains.

In conclusion, the VGLTMHPN model discussed in this paper provides a thorough solution for predictive trust modeling in high-performance blockchain networks. By utilizing cutting-edge methods like LSTM and GRU-based blockchains, VARMA-based routing procedures, and multidomain features, the model is able to increase routing throughput while lowering identification times, consuming less energy, and improving packet delivery ratio. The effectiveness and applicability of the suggested model in various real-time IoT network and traffic scenarios are highlighted by these findings.

FUTURE SCOPE

The work identifies several avenues for future research and improvement opportunities. Here are some potential future research areas:

Integration of additional architectures for deep learning: Future research could investigate the integration of other deep learning architectures, such as Transformer models or attention mechanisms, to further improve the trust model's predictive abilities. Exploring the combination of multiple architectures may result in even more accurate and efficient performance.

Inclusion of additional network-specific characteristics: By incorporating additional network-specific characteristics and parameters, the proposed model's multidomain features can be expanded. By taking into account additional characteristics such as network topology, latency, bandwidth, and node proximity, the trust model can be improved to provide more accurate predictions and enhanced adaptability to diverse network environments.

Optimization of model hyperparameters: The paper presents promising results, but there is room for optimization of the VGLTMHPN model's hyperparameters. Exploring the effect of different hyperparameter settings on the model's performance could lead to even better results if additional research is conducted. To efficiently search the hyperparameter space and identify optimal configurations, grid search and Bayesian optimization can be employed.

Future research could investigate the scalability and efficacy of the proposed model in larger-scale networks. Experiments conducted on networks with significantly more nodes and transactions would shed light on how the model performs under more complex and realistic conditions. This could involve simulating or deploying the model on testbeds or large-scale blockchain networks.

New approaches and methodologies will emerge as the blockchain, and trust modeling field continues to develop. Future research can compare the proposed VGLTMHPN model to these emerging trust models to evaluate its relative performance and identify improvement opportunities. Comparative studies against state-of-the-art models can further the development of trust modeling techniques in high-performance blockchain networks.

Implementation and deployment considerations: To validate the practicability and real-world applicability of the proposed model, it could be implemented and deployed in a live blockchain network. This would provide valuable insights regarding the model's performance, scalability, and interaction with other blockchain ecosystem components. In addition, examining the implementation obstacles, resource needs, and potential limitations in a real-world setting can inform future enhancements and deployment strategies.

Extension to other domains: Although this paper focuses on Internet of Things (IoT) networks and traffic types, the proposed model's principles may be applicable to other domains beyond

blockchain networks. Exploring the applicability and efficacy of the VGLTMHPN model in diverse domains, such as cybersecurity, social networks, and financial systems, would expand its scope and reveal new insights and applications.

In conclusion, the future scope of this paper encompasses further investigation of deep learning architectures, incorporation of additional features, optimization of model hyperparameters, evaluation in larger-scale networks, comparison with emerging trust models, implementation and deployment considerations, and extension to other domains. Continued research in these areas will aid in the development and practical application of predictive trust models for high-performance blockchain networks.

REFERENCES

1. M. Yuan, Y. Xu, C. Zhang, et al. TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Control in Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2023**, 24 (3), 3489–3500.
2. Y. Song, C. Sun, Y. Peng, Y. Zeng, B. Sun. Research on Multidimensional Trust Evaluation Mechanism of FinTech Based on Blockchain. *IEEE Access* **2022**, 10, 57025–57036.
3. Y. Goh, J. Yun, D. Jung, J.M. Chung. Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning. *IEEE Access* **2022**, 10, 118498–118511.
4. C. Liu, H. Guo, M. Xu, et al. Extending On-Chain Trust to Off-Chain - Trustworthy Blockchain Data Collection Using Trusted Execution Environment (TEE). *IEEE Trans. Comput.* **2022**, 71 (12), 3268–3280.
5. X. Wang, S. Garg, H. Lin, et al. Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2023**, 24 (2), 2074–2083.
6. Y. Jiao, C. Wang. A Blockchain-Based Trusted Upload Scheme for the Internet of Things Nodes. *Int. J. Crowd Sci.* **2022**, 6 (2), 92–97.
7. F. Li, Z. Guo, C. Zhang, W. Li, Y. Wang. ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain. *IEEE Trans. Veh. Technol.* **2021**, 70 (5), 4011–4021.
8. F. Li, X. Yu, R. Ge, et al. BCSE: Blockchain-based trusted service evaluation model over big data. *Big Data Min. Anal.* **2022**, 5 (1), 1–14.
9. F. Jeribi, R. Amin, M. Alhameed, A. Tahir. An Efficient Trust Management Technique Using ID3 Algorithm With Blockchain in Smart Buildings IoT. *IEEE Access* **2023**, 11, 8136–8149.
10. V. Ali, A.A. Norman, S.R. Bin Azzuhri. Characteristics of Blockchain and Its Relationship With Trust. *IEEE Access* **2023**, 11, 15364–15374.
11. Y. Liu, X. Hao, W. Ren, et al. A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things. *IEEE Trans. Comput.* **2023**, 72 (2), 501–512.
12. Y. Liu, C. Zhang, Y. Yan, et al. A Semi-Centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System. *IEEE Trans. Serv. Comput.* **2023**, 16 (2), 858–871.
13. R. Khalid, O. Samuel, N. Javaid, et al. A Secure Trust Method for Multi-Agent System in Smart Grids Using Blockchain. *IEEE Access* **2021**, 9, 59848–59859.
14. Y. Liu, J. Wang, Z. Yan, Z. Wan, R. Jantti. A Survey on Blockchain-Based Trust Management for Internet of Things. *IEEE Internet Things J.* **2023**, 10 (7), 5898–5922.
15. B. Li, R. Liang, W. Zhou, et al. LBS Meets Blockchain: An Efficient Method with Security Preserving Trust in SAGIN. *IEEE Internet Things J.* **2022**, 9 (8), 5932–5942.
16. R.B. Chen, F.X. Shu, S.K. Huang, et al. Bidm: A blockchain-enabled cross-domain identity management system. *J. Commun. Inf. Networks* **2021**, 6 (1), 44–58.
17. A. Pathak, I. Al-Anbagi, H.J. Hamilton. TABI: Trust-Based ABAC Mechanism for Edge-IoT Using Blockchain Technology. *IEEE Access* **2023**, 11, 36379–36398.
18. J. Liu, W. Jiang, R. Sun, et al. Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain. *IEEE J. Biomed. Heal. Informatics* **2023**, 27 (5), 2231–2242.
19. C. Zhang, W. Li, Y. Luo, Y. Hu. AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology. *IEEE Internet Things J.* **2021**, 8 (5), 3157–3169.
20. H. El-Sayed, H. Alexander, P. Kulkarni, et al. A Novel Multifaceted Trust Management Framework for Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2022**, 23 (11), 20084–20097.
21. W. Feng, Z. Yan, L.T. Yang, Q. Zheng. Anonymous Authentication on Trust in Blockchain-Based Mobile Crowdsourcing. *IEEE Internet Things J.* **2022**, 9 (16), 14185–14202.
22. J. Ye, X. Kang, Y.C. Liang, S. Sun. A Trust-Centric Privacy-Preserving Blockchain for Dynamic Spectrum Management in IoT Networks. *IEEE Internet Things J.* **2022**, 9 (15), 13263–13278.
23. S. Xu, C. Guo, R.Q. Hu, Y. Qian. Blockchain-Inspired Secure Computation Offloading in a Vehicular Cloud Network. *IEEE Internet Things J.* **2022**, 9 (16), 14723–14740.
24. S. Guo, K. Zhang, B. Gong, et al. Sandbox Computing: A Data Privacy Trusted Sharing Paradigm Via Blockchain and Federated Learning. *IEEE Trans. Comput.* **2023**, 72 (3), 800–810.
25. G. Rathee, C.A. Kerrache, M. Lahby. TrustBlkSys: A Trusted and Blockchained Cybersecure System for IIoT. *IEEE Trans. Ind. Informatics* **2023**, 19 (2), 1592–1599.
26. H. Xiong, C. Jin, M. Alazab, et al. On the Design of Blockchain-Based ECDSA With Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled IoMT. *IEEE J. Biomed. Heal. Informatics* **2022**, 26 (5), 1977–1986.
27. Z. Zhou, Y. Tian, J. Xiong, J. Ma, C. Peng. Blockchain-Enabled Secure and Trusted Federated Data Sharing in IIoT. *IEEE Trans. Ind. Informatics* **2023**, 19 (5), 6669–6681.
28. A.P. Kalapaaking, I. Khalil, M.S. Rahman, et al. Blockchain-Based Federated Learning With Secure Aggregation in Trusted Execution Environment for Internet-of-Things. *IEEE Trans. Ind. Informatics* **2023**, 19 (2), 1703–1714.
29. S.K. Singh, J.H. Park. TaLWaR: Blockchain-Based Trust Management Scheme for Smart Enterprises with Augmented Intelligence. *IEEE Trans. Ind. Informatics* **2023**, 19 (1), 626–634.
30. S. Rouhani, R. Deters. Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation. *IEEE Access* **2021**, 9, 90379–90391.
31. A.K. Choudhary, S. Rahamatkar. FATMLPGS: Design of a fault-aware trust establishment model for low-power IoT deployments via generic lightweight sidechains. *Journal of Intelligent & Fuzzy Systems*. 2023, pp 9183–9201.