

Design of Running Training Assistance System Based on Blockchain Technology in Wireless Network

Fuxing Ma (✉ junniula21973gey@163.com)

Research

Keywords: Running Training, Wireless Sensing, Blockchain, Privacy Protection

Posted Date: December 23rd, 2020

DOI: <https://doi.org/10.21203/rs.3.rs-51851/v2>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Version of Record: A version of this preprint was published on January 31st, 2021. See the published version at <https://doi.org/10.1186/s13638-021-01897-4>.

Design of Running Training Assistance System Based on Blockchain Technology in Wireless Network

Fuxing Ma

Physical Education Department, Hunan Institute of Technology, Hengyang 421002,
China

Email: junniula21973gey@163.com

Abstract: Running exercise can increase the basal metabolic rate and increase the time of aerobic exercise. Based on the current needs of the general public for running auxiliary training, this paper combines wireless sensing and blockchain technology in the design scheme, and designs and implements a running training auxiliary technology. First, it obtains the user's gait information and other related parameters in the process through the wireless sensor network, and optimize the calculation gait in different states through the noise processing algorithm. Then, we use the blockchain technology to design a data transmission and storage plan for the protection and analysis of the user's personal privacy data. The proposed method builds a new type of sports training assistance system for the masses of modern society and contributes to the masses' physical exercise.

Keywords: Running Training, Wireless Network, Blockchain Technology, Privacy Protection

1 Introduction

With the abundance of food and the reduction of physical labor, obesity has become a social problem in all countries. Modern sports medicine has proved that the energy consumption of the human body is mainly composed of basic metabolism, the thermal effect of food and physical activity [1-2]. Exercise can increase the basal metabolic rate and increase the time of aerobic exercise. It is a healthy and effective way to lose weight. When the human body walks or runs, it is often accompanied by

the swing of the limbs, and the periodic swing information of the body can be collected by placing the sensor on the limbs or torso [3]. Through preprocessing and algorithm analysis of the collected data, we can get the intuitive quantities of step frequency, pace, and stride that reflect the state of motion [4].

With the continuous development of sensor technology, wearable devices have gradually integrated into people's lives. Early wearable devices are used in smart gaming glasses and controllers, which can improve the user's more comfortable gaming experience [5-6]. The improvement of living standards has caused people to pay attention to health problems, and smart wearable devices are gradually being used in sports medicine to detect people's healthy exercise. Because the sensor is interfered by the environment and its own noise, it will have a great impact on the output data, and it is easy to cause misjudgment in the gait judgment, so it is particularly important to filter the collected information. Two common types of noise are the high-frequency noise of the sensor and the burst noise caused by the external environment during the movement [7]. Song Haoran et al. proposed an anti-aliasing filtering method to filter out the noise generated by the system when studying high-precision pedometers, reducing the probability of pedometer misjudgment caused by noise [8]. Before Liu Yuhang conducts algorithm design on the data, he needs to filter the output data, because the frequency of human body movement belongs to the low-frequency signal [9]. There are many ways of filtering, and it is very important to select a suitable filtering method to filter out different noises.

Gait is a kind of information that intuitively expresses the human body's movement state. Factors such as the user's stride speed, stride frequency and stride length during exercise determine the exercise intensity and amount of exercise [10]. With the continuous application of inertial sensors in smart devices and the in-depth research of various pedometer algorithms, the acceleration and angular velocity of gait information are collected, and the data is fused in various ways to calculate the movement velocity and attitude angle. Waiting for physical quantities to reflect the state of motion has gradually become the main direction of today's smart device research [11]. Therefore, in today's society, the development of a running training assistance system for the general public has important research significance and application value. Therefore, this paper proposes a running training model based on blockchain and wireless sensing technology [12].

The specific contributions of this paper include:

(1) Combining wireless sensing and blockchain technology into the design scheme, designing and realizing running auxiliary training technology.

(2) Obtain the user's gait information and other related parameters through the wireless sensor network, and optimize the calculated gait in different states through the noise processing algorithm.

(3) Propose the use of blockchain technology to design data transmission and storage plans to protect and analyze users' personal privacy data.

(4) The proposed method has established a new type of sports training auxiliary system for the masses of modern society, and has made contributions to the masses' physical exercise.

The rest of this paper is organized as follows. Section 2 discusses related work, followed by the methods is discussed in Section 3. The experiment is discussed in Section 4. Section 5 concludes the paper with summary and future research directions.

2 Related work

2.1 Wireless sensing technology

A wireless sensor network (WSN) can be defined as a network composed of sensor nodes, which are distributed in the network deployment area and work together. The information collected from the monitoring site is transmitted through the wireless link [13]. The data collected by the sensor nodes are sent to the base station, which can process the data locally, or further transmit the data to other data storage or processing centers through the network. Compared with traditional network solutions, WSN technology provides many advantages [14]. For example, lower cost, scalability, reliability, accuracy, flexibility, and ease of deployment make WSN technology a wide range of application scenarios. The schematic diagram of wireless sensor node intrusion and scene detection is shown in Figure 1.

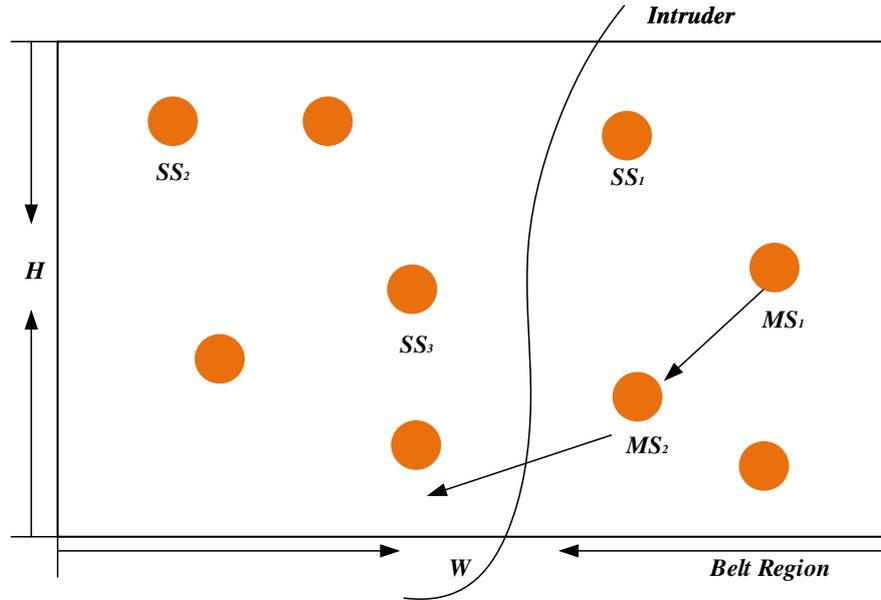


Figure 1. Schematic diagram of wireless sensor node intrusion and scene detection

In the military, sensor nodes can be used to detect, locate or track the actions of the enemy. In the field of disaster prevention, sensor nodes can sense and detect the environment to predict disasters in advance. In medical applications, wearable sensor nodes can help monitor the health of patients [15]. In the security field, sensors can provide intrusion detection and border inspection functions. On the other hand, compared with traditional networks, WSN has several resource constraints, including but not limited to limited node energy, limited communication range, low bandwidth, and limited node computing capabilities. The research goal of wireless sensor networks is to solve the above design and resource constraints by introducing new design concepts, improving existing protocols and developing new algorithms.

2.2 Blockchain technology

Generally speaking, the blockchain is a decentralized distributed storage database, and various mining technologies and electronic currencies are implemented based on the blockchain. From a small point of view, blockchain is a data structure that can form a single-linked list of data in a specific order, and various encryption methods ensure that these data cannot be tampered with [16]. From a large perspective, blockchain is a distributed architecture that uses distributed storage, distributed algorithms, and encryption security methods to form smart contracts to store operating data and operating records. The schematic diagram of the

authentication path of Merkle hash tree is shown in Figure 2.

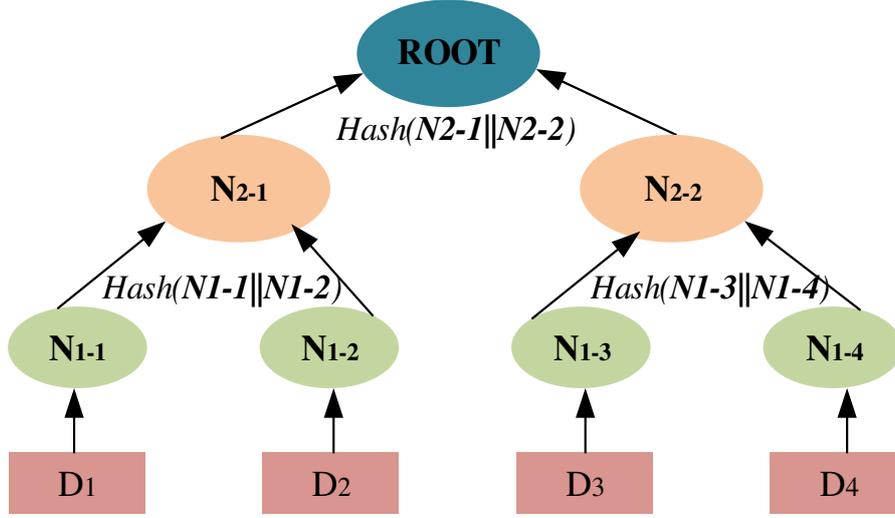


Figure 2. Schematic diagram of the authentication path of the Merkle Hash tree

It is possible to determine whether the decentralized node data is effective and quickly reach a common test through the decision-making design of various distributed nodes scattered everywhere [17]. The main solution of the blockchain consensus layer is to make distributed nodes reach a consensus and establish a trust mechanism. For example, whether a node is valid, all nodes in the blockchain need to reach a consensus to form a unified opinion. The system implemented in this article adopts the DPOS mechanism to establish Blockchain consensus layer.

The core idea of POW is to use fog computing to disperse the calculations to the end of the node, and then use these nodes to complete the proof of the node's workload through the algorithm, so as to reach a consensus under the premise of ensuring security. The definition of POW target value is shown in the formula [18].

$$T=m/dig \quad (1)$$

The workload of the search methods that have been tried as above proves that there are efficiency disadvantages, and the Ethos algorithm can be used to prevent the impact of the efficiency difference of each node. The characteristic of this kind of algorithm is that the point where the algorithm improves the efficiency has nothing to do with the improvement of memory and bandwidth, only I/O determines the speed.

$$SHA256(\text{Parent Block Hash} + \text{Hash} + \text{Merkle Root} + \text{Nonce} + \dots) \leq T \quad (2)$$

The disadvantage of the above search method is that the method of finding the

target value is to keep trying. The Ethos algorithm can be used to prevent the impact of the efficiency difference of each node. The characteristic of this kind of algorithm is that the point where the algorithm improves the efficiency has nothing to do with the improvement of memory and bandwidth, only I/O determines the speed.

Smart contracts have general features such as decentralization and anti-tampering of the blockchain. In essence, they are a special code or script running on the blockchain [19]. As a script or program, the contract is distributed on each node and has the characteristics of decentralization and distribution. Any problem on any node does not affect the operation of the entire contract.

The formula of Ethos algorithm is as follows:

$$RAND(h, n) \leq M/d \quad (3)$$

Bring Eq. (2) into Eq. (3) to get the basic formula, which means the probability of the output category A given the instance Y.

$$P(Y = c_k / X = x) = \frac{\prod_{j=1}^n P(X^{(j)} = x^{(j)} / Y = c_k) P(Y = c_k)}{\sum_{k=1}^K (Y = c_k) \prod_{j=1}^n P(X^{(j)} = x^{(j)} / Y = c_k)} \quad (4)$$

In practical application, when classifying feature instances, we choose the one with the largest probability value as the final category, which can be formalized as Eq. (5).

$$y = f(x) = \operatorname{argmax} \frac{\prod_{j=1}^n P(X^{(j)} = x^{(j)} / Y = c_k) P(Y = c_k)}{\sum_{k=1}^K (Y = c_k) \prod_{j=1}^n P(X^{(j)} = x^{(j)} / Y = c_k)} \quad (5)$$

Each node will verify the validity of the received data block, valid data will be broadcast, otherwise it will be discarded [20]. Only when all nodes are artificially valid data block can the data block be valid. Otherwise, it is invalid data. The valid data will be added to the main chain. The elements for detection include Merkle root, hash value and timestamp.

3 Methods

3.1 Overall design plan

This topic combines a heart rate sensor with an inertial sensor, and uses a heart rate sensor to collect heart rate values. The heart rate value is compared with the target heart rate to determine whether the user is doing aerobic exercise, and the voice module is used to remind the user. Using inertial sensors to collect gait information, after preprocessing and algorithm analysis, the user's movement steps are finally

displayed in real time [21]. The influencing factors of energy expenditure are mostly related to the biological factors of the individual. Users can input their own personal information such as age, gender, and weight to provide individual parameters for the calculation of energy expenditure. The system framework is shown in Figure 3.

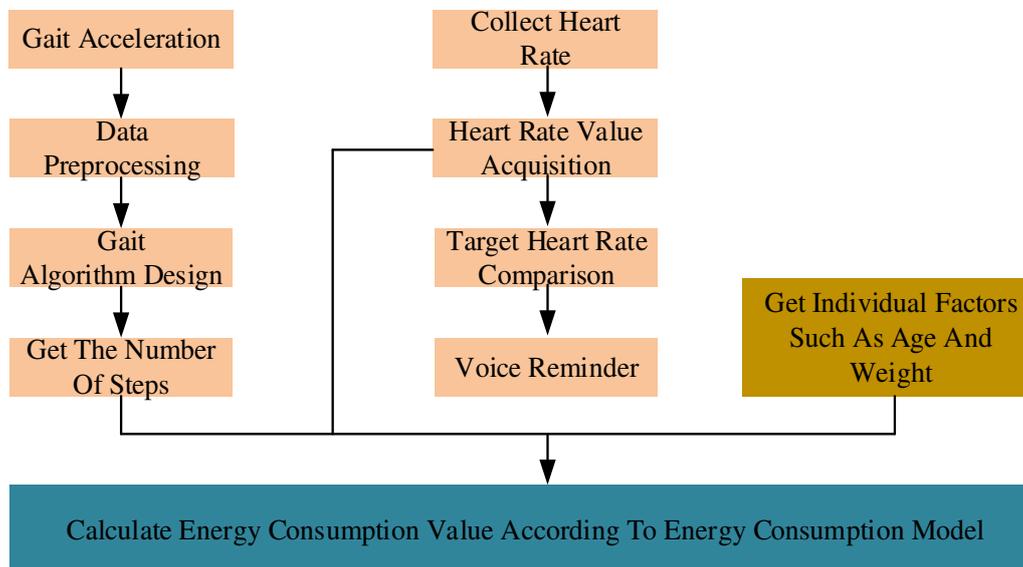


Figure 3. Frame diagram of running training assistive technology system

3.2 Design of wireless sensor running posture conversion

The research on pedometer involves the extraction of gait information and the design of gait algorithm, taking into account the accuracy of data collection and the real-time nature of the system [22]. This subject collect gait acceleration and angular velocity data, uses the quaternion algorithm to obtain the attitude angle, and analyzes the change of the attitude angle during exercise to design a step counting algorithm. In the inertial navigation system, there are three ways to express the attitude of the carrier: attitude angle, direction cosine matrix and quaternion, which can be mutually converted. This section introduces the conversion principle of quaternion and attitude angle [23].

The posture coordinate system is established with the body of the equipment as the center, and the coordinate system that is commonly known by everyone is established on the basis of geographic space. The relationship between the posture coordinate system and the geographic coordinate system is shown in Figure 4.

The definition of geographic coordinate system is:

Step 1: Select a point O on the ground as the origin;

Step 2: Make the X axis direction in the horizontal plane and point to any direction;

Step 3: The Z axis is perpendicular to the ground and points to the center of the earth;

Step 4: The Y axis is in the horizontal plane and perpendicular to the X axis, and its direction is determined by the right-hand rule.

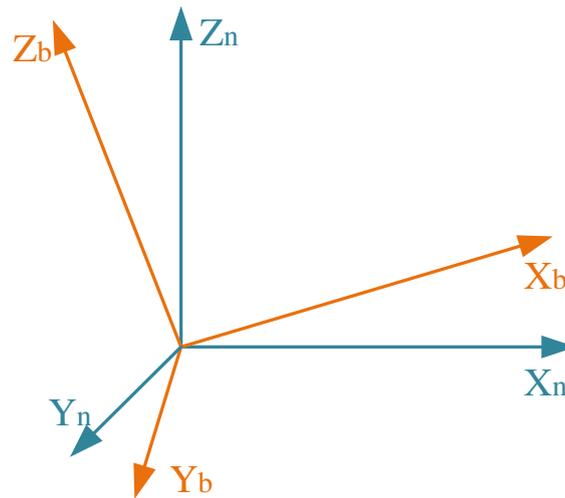


Figure 4. Posture coordinate system $O-X_bY_bZ_b$, Geographic coordinate system $O-X_nY_nZ_n$

When studying the angular position relationship between the attitude coordinate system and the geographic coordinate system, the origin of the two coordinate systems can be made to coincide with each other through translation [24]. Then rotate the geographic coordinate system around the space axis to obtain the posture coordinate system. The rotation equivalent diagram is shown in Figure 5.

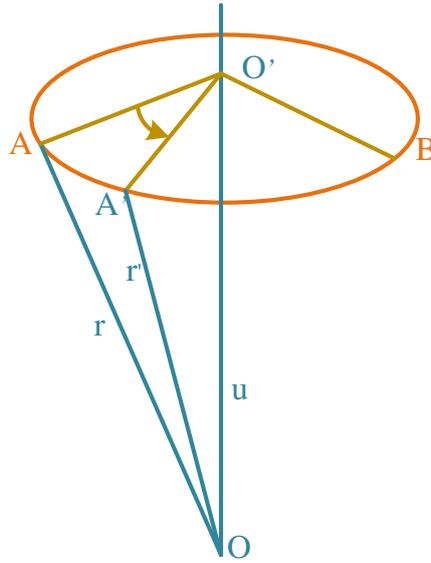


Figure 5 Schematic diagram of equivalent conversion effect of coordinate system

Rotate the geographic coordinate system to obtain the posture coordinate system. Any complicated angular position relationship between the two coordinate systems can be equivalent to a combination of finite basic rotations [25-26]. One basic rotation matrix is determined for each basic rotation, and the multiplication of multiple basic rotation matrices is equal to the posture matrix required for coordinate system conversion. Perform three basic rotations of the geographic coordinate system to obtain the attitude coordinate system.

4 Experiment

4.1 Data source and test environment

This system is dedicated to collecting human gait information and heart rate information, and calculating the energy consumption value under the premise of aerobic exercise. The system test mainly involves the accuracy of the collection of exercise steps and the accuracy of the collection of heart rate values [27]. The test environment is a treadmill in a gym, the slope of the treadmill is set to zero, and people of different genders and different age groups are selected for testing. Wear a portable device on your ankle and follow the prompts on the screen to enter your gender, age, and weight, then you can walk or run [28]. At the same time, the tester should wear a sports bracelet to compare and analyze the data collected by the system and the data collected by the bracelet.

4.2 Comparison of user privacy protection based on blockchain

In the initialization phase, in order to verify the parameter protection effect of blockchain technology on the running training process, the following test process was carried out. The selected parameters are as follows: the hash function is SHA-256, and the asymmetric encryption algorithm is RSA-1024. According to the security requirements of OPE, the ciphertext space of OPE is assumed to be the third power of the plaintext space. Test the computational cost of N with different privacy protection levels.

In the initialization phase of I-MPLS, the LDO must first divide R iteratively into N times in a quad-tree manner, which means that N different degrees of privacy protection can be achieved. Subsequently, all the dividing lines are subjected to OPE operation, and then the dividing line perpendicular to the x-axis and the dividing line perpendicular to the y-axis are used as leaf nodes to generate two Merkle hash trees. Figure 6 shows the influence of the privacy protection level and computational overhead of the blockchain-the initialization phase. Figure 7 shows the impact of blockchain protection level and computational overhead-location recording stage.

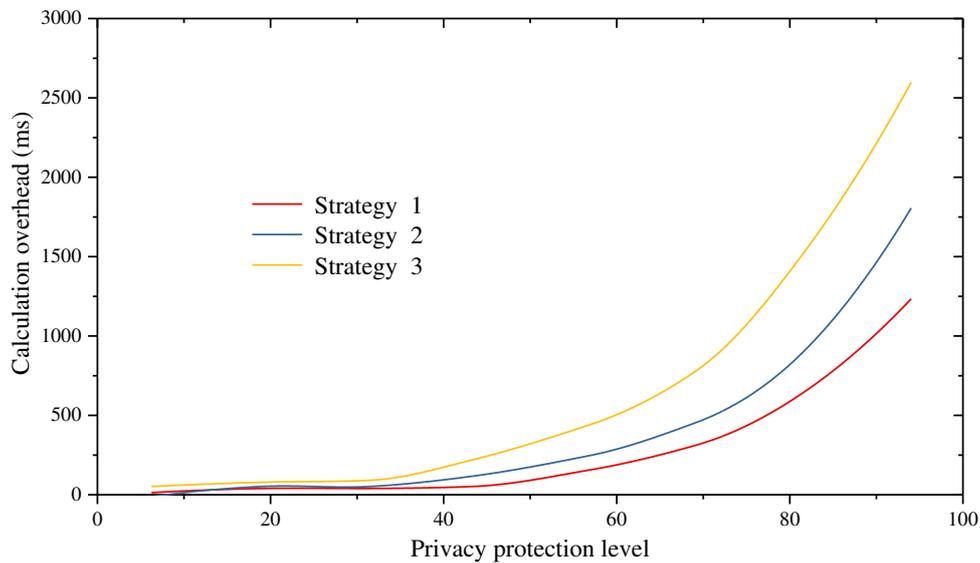


Figure 6. The privacy protection level of the blockchain and the impact of computational overhead-initialization phase

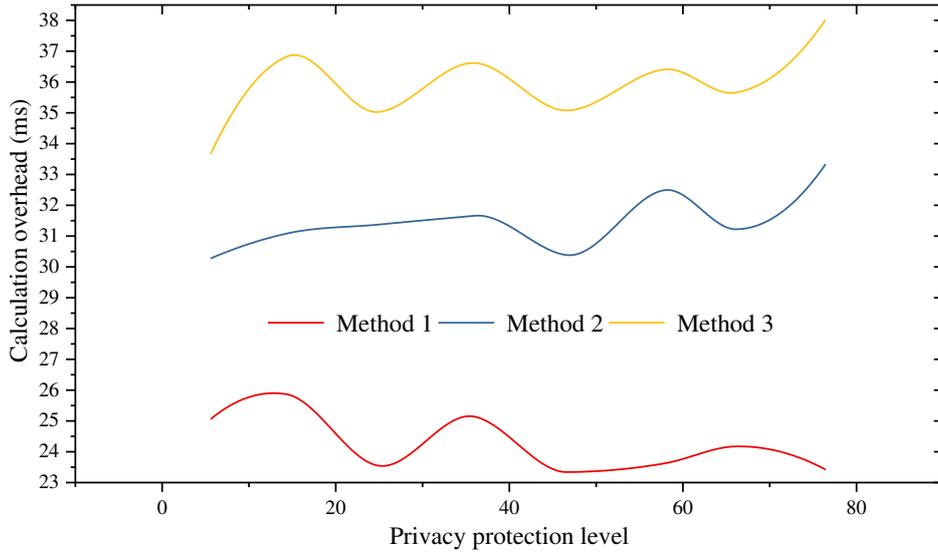


Figure 7. Blockchain protection level and the impact of computational overhead-location recording stage

It can be seen from Fig. 6 and Fig. 7 that under the same size of the OPE plaintext space, the computational overhead of the LDO initialization phase increases approximately exponentially as N increases. Under OPE (30), the computational overhead of the initialization phase exceeds 2500ms when $N=8$. Therefore, OPE encryption operation is required in the initialization phase. Since the computational cost of generating a Merkle hash tree is much smaller than that of OPE encryption, the OPE encryption operation is the main factor affecting the initialization phase of I-MPLS. At the same time, under the same privacy protection level number N , the different plaintext space sizes of OPE also make the calculation overhead of the initialization phase different. A larger OPE plaintext space will lead to a slightly higher calculation cost at this stage, because the larger the OPE plaintext space, The lower the execution efficiency of OPE encryption operation.

4.3 Comparison of running training efficiency based on wireless sensing

The test is divided into two scenarios. The first scenario is to make the tester walk 100 steps at a speed of 4km/h and run 150 steps at a speed of 7km/h, and record the number of steps finally displayed by the system. The second scenario is to measure the tester's static heart rate, and first calculate the tester's target heart rate range before the test, so that the tester can run. Observe and record the heart rate value measured by this system and the heart rate value measured by the bracelet in real time. Figure 8 shows the comparison result of running training efficiency based on wireless

sensing.

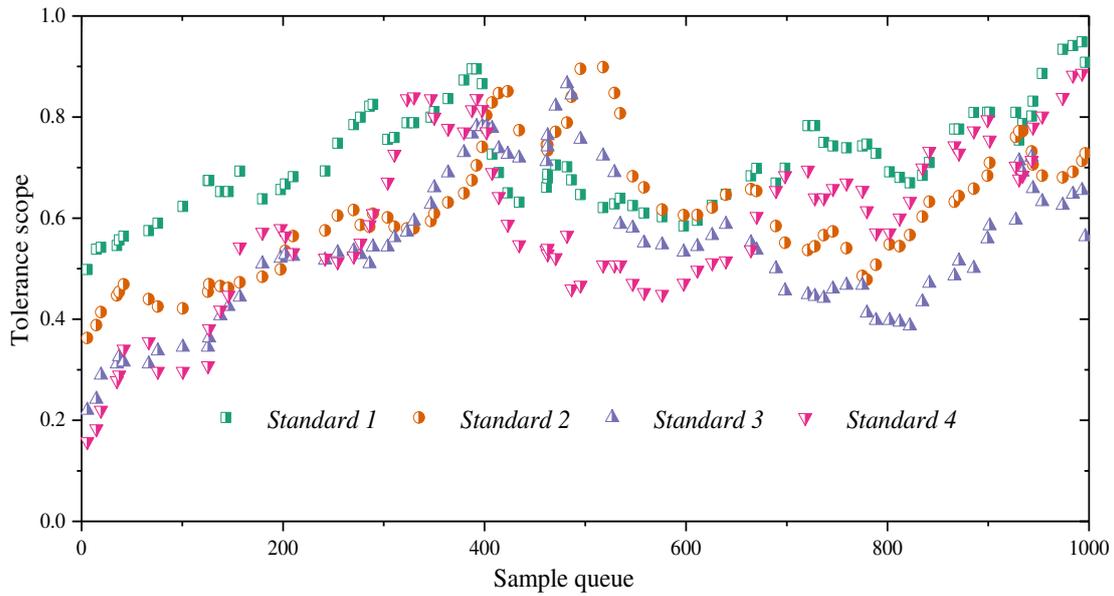


Figure 8. Comparison results of running training efficiency based on wireless sensing

This chapter tests the performance of the system based on the completion of the software and hardware platform of the system. The zero-input error of the attitude angle is corrected, and random noise and burst impulse noise are filtered out. By collecting gait information of different people in different motion states, the judgment accuracy of the system's step counting algorithm is verified. The system has basically removed the influence of human physiological parameters on step counting, and can be applied to the detection of different ages, different genders, and different exercise states. The improvement direction of the system's step counting algorithm and energy consumption value calculation model is proposed. At the same time, the accuracy of the heart rate sensor collected by the heart rate sensor is verified. It is found that the system is relatively stable in the detection of static heart rate. As exercise intensity increases, The heart rate collection error of the sensor increases accordingly, which may be related to the contact surface between the sensor and the skin, and the stability of the contact between the sensor and the skin needs to be enhanced.

5 Results and discussion

In recent years, the application of inertial sensors has gradually integrated into all aspects of people's lives, and it has a very mature product market in the fields of

gesture recognition, gait recognition, and smart home. As one of the applications of inertial sensors, wearable devices were the first to be used in smart games. With the improvement of living standards, people's attention to their own health has gradually increased. Wearable devices have received more and more products in health detection. Pay more attention. In this paper, the combination of wireless sensing and blockchain technology is applied to the design plan, and a running training auxiliary technology is designed and implemented. Obtain the user's gait information and other related parameters in the process through the wireless sensor network, and optimize the calculation gait in different states through the noise processing algorithm. Design data transmission and storage schemes through blockchain technology for the protection and analysis of user-related personal privacy data. There are still some problems in the design of this system that need to be improved. In the future, further research on assistive technology for running training will be carried out.

List of abbreviations

(DPOS)

Delegated proof of stake

Declarations

Availability of data and material

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

- [1] A. Nunomiya, Activation of the hypoxia-inducible factor pathway induced by phd2 deficiency enhances the effect of running training in mice. *Acta Physiologica* 220(1), 99-112(2017).
- [2] C. Adam, C. Lake, Adjustments with running speed reveal neuromuscular adaptations during landing associated with high mileage running training. *Journal of applied physiology*(2017).

- [3] J. Verheul, Clansy, A. C. Lake, Adjustments with running speed reveal neuromuscular adaptations during landing associated with high mileage running training. *Journal of Applied Physiology* 122(3), 653-665(2016).
- [4] S. Hogg, G. Hopker, L. Coakley, Prescribing 6-weeks of running training using parameters from a self-paced maximal oxygen uptake protocol. *European Journal of Applied Physiology*(2018).
- [5] H. James, S. Hopker, Prescribing 6-weeks of running training using parameters from a self-paced maximal oxygen uptake protocol. *European Journal of Applied Physiology*(2018).
- [6] A. L. Rocha, B. C. Pereira, R. Pauli, José, T. De, Downhill running excessive training inhibits hypertrophy in mice skeletal muscles with different fiber type composition. *Journal of Cellular Physiology* 231(5), 1045-1056(2016).
- [7] H. Ma, X. Hui, B. David, Eco-driving assistance system for a manual transmission bus based on machine learning. *IEEE Transactions on Intelligent Transportation Systems* 19(2), 572-581(2018).
- [8] Y. Wang, S. Guo, Y. Li, T. Tamiya, Y. Song, Design and evaluation of safety operation vr training system for robotic catheter surgery. *Medical & Biological Engineering & Computing*(2017).
- [9] D. Karaboga, E. Kaya, Adaptive network based fuzzy inference system (anfis) training approaches: a comprehensive survey. *Artificial Intelligence Review*(2018).
- [10] J. M. Peters, R. S. Schumacher, Dynamics governing the maintenance and evolution of a simulated mesoscale convective system with a training convective line. *Journal of the Atmospheric Sciences* 73(7), 2643-2664(2016).
- [11] N. Bradley, A. Joseph, R. Kevin, R. Shawn, Differential basal and exercise-induced igf-i system responses to resistance vs. calisthenic-based military readiness training programs. *Growth Hormone & IGF Research* 32(5), 33-40(2017).
- [12] L. Puthon, P. Bouzat, T. Rupp, Physiological characteristics of elite high-altitude climbers. *Scandinavian Journal of Medicine & Science in Sports*(2016).

- [13] L. Mingsheng, M. Faqiang, Integrated passive wireless pressure and temperature dual-parameter sensor based on ltcc technology. *Ceramics International*(2018).
- [14] A. G. Bahram, K. Sanaz, S. Samaneh, Design of small size and high sensitive less-invasive wireless blood pressure sensor using mems technology. *Iet Circuits Devices & Systems*(2018).
- [15] C. Lin, D. Han, J. Deng, G. Wu, P²S: a primary and passer-by scheduling algorithm for on-demand charging architecture in wireless rechargeable sensor networks. *IEEE Transactions on Vehicular Technology*(2017).
- [16] M. Zhong, C. Ping, C. Wen, Highly sensitive, printable nanostructured conductive polymer wireless sensor for food spoilage detection. *Nano Letters*(2018).
- [17] R. Khelladi, F. Ghanem, M. Djeddou, Dual-band sensor-antenna design for low energy consumption/cost wireless sensor nodes. *IET Microwaves Antennas & Propagation*(2018).
- [18] C. Li, J. Zhou, C. Guo, H. Son, G. Wu, M. Obaidat, Tsca: a temporal-spatial real-time charging scheduling algorithm for on-demand architecture in wireless rechargeable sensor networks. *IEEE Transactions on Mobile Computing*(2018).
- [19] K. Chau, I. W. H. Ho, Z. Situ, C. Liew, J. Zhang, Effective static and adaptive carrier sensing for dense wireless csma networks. *IEEE Transactions on Mobile Computing* 16(2), 355-366(2017).
- [20] F. Long, N. Xiong, A. V. Vasilakos, L. T. Yang, F. Sun, A sustainable heuristic QoS routing algorithm for pervasive multi-layered satellite wireless networks. *Wireless Networks* 16(6), 1657-1673 (2010).
- [21] H. Liang, J. Zou, K. Zuo, M. J. Khan, an improved genetic algorithm optimization fuzzy controller applied to the wellhead back pressure control system. *Mechanical Systems and Signal Processing* 142(1) ,106-114 (2020).
- [22] H. Liang, J. Zou, Z. Li, M. J. Khan, Y. Lu, Dynamic evaluation of drilling leakage risk based on fuzzy theory and PSO-SVR algorithm. *Future Generation Computer Systems* 95(4),454-466 (2019).
- [23] J. Li, N. Xiong, J. H. Park, C. Liu, M. A. Shihua, S. Cho, Intelligent model design

of cluster supply chain with horizontal cooperation. *Journal of Intelligent Manufacturing* 23(4), 917-931 (2012).

- [24] W. Guo, N. Xiong, A. V. Vasilakos, G. Chen, C. Yu, Distributed k-connected fault-tolerant topology control algorithms with PSO in future autonomic sensor systems. *International Journal of Sensor Networks* 12(1), 53-62 (2012).
- [25] Z. Liu, B. Hu, Y. Zhao, L. Lang, H. Guo, K. Florence, S. Zhang . Research on Intelligent Decision of Low Carbon Supply Chain Based on Carbon Tax Constraints in Human-Driven Edge Computing. *IEEE ACCESS* 8(3), 48264-48273 (2020).
- [26] C. Xu. A novel recommendation method based on social network using matrix factorization technique. *Information processing & management* 54(3), 463-474 (2018).
- [27] L. Dong, Q. Guo, W. Wu, Speech corpora subset selection based on time-continuous utterances features. *Journal of Combinatorial Optimization* 37(4), 1237-1248 (2019).
- [28] W. Wei, K. Qiao, J. Nowak, M. Scherer, M. Woźniak, Accurate and fast URL phishing detector: A convolutional neural network approach, *Computer Networks*. 178, 107275(2020).

Competing interests

declares that he has no conflict of interest.

* Research involving human participants and/or animals

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

* Informed consent

All authors agree to submit this version and claim that no part of this manuscript has been published or submitted elsewhere.

Funding

Education Science Planning Office of Hunan Province (Approval No. XJK19ciw004)

Authors' contributions

Fuxing Ma wrote the entire article.

Acknowledgements

Education Science Planning Office of Hunan Province (Approval No. XJK19ciw004)

Figures

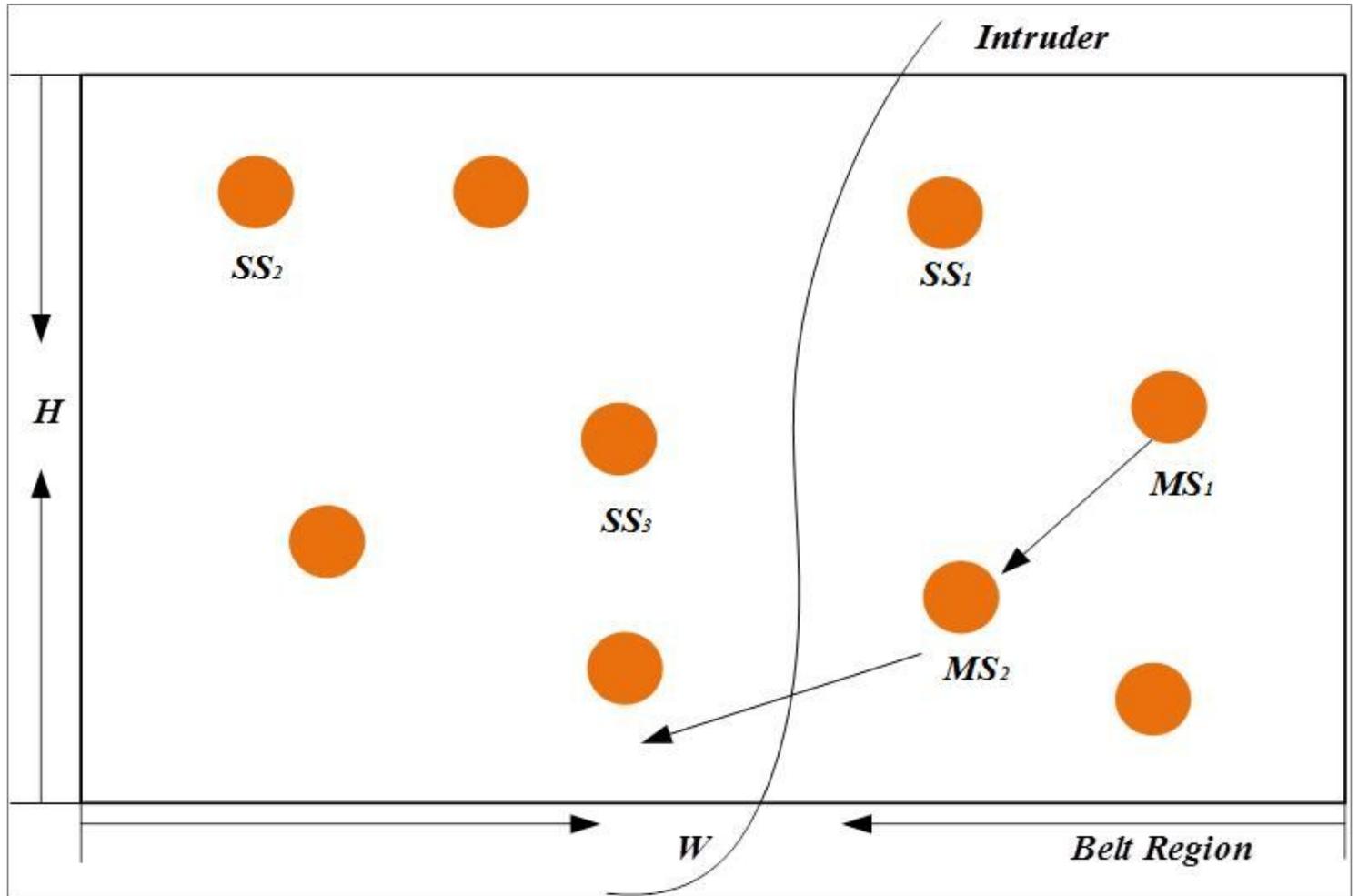


Figure 1

Schematic diagram of wireless sensor node intrusion and scene detection

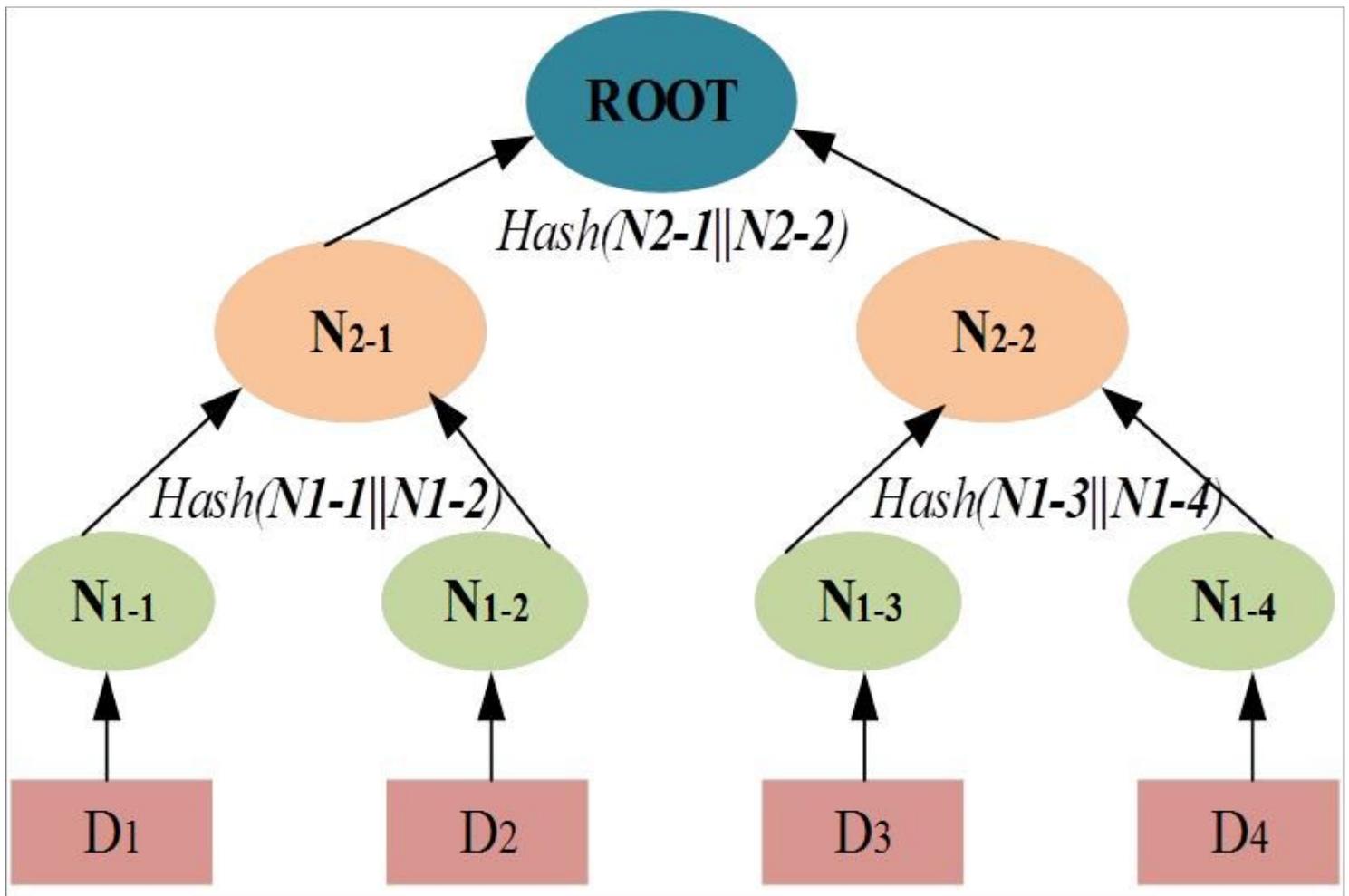


Figure 2

Schematic diagram of the authentication path of the Merkle Hash tree

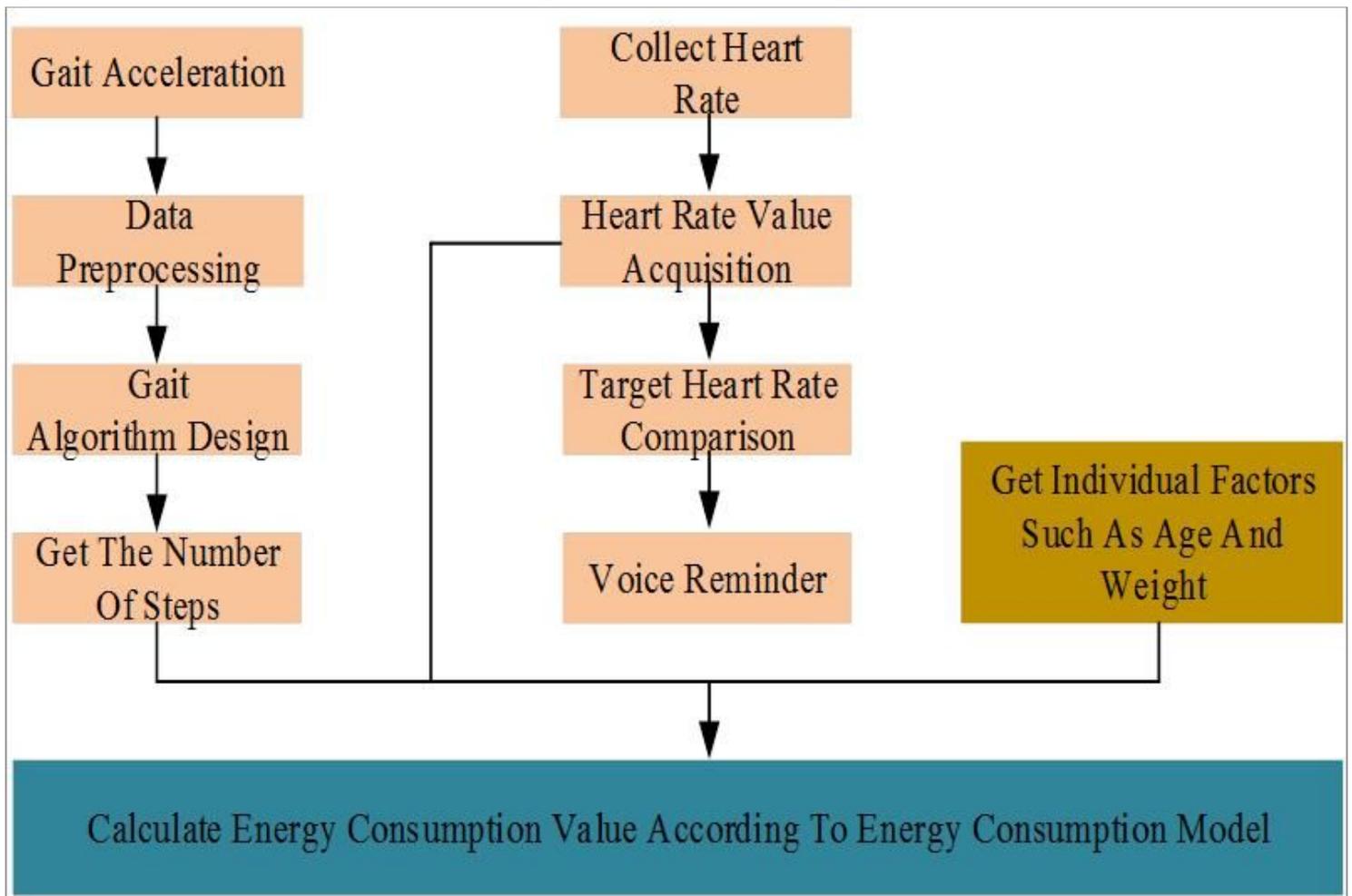


Figure 3

Frame diagram of running training assistive technology system

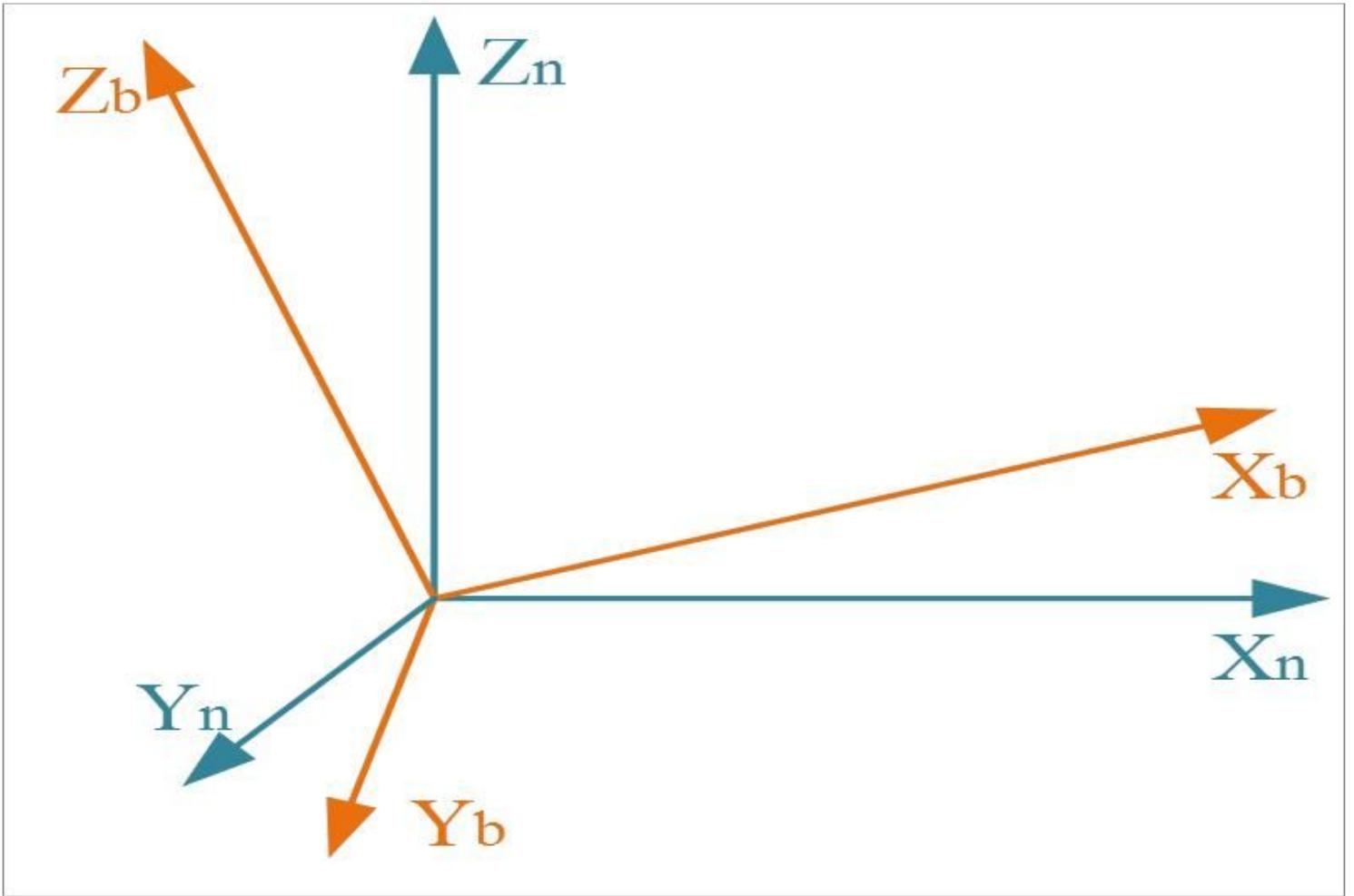


Figure 4

Posture coordinate system $O-X_bY_bZ_b$, Geographic coordinate system $O-X_nY_nZ_n$

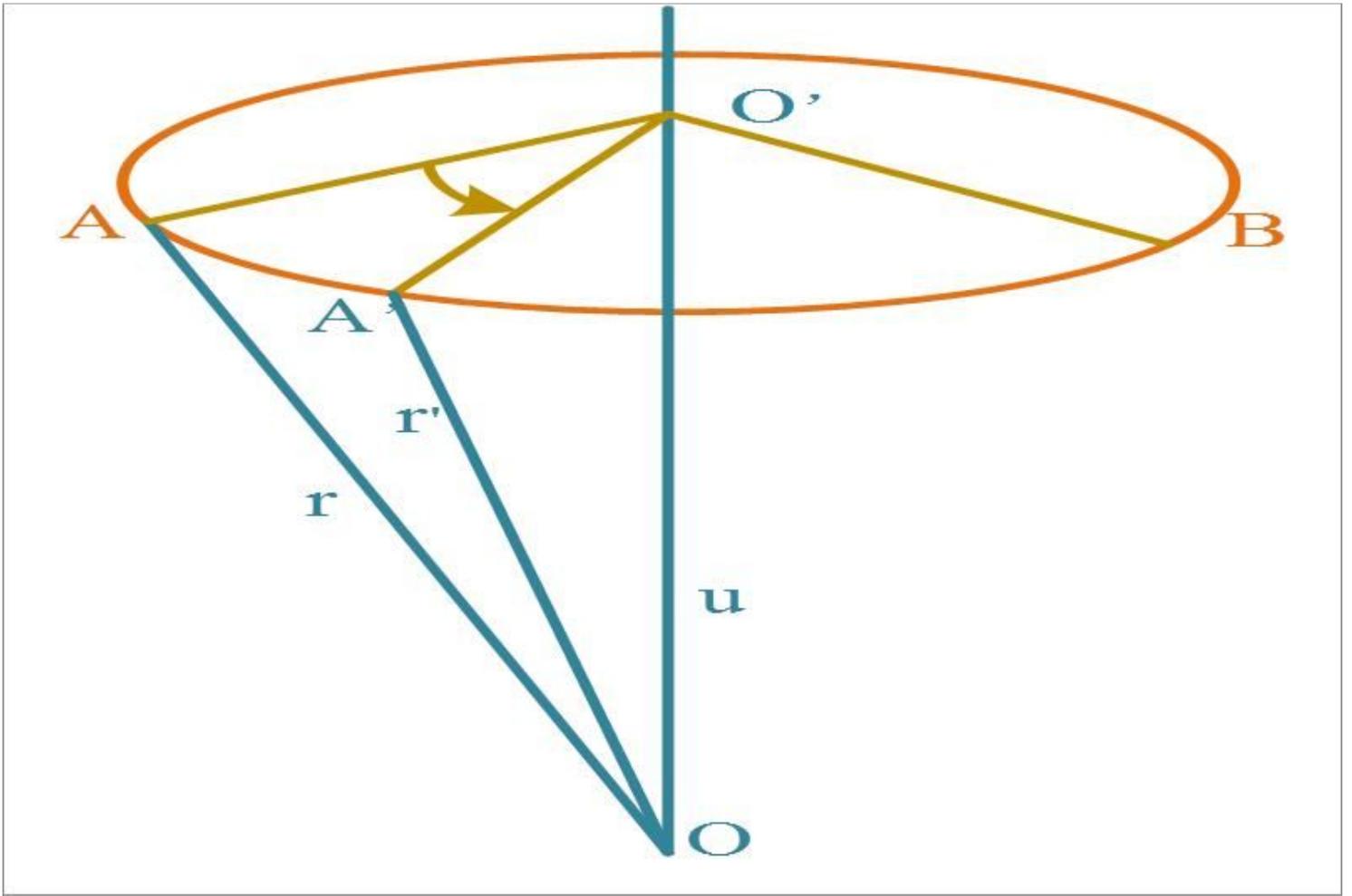


Figure 5

Schematic diagram of equivalent conversion effect of coordinate system

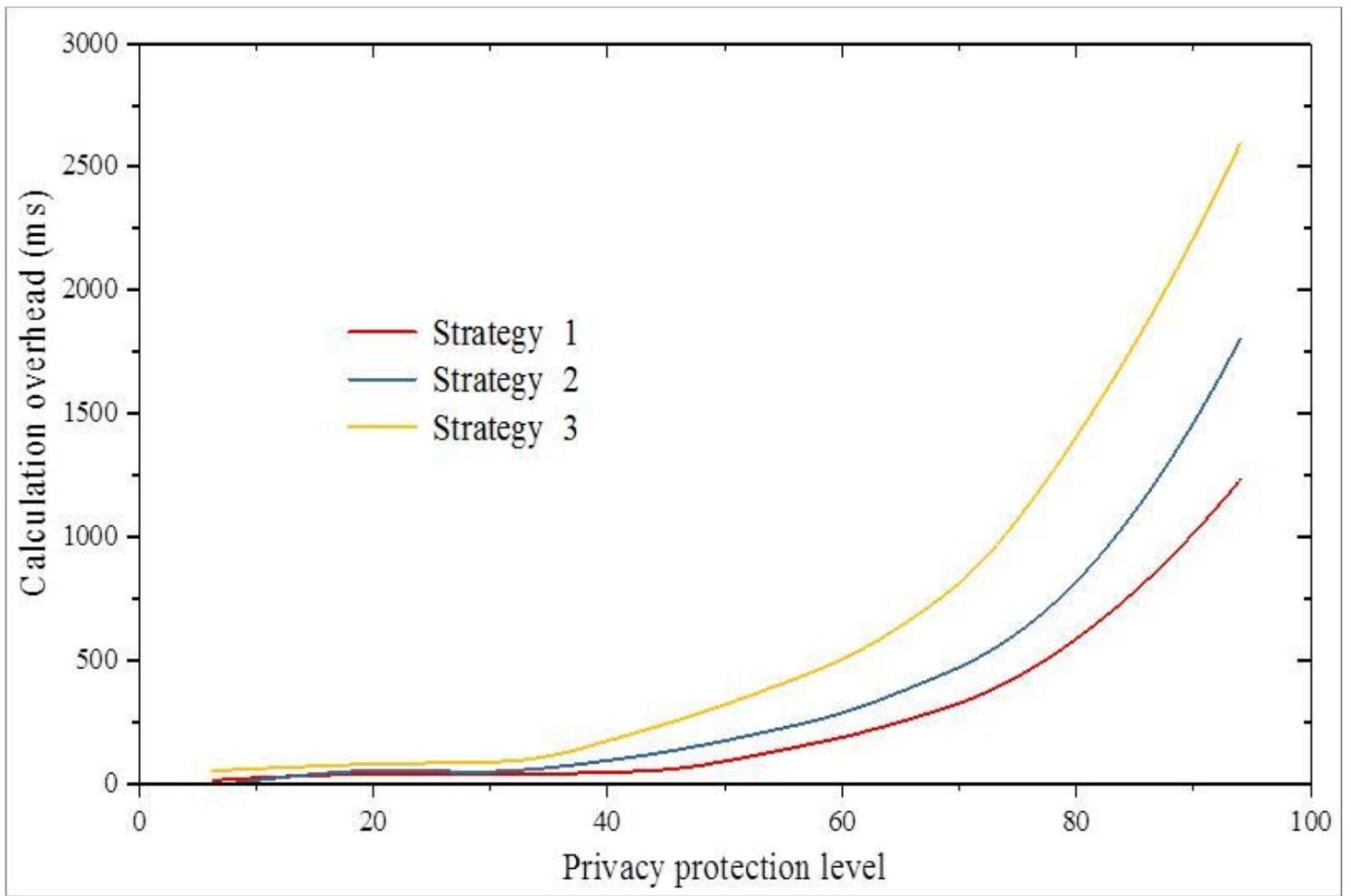


Figure 6

The privacy protection level of the blockchain and the impact of computational overhead-initialization phase

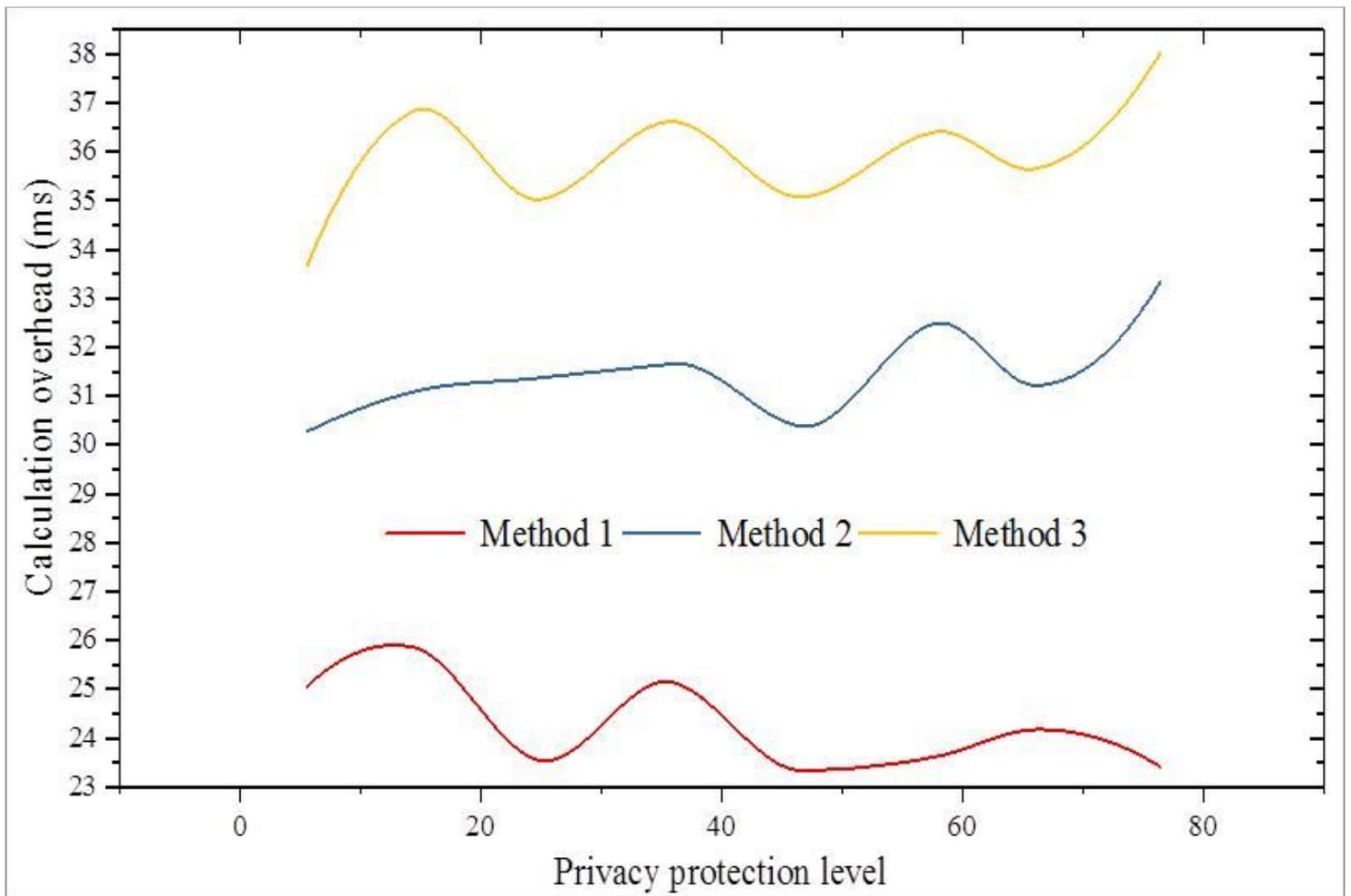


Figure 7

Blockchain protection level and the impact of computational overhead-location recording stage

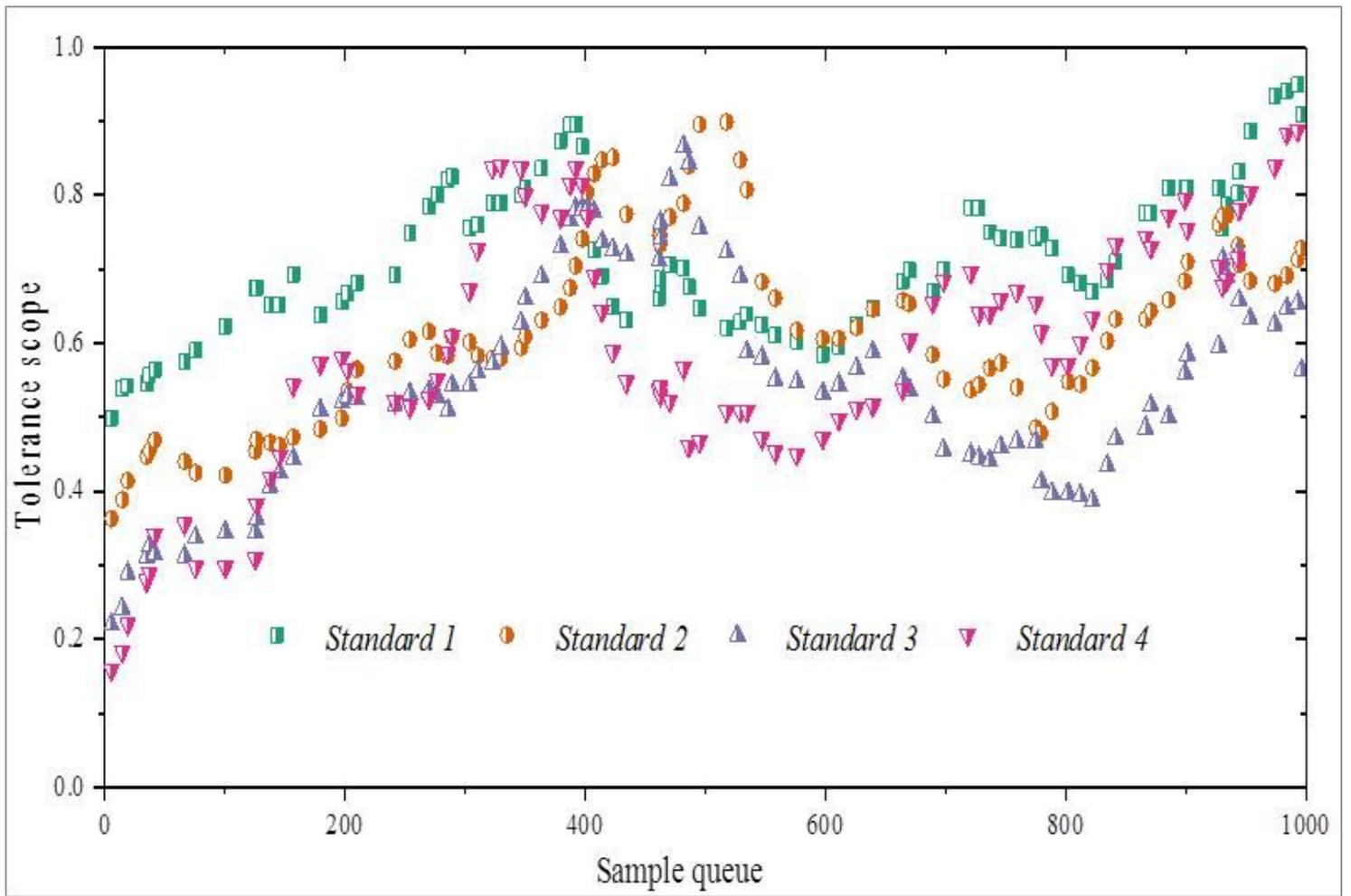


Figure 8

Comparison results of running training efficiency based on wireless sensing