INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Critical Infrastructures

ISSN online: 1741-8038 - ISSN print: 1475-3219
https://www.inderscience.com/ijcis

Game of life-based critical security key mechanism infrastructure in internet of things

A. Anandhavalli, A. Bhuvaneswari

DOI: 10.1504/IJCIS.2025.10060623

Article History:

Received:	11 May 2023
Last revised:	25 June 2023
Accepted:	27 June 2023
Published online:	15 January 2025

Game of life-based critical security key mechanism infrastructure in internet of things

A. Anandhavalli* and A. Bhuvaneswari

Department of Computer Science,
Cauvery College for Women (Autonomous),
Trichy, Tamil Nadu,
620018, India
and
Affiliated to: Bharathidasan University, India
Email: anandhavalli.ca@cauverycollege.ac.in
Email: bhuvaneswari.it@cauverycollege.ac.in
*Corresponding author

Abstract: Modern technology's blessing, the internet of things (IoT), has made remote monitoring and automation a reality. IoT devices are now the most economical option for wireless sensor networks. These gadgets were created with a specific purpose; therefore, computing power and power sources are restricted to meet that need. Due to power limitations, providing security for this type of network is a real issue. The game of life-based security key mechanism (GLSKM) technique is designed to leverage more low-level hardware bitwise operations during the key generation and exchanging phase instead of more computationally integrated energy-starving activities. This work presents two modules: the game of life-based key exchange mechanism and the random seed and iteration limit selector. Both modules are built to use simpler bitwise hardware-targeted instructions to achieve minimal power consumption without sacrificing security. The GLSKM approach also recognises the network's overall performance.

Keywords: energy efficient; internet of things; IoT; game of life; security key exchange; wireless sensor networks; WSNs.

Reference to this paper should be made as follows: Anandhavalli, A. and Bhuvaneswari, A. (2025) 'Game of life-based critical security key mechanism infrastructure in internet of things', *Int. J. Critical Infrastructures*, Vol. 21, No. 1, pp.44–69.

Biographical notes: A. Anandhavalli pursued a Master's in Computer Application from the Bharathidasan University in 2003. She is pursuing her PhD and working as an Assistant Professor in the Department of Computer Science at the Cauvery College for Women, Trichy, Tamil Nadu, India. She is a life member of ISSE. Her main research work focuses on the internet of things. She has 16 years of teaching experience.

A. Bhuvaneswari completed her Master's in Computer Science and Master of Philosophy in Computer Science in 2002 and 2005, respectively. She also completed his Doctorate in Computer Science in 2015. She has around 21 years of academic experience and ten years of research experience in computer science. Currently, she is working at the Cauvery College for Women (under the Affiliation of Bharathidasan University), Trichy, Tamil Nadu, India. She

has published several papers in international journals and conferences related to computer science. Her area of interest is mobile communication and the internet of things.

1 Introduction

Wireless sensor networks (WSN) are the backbone of environmental monitoring and smart city development (Lanzolla and Spadavecchia, 2021). Responsible resource conservation is the need of time to sustain the green earth. WSN is inevitable in remote sensing and natural resource monitoring such as soil, freshwater (Lloret et al., 2021) and mineral ingestion (Fascista, 2022). Conventional Wireless sensor nodes are prone to several stipulations, such as communication hardware discrepancy, higher implementation cost, vulnerable to simple attacks, retard communication speeds, high energy consumption, static network topology, inferior mobility, lack of scalability and outrageous manual dependency in configuration (He et al., 2021). The introduction of IoT made a major revolution in the wireless sensor node manufacturing industry. The combination of sensor and IEEE802.11 b/g/n-based IoT connectivity is a game changer in WSN technology (Huang et al., 2021; Ghayvat et al., 2015; Ullo, 2020). The communication frequency bandwidth uniformity of the IoT devices has a huge benefaction of greater compatibility between nodes and swifter communication speeds to the WSN technology (Rani et al., 2020; Adame et al., 2021). This evolution provides an opportunity to connect every IoT device with almost every other connectable smart device through edge, fog and cloud computing (Santi et al., 2022).

The proposed work and the motivation is the digital age of things is an exciting new concept that makes it possible for electrical gadgets and sensors to communicate with one another over the internet to make our lives easier. IoT uses smart gadgets and internet connectivity to offer creative answers to problems faced by businesses, governments, and both public and private sectors worldwide. IoT is steadily growing in importance and pervasive throughout our daily lives (Khan et al., 2019). As a whole, IoT is a technological advancement combining a wide range of smart systems, frameworks, intelligent devices, and sensors (Sharma and Sharma, 2021). Additionally, it uses nanotechnology and information technology to achieve previously unthinkable levels of storage, sensing, and computing speed. Substantial studies have been conducted to demonstrate the probable efficacy and practicality of IoT changes (Rani et al., 2021). They are available in academic papers and press reports on the World Wide Web and in printed publications. It could be used as a pre-work before creating original, inventive company concepts while considering security, assurance, and scalability (Khasawneh et al., 2021).

The uniformity in the communication frequency and the IEEE 802.11 protocol constraint leads to the vulnerability towards modern-day network attacks as an adverse effect (Shahidinejad et al., 2022). As a result, there is a crucial requirement to invent upgraded security protocols for IoT network environments persistently (Mast et al., 2021). The prevalent challenges in IoT security designs are eliminating default password Brute-force attacks, dynamic update testing, malware protection, and sustaining network performance and lifetime. Providing high security and maintaining energy consumption

in control is an exceptionally complicated task (Aldabbagh et al., 2022). High-security protocols use more complicated mathematical calculations, which devour more power. The GLSKM work is targeted to replace complicated mathematical calculations with processor-friendly bitwise hardware operations to preserve the energy of a battery-powered IoT device.

IoT aims to connect hardware to the internet so that anybody, anywhere, at any time, can access it. The internet of things (IoT) is enabling extraordinary uses such as intelligent public transport, smart healthcare, smart houses, smart cities, etc. by way of seamless integration and smart items like washers, dryers, microwave ovens, metres, vehicles, phones, fridges and freezers and devices for medicine. IoT and safety concerns are increasing due to the widespread use of IoT devices. Furthermore, a lot of unsecured gadgets will be installed in rural areas. A hacker may take control of the devices and locate a way into the network (Priscila et al., 2023). Web servers, databases, and other storage sources could leak sensitive information to any outside the organisation, which would not only cause data loss but also threatens the confidentiality of system data, and appropriate encryption techniques will prevent such spills.

Dependent on the point-wise, shared, or environmental forms, anomalies may be found. When batch modifications are not linear, in terms of points, anomalies are used to find data points that substantially depart from the other points of evidence. It was typically used to identify fraud. Group abnormalities were found in the time series' typical themes, such as repeating patterns or shapes from multiple IoT devices. In the supply chain, delays in shipping are quite common, but if there are several delays, conducting an inquiry and a group study may be necessary. Environmental inconsistencies are noticed by considering the previous type of detail or context, such as the day of the week. Contexts are always highly distinctive to a certain domain.

2 Existing methods

Some prominent security-energy balanced security protocols are selected among the highly secure energy-starving and energy-efficient low-security protocols to make a clear evaluation comparison with the proposed method. They are a secure and efficient method to protect communications and energy consumption in IoT WSNs (Anajemba et al., 2020), compressive sensing (CS)-based secure data aggregation scheme for IoT-based WSN applications (Hussein et al., 2022), improved blowfish algorithm-based secure routing technique in IoT-based WSN (Salim et al., 2021), weighted connected vertex cover-based energy-efficient link monitoring for WSNs towards secure IoT (Alotaibi, 2021), a neuro-fuzzy-based IDS for internet-integrated WSN (Dagdeviren, 2021), lightweight security algorithm on PMIPv6 protocol for IoT-based WSNs (Paul et al., 2021) and masked location-based key exchange mechanism for IoT nodes (Anandhavalli and Bhuvaneswari, 2019). A concise study about the methodologies used, advantages and limitations of these methods are carried out in this section.

2.1 A secure and efficient method to protect communications and energy consumption in IoT WSNs (MLEACH)

Hussein et al. (2022) proposed a key distribution and management modification procedure to the existing LEACH to achieve a fast, reliable, secure IoT-based WSN

environment. The Elliptic curve cryptography-based key establishment method is used in the MLEACH method. MLEACH is designed to protect against jamming attacks, node capturing attacks, Sybil attacks, sinkhole attacks, warm hole attacks and node ID clone attacks. The integration of ECC into the conventional LEACH protocol is mended in the MLEACH work. Specialised algorithms for cyclic ECC key generation and distribution are presented in MLEACH work. A MATLAB-based simulation is performed to measure different parameters such as time consumption vs. number of threats, number of rounds vs. dead node count, time consumption for key update round, number of hops per round, and node failure vs. number of rounds. Integrating a specialised ECC key generation method with LEACH is the stated novelty of MLEACH work. The performance between the LEACH and MLEACH is evaluated during the experiments conducted in work. The computational resource dependency of ECC is much higher during the exponent calculations, which may trigger abnormal power usage of the limited resource nodes. The entire paper discussed security, which is not measured during the simulation. Faster key generation is the advantage of MLEACH work. In contrast, missing evaluation for important network parameters such as throughput, delays, packet delivery rates and security are the identified limitations of this work.

2.2 Compressive sensing-based secure data aggregation scheme for IoT-based WSN applications (CSSDA)

Salim et al. (2021) introduced CSSDA work in 2021 to improve the IoT-based WSN network quality by integrating the CS-based data collection scheme with ECC. CSSDA work is designed to retain all advantages of CS-based data collection schemes and eliminate the disadvantages by amalgamating ECC with it. Key generation, CS-key exchange, data compression with CS encryption, data aggregation and ECC encryption and CS key regeneration are the phases of CSSDA work. A dedicated pseudo-random key-based key-sharing method is introduced in CSSDA work. Several CS-based data collection schemes targeting attacks, such as Ciphertext only attacks, chosen plaintext attacks and known plaintext attacks, are diminished by incorporating ECC-based key generation in CSSDA work. A simulation for a 100 m × 100 m area with 100 sensor nodes is used to evaluate the performance of CSSDA work. Parameters such as energy efficiency, alive nodes count and network lifetime are measured during the simulation. There is no specific practical measurement methodology used for security in CSSDA work. Improved energy efficiency is noted as the advantage of CSSDA work, whereas missing security analysis and network performance parameters can be the limitations.

2.3 Improved blowfish algorithm-based secure routing technique in IoT-based WSN (CM-MH)

Alotaibi (2021) introduced a work in which crossover mutated marriage in honeybee (CM-MH) algorithm is used for optimal path selection and encryption in IoT-based WSNs. CM-MH is used to improve the data transfer performance of the network. An improved blowfish algorithm is used to ensure the security of the CM-MH work. The CM-MH work considers various network performance factors such as energy, Euclidean distance between the data source and destination, communication delays and the trust index. A dedicated objective function is formed to achieve the shortest optimal path

during the routing phase. The improved blowfish algorithm in CM-MH work guards the data transmission. The experimental setup of CM-MH consists MATLAB simulation tool and a ThinkSpeak environment. The performances of the genetic algorithm, firefly algorithm, particle swarm optimisation algorithm and marriage in honeybee optimisation algorithm are compared with CM-MH work. Evaluation metrics such as throughput, communication cost, encryption time and decryption time are measured during the simulation.

Achievement of higher throughput and lower communication cost is the advantage of CM-MH work. In contrast, the rigidity of the improved blowfish algorithm is not up to the mark in security aspects, observed as the limitation of this work.

2.4 Weighted connected vertex cover-based energy-efficient link monitoring for WSNs towards secure IoT (WCVC-HGA)

Dagdeviren (2021) introduced a WCVC-based hybrid genetic algorithm (HBA) in 2021 to improve communication security in an IoT environment. Most network improvements are carried over in WCVC-HGA by calculating the minimum vertex cover using graph theory. The WCVC-HGA model ensures that connection between the monitor nodes by introducing a subgraph with node weights. A greedy heuristics approach is used to build the HGA algorithm, chromosome repair algorithm, monitor node set algorithm, chromosome minimisation algorithm, and redundancy find the algorithm of WCVC-HGA work. The implementation of the CVC-HGA work is done in Java programming language. The experiments are performed using randomly generated datasets. Graph weight and monitor count are measured during the experiments. By observing the experimental results, it is understood that the performance of energy efficiency and communication cost of the WCVC-HGA method is more optimised than other methods in the comparison. Achievement of higher throughput and lower communication delays is the advantage of the work. The security aspects of the WCVC-HGA are not measured using a network-based simulation, which is the perceived limitation.

2.5 A neuro-fuzzy-based IDS for internet-integrated WSN (NFIDS)

Paul et al. (2021) introduced a fuzzy-based intrusion detection method in 2021 exclusively for heterogeneous IoT-based WSN environments. NFIDS work is centric on the limited computational resource of tiny IoT nodes and their power-constrained working environment. Therefore, the authors of NFIDS define a fuzzy-based intrusion detection procedure for different approaches, such as centralised approach, gateway-based approach and topology-based integration approach. Different characteristics of IoT-based WSNs, such as robustness, user authentication, authorisation, secure communication medium, sensor node hardware properties, network redundancy, protocol optimisations and different kinds of possible network attacks, are taken care of and discussed in NFIDS work. The attack possibilities at the physical, link, network, transport, and application layers are discussed clearly in NFIDS work. True positive and false positive rates are measured during the experiments. Achievement of low energy consumption-based security scheme is the advantage of NFIDS work, and compromised security in higher dense networks is the limitation of this work.

2.6 Lightweight security algorithm on PMIPv6 protocol for IoT-based WSNs (LSA)

Anandhavalli and Bhuvaneswari (2019) said that LSA work attempts to provide adequate security for IoT-based WSNs; thus, PMIPv6 is selected as the base protocol. The regular security authentication mechanism of PMIPv6 is overridden by a legacy media access control (MAC) address-based session key generation and Diffie-Hellman key exchange mechanism to achieve higher security without much impact on normal performance. The LSA work integrates two functional modules they are MAC address XOR key exchange authentication (MAXOR) and legacy random number generator (LRG). The MAXOR module provides abundant obfuscation of the MAC address-based key generation process without involving complicated power-consuming mathematical equations. Most the processes of MAXOR take advantage of single-cycle hardware operations; thus, the key generation phase of LSA work runs seamlessly even in resource-constrained devices with less power consumption. The LRG module introduces a legacy seed-based random number generator to share the nodes' keys and initiate communication accordingly.

The industrial standard OPNET Network Simulator is used to perform the experiments. Vital network metrics such as throughput, latency, end-to-end delay, packet delivery rate, energy consumption and security are measured during the experiments. The evaluation results show that the performance of LSA is well suited for secured IoT-based WSN environments, which is the prominent advantage of this work. Security is measured as integer quantities that lack high precision variations in floating values, which is observed as the limitation of LSA work.

2.7 Masked location-based key exchange mechanism for IoT nodes (MLKEM)

Anandhavalli and Bhuvaneswari (2019) said that MLKEM work is introduced to bring a balance between the security and energy efficiency of the nodes in a heterogeneous IoT-based WSN. The main theme of MLKEM work is based on dual rosenberg pairing location masker (DRPLM), fuzzy computational complexity determiner (FCCD) and Miller's Elliptic curve key exchange procedure (MECKEP) modules. A set of dedicated hash functions are introduced in MLKEM for bitwise diffusion operations, which are responsible for the obfuscation of location and hardware MAC identification of a node. The Geo-Hash function encodes the latitude and longitude location information of a node, the MAC-Hash is used to encode the hardware address of a node, and the DRPLM binds the two encoded values into a single one. The FDDC module determines the customary computational ability between two nodes with different hardware configurations. Based on the FCCD equation, the number of bits for the communication is determined and used to establish the communication. OPNET network simulator is used to carry on the experiments, and the results are obtained regarding throughput, communication delays, energy consumption and security. Based on the experimental results, it is observed that the performance of MLKEM work is better than the compared methods – which are the advantage of this work. Missing higher precisions in security measurement is known as the limitation of MLKEM work.

An outline of the existing works, methodologies used, advantages and limitations are put forward in Table 1.

Table 1 Existing works key points

Author	*Work*	*Methodology*	*Advantages*	*Limitations*
Hussein et al. (2022)	A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks	ECC+LEACH	Limited resource consumption	Low performance, security
Salim et al. (2021)	Compressive sensing-based secure data aggregation scheme for IoT-based WSN applications	Compressive sensing, ECC	Energy efficiency	Network performance
Alotaibi (2021)	Improved blowfish algorithm-based secure routing technique in IoT-based WSN	Crossover mutated marriage in honeybee	Higher throughput, lower communication delays	Security
Dagdeviren (2021)	Weighted connected vertex cover-based energy-efficient link monitoring for wireless sensor networks towards secure internet of things	Weighted connected vertex cover hybrid genetic algorithm	Higher throughput, lower communication delays	Security
Paul et al. (2021)	A neuro-fuzzy-based IDS for internet-integrated WSN	Neuro-fuzzy-based IDS	Low energy consumption	Security
Anandhavalli and Bhuvaneswari (2019)	Lightweight security algorithm on PMIPv6 protocol for IoT-based wireless sensor networks	MAXOR-LRG	High performance	Missing precision in security measurement
Anandhavalli and Bhuvaneswari (2019)	Masked location-based key exchange mechanism for IoT nodes	Dual Rosenberg pairing location masker	High performance	Missing precision in security measurement

3 Related works

A simple low-latency real-time certifiable random number generator (LRCRNG) and entanglement in the quantum game of life concepts are exerted as the central cores of the proposed MLKEM method. A brief interpretation of the random number real-time random number generator and quantum entanglement in the game of life concepts is immensely required to explain the functionalities of proposed MLKEM modules. This section is committed to elucidating the concepts mentioned above. The vital infrastructure of water supply, heating, water conservation, and other systems is included in industrial IoT security. Studying industrial internet security weaknesses is crucial to lowering the likelihood of industrial internet security accidents because it will have severely negative impacts once the network is hacked. To create a modern, digital economy, it is required to establish a nationally aware intelligent security command

platform and to encourage the high-quality growth of a smart society through the secure game of life concepts technology (He et al., 2021). It has been challenging for traditional risk management theories to offer useful decision-making advice for the security protection of game-of-life concepts for industrial IoT (Adame et al., 2021; Santi et al., 2022; Shahidinejad et al., 2022). Based on the security needs of the MLKEM for industrial IoT, game theory is used in this study to characterise the procedure of interaction among attackers and defenders in the network. Additionally, the weakness of life cycle management's significance to the protection of the MLKEM for industrial IoT is defined; the security issues that arise during network flaws are identified and fixed, and a targeted allocation strategy for secure network safeguards resources is suggested. The novel aspect of this study is the use of game theory in analysing internet security threats, which offers fresh perspectives on how to perceive and effectively address weaknesses in MLKEM networks.

3.1 A simple LRCRNG

Random number generation is one of the vital components in key generation and cryptography. The security of the entire procedure directly depends on the randomness of the base algorithm (Anandhavalli and Bhuvaneswari, 2019). A generic random number generation algorithm is in Algorithm 1.

Algorithm 1 Random number generation

Step 1	Let $f(b)$: be the target distribution
Step 2	Let $F(b)$ be a cumulative distribution function for $f(b)$:
Step 3	$\int_{-\infty}^{b} f(b')db'$ with the condition $0 = F(-\infty) \le F(b) \le F(\infty) = 1$
Step 4	For a random number c, the uniform distribution as the probability density is $F(b) = c$
Step 5	compute $b = F^{-1}(c)$ where b is the randomly selected distribution from distribution $F(b)$
Step 6	Repeat step 4 for successive numbers.

This algorithm can generate random numbers based on the initial random number c, considered a seed.

3.2 Entanglement in the quantum game of life

Game of life is a cellular automation game devised by the British mathematician John Horton Conway. The playground is set to be an infinite two-dimensional orthogonal grid of square cells. The idea of a critical security key mechanism was put forth many years ago, and it is a technology created by researchers from the space industry that compares digital objects with actual ones. The digital models can be used to alter, simulate, and evaluate the underlying system governed by physics since they are based on the game of life-based critical security key mechanism infrastructure. A vital security key mechanism network platform can be built by implementing the security key technique to produce a virtual representation of real network services. The essential security key mechanism network platform can assist the network in achieving low-cost trial-and-error, wise decision-making, and high-efficiency innovation through real-time communication

and mutual impact on the network's physical structure and the twin network (He et al., 2021). Critical security key mechanisms are utilised extensively in manufacturing, industry, and other sectors. Vital security key mechanisms are based on the real-time operation process of tangible things and manufacturing systems to improve the accuracy of information analysis and reconfiguration. They are a virtual manifestation of physical entities' planning, building, and upkeep. IoT and critical security key mechanism growth in technology have increased due to falling technological costs.

The possible cell states are set to be binary, in which 0 refers to dead, and 1 refers the live. A user can set the initial state of the cells in the playground at time t and initiate the iterations. Every cell can interact with its immediate nearby neighbour in horizontal, vertical and diagonal directions. A set of transition rules are defined to determine the state of the cells during successive iterations. The transition rules are as below.

Rule 1 Any live cell with less than two live neighbours dies by underproduction.

Rule 2 Any live cell that has two or three neighbours sustained in the live state in the next iteration

Rule 3 Any live cell with more than three neighbours will die of overpopulation

Rule 4 Any dead cell with exactly three numbers of neighbours will become life by regeneration

Though there are only four simple rules those define the way of the game of life, there are several possibilities of the future generation evolutions with different patterns with strange or entangled behaviour. The endless possibilities of generating future generations make the game of life concept harder to define in a single polynomial or by machine learning methodologies. The set of four rules can generate numerous mystical patterns, divided into three major categories: still life patterns, oscillators and spaceships. still, the life pattern category consists of several patterns such as boat, block, bee-hive, loaf and tub. The oscillator category has blinker, beacon, pulsar, toad and penta-decathlon patterns. The spaceships category consists of glider, lightweight spaceship, middleweight spaceship and heavyweight spaceship patterns. Therefore, the prediction of the n^{th} generation for the given initial generation is not yet accurately achieved by any methodology other than following the predefined rules and iterations.

4 Proposed method

Game of life-based security key mechanism (GLSKM) work integrates the random seed and iteration limit selector (RSILS) module and the game of life-based key exchange mechanism (GoLKEM). The detailed descriptions of these modules are elucidated unambiguously in this section. The motivation behind this study is IoT networks are made up of inexpensive detectors deployed across a large area in three different formats: hierarchical networks with many nodes, unmanaged connections, and distributed networks powered by the technology known as the blockchain. These IoT networks' sensors ensure the network's overall effectiveness.

Real-world datasets include examples that differ from one another and are referred to as abnormalities. The anomaly identification process aimed to pinpoint certain criteria whose activity has been found to be abnormally connected to normal nodes. Anomalies

can have various reasons, including data loss, identifying fraudulent activity, and detecting intrusions system.

There are three levels in a channel-wise convolution: an input layer, concealed layers, and an output layer. The hidden layers in a channel-wise convolution contain one or more convolutional layers. This typically contains a layer that does a dot product of the input matrix of the layer with the convolution kernel. The activation function of this product, which is typically the inner product, is frequently convolution. The convolution procedure develops a feature map as the convolution kernel moves across the given input matrices for the layer, adding to the input of the following layer. Following this are further layers like normalising, pooling, and fully interconnected layers. A constantly changing network of billions or trillions of wirelessly identified 'things' will be created by the IoT, including advancements from ideas like the IoT, widespread computing, and intelligent surroundings. By requiring full connectivity and computing capabilities among things and integrating the features of ongoing communication, identification, and engagement, the IoT hosts the concept of omnipresent computing and ambient intelligence, strengthening both. Combining several ideas and technical elements – including pervasive networks, device downsizing, communication via mobile devices, and novel formats for business processes – the IoT unifies the digital and physical worlds. The IoT will result in measurable savings for companies, including better life-cycle management, high-resolution asset and product management, and improved enterprise collaboration. Many of these advantages are made possible by using distinct verification for individual things and searching and finding services, allowing each thing to interact separately, accumulating a record of one's interactions and activities over time.

Each neuron in a typical convolution receives input from a few different places in the preceding layer. Each neuron in a convolution layer only gets input from a small region of the preceding layer, known as the network's receptive field. The area is typically square. In contrast, the entire prior layer is the receptivity field in a fully linked layer. As a result, compared to earlier layers, each neuron in a convolutional layer receives information from a greater area of the input. This is caused by repeatedly using convolution, which considers both the value of an individual pixel and the pixels around it. When utilising enlarged layers, the receiver field's pixel count stays constant, but when integrating the effects of many layers, the field becomes sparser as its dimensions increase.

4.1 Random seed and iteration limit selector

Due to the heterogeneity of an IoT network, several devices with various hardware capabilities may be present. Not every gadget is equally capable of handling the same computational tasks. In IoT nodes, the disparity in computational power used to be enormous. Different types of devices are devoted to various tasks in an IoT network. As a result, the performance and cost of the computational capabilities are kept in balance. For instance, a sensor node's function measures environmental and physical factors for which more advanced computational power is unnecessary. However, a data processing node needs a lot of computing power to handle large amounts of data. A biased node, in higher computational device zones, key agreement procedures could not guarantee enough security or might exhaust a low-powered, compact node. The RSILS module introduces a smooth bridging procedure to enable communication between two devices of various

categories. Conventional computational power calculations use different hardware characteristics of a device, such as a processor frequency, onboard installed memory, storage, etc. In RSILS, a simple count-based procedure is introduced to get the computational power index of a node within a second. The computational power index ρ calculation algorithm of RSILS is given in Algorithm 2.

Algorithm 2 Computational power index calculator

Input:	
Output: Computational power index	
Step 1	Let C be the set of counters $\{c_1, c_2, c_3\}$ with initial values as 0 s
Step 2	For $i = 1, 2, 3$
Step 3	Initiate timer interrupt for 300 ms
Step 4	Increment c_i by 1 until the timer event ends
Step 5	End for
Step 6	Return computational index $\rho = \dfrac{\sum_{i=1}^{3} c_i}{3}$

As the cluster head knows the computational power indexes of all the devices during the registration phase, the maximum achieved power index $\rho_{\max}$ is computed using equation (1).

$$\rho_{\max} = \max\left(\rho_1, \rho_2, \ldots, \rho_n\right) \tag{1}$$

In which n refers to the number of nodes in the cluster.

Based on the computed power index of every node, the node will be classified into one of the five different categories, such as very low, low, medium, high and very high, by using equation (2).

$$NodeType = \begin{cases} Very\ low & \text{if } \rho_x > \dfrac{1}{5}\rho_{\max} \\ Low & \text{if } \rho_x > \dfrac{2}{5}\rho_{\max} \text{ and} \leq \dfrac{2}{5}\rho_{\max} \\ Medium & \text{if } \rho_x > \dfrac{2}{5}\rho_{\max} \text{ and} \leq \dfrac{3}{5}\rho_{\max} \\ High & \text{if } \rho_x > \dfrac{3}{5}\rho_{\max} \text{ and} \leq \dfrac{4}{5}\rho_{\max} \\ Very\ high & \text{otherwise} \end{cases} \tag{2}$$

where ρ_x is the computation power index of x^{th} node.

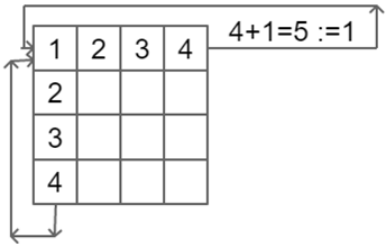
Permitted grid sizes, minimum number of iterations and maximum number of iterations for the node categories are given in Table 2.

The grids are considered circular; thus, any row or column value that exceeds the maximum limit will enter the beginning row or column accordingly, as illustrated in Figure 1.

Table 2 Permitted key sizes and iteration ranges

Node category	*Grid size*	*Minimum number of iterations*	*Maximum number of iterations*
Very low	16	12	24
Low	32	24	36
Medium	64	36	48
High	128	48	60
Very high	256	60	72

Figure 1 Rotational square grid



4.2 Game of life-based key exchange mechanism

The GoLKEM module has a key generation phase and a key exchange phase. The security keys are generated based on the output of RSILS during the key generation phase, and the keys are securely exchanged between the sender and the receiver during the key exchange phase.

4.2.1 Key generation phase

The purpose of the wireless sensor node is to detect a physical parameter and to provide corresponding electronic signals. Therefore, every sensor node will contain several internal electronic components such as analogue-to-digital converter (ADC), digital-to-analogue converter (DAC), operational amplifiers (Op-Amp), etc. A standard Op-Amp-based integrator (Cang et al., 2021) is given in Figure 2.

The integral process receives V_{in} as the input which will be integrated to value V_{out} based on equation (3)

$$V_{out} = \frac{1}{R_1 C_F} \int_0^t V_{in} d_t \tag{3}$$

The complicated integral calculation of LRCRNG is simply configured in GoLKEM by using the internal components of a wireless sensor node to reduce the computational complexity, as in Figure 3.

A set of equations derived for the GoKEM algorithm are listed below

- Random iteration count selection:

$$i_r = (i_{\min} + R_S) \bmod i_{\max} \tag{4}$$

where i_r refers to the random iteration count, i_{min} is the minimum required number of iterations, i_{max} refers to the maximum permitted number of iterations, and R_S refers sender's random number

- Iteration count and ID masking equation:

$$x_m = R_x \oplus ID_x \tag{5}$$

where x_m is the masked number of node x, R_x is the random number, and ID_x is the registered hardware identification number of node x.

- Unmask equation:

$$R_x = x_m \oplus ID_x \tag{6}$$

An example of setting up GoLplay ground for a random number sequence is illustrated in Figure 4.

Algorithm 3 GoLKEM key exchange algorithm

Input: Grid size and iteration range (supplied by RSILS)	
Output: Establishment and exchange of private keys	
Step 1	Let S be the sender, R be the receiver, and C be the cluster head
Step 2	S selects a random number R_S using GoLKEM integrator
Step 3	S masks the random value with its id ID_S to compute S_m using equation (5)
Step 4	S initiates the communication request by sending S_m to C
Step 5	C demasks the value R_S using equation (6)
Step 6	C computes a ping token t using R_S and the receivers node id ID_R
Step 7	C pings R with t
Step 8	R computes the value of R_S using equation (6)
Step 9	R selects a random number R_R using GoLKEM integrator
Step 10	R masks the random value with its id ID_R to compute R_m using equation (5)
Step 11	R replies to the communication request by sending R_m to C
Step 12	C demasks the value R_R using equation (6)
Step 13	C computes a ping reply token t using R_R and the sender node id ID_S
Step 14	C pings S with t
Step 15	S computes the value of R_R using equation (6)
Step 16	Now both S and R compute the iterations using equation (4) till reaching R_S
Step 17	Similarly, S and R sets the R_R as the random generation seed
Step 18	S and R compute a sequence of random numbers to setup the GoL playground
Step 19	GoL final resultant matrix will be calculated by the initial GoL playground and the number of iterations
Step 20	Now both sender and receiver can communicate with the common key extracted from GoL

The random binary coded decimal (BCD) numbers are converted into binary, and in the GoL playground, all 0 s are set as dead cells, and 1 s are set to live cells. Therefore, a QR code-like pattern is generated from the input random numbers.

Figure 2 Standard op-amp-based integrator

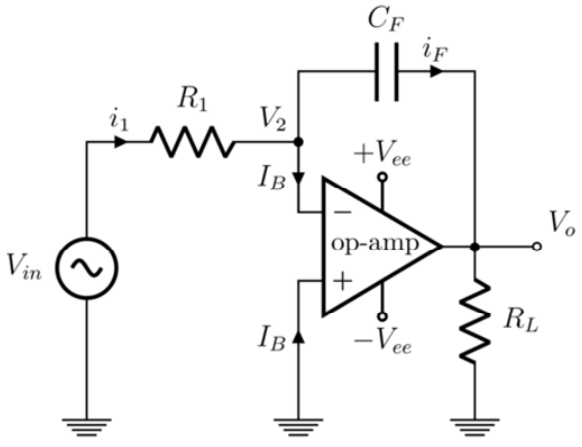


Figure 3 GoLKEM integrator (see online version for colours)

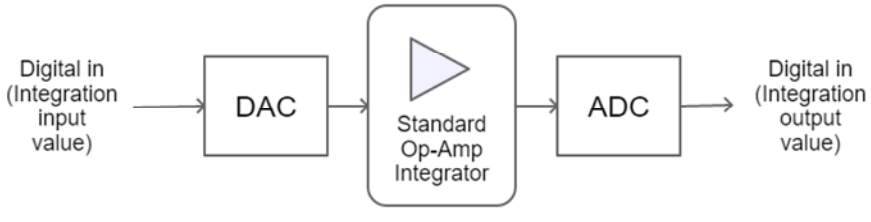
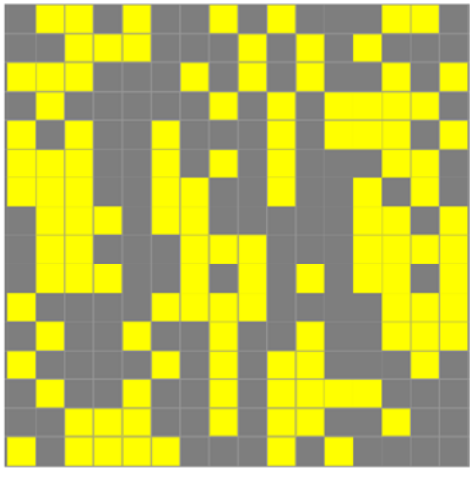


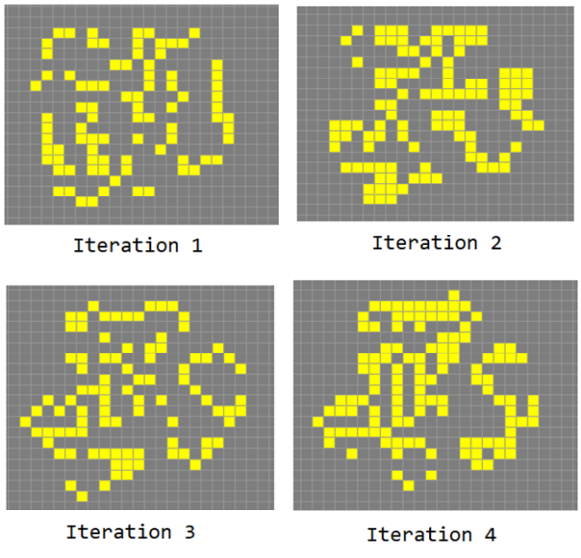
Figure 4 GoL playground setup (see online version for colours)

Random BCD	Binary
6946	0110100101000110
7150	0111000101010000
E2A5	1110001010100101
415E	0100000101011110
A45D	1010010001011101
E546	1110010101000110
E64A	1110011001001010
760D	0111011000001101
638F	0110001110001111
72AD	0111001010101101
8787	1000011110000111
4927	0100100100100111
8562	1000010101100010
4978	0100100101111000
3964	0011100101100100
BC50	1011110001010000



The iteration will be performed till the counter reaches the value of R_S. The iterative pattern changes of the initial GoL playground are illustrated in Figure 5.

Figure 5 GoL playground iterative patterns (see online version for colours)



After the iterative pattern updates, the GoL playground can be reversed to form the binary numbers and then converted to BCD to represent the keys. Since a set of keys is generated for every phase, the sender and the receiver can initialise the communication between them with the first key, and the successive keys will be taken one by one for every key revocation. Creating a set of keys process reduces the intermittent key calculation times in vulnerable attack-prone IoT-based WSN environments.

5 Experimental setup

The complete evaluation procedure is carried out based on simulations run by the commercial network simulator OPNET (Vayadande et al., 2022). In order to validate various measures, such as operational validation (Springer and Kenyon, 2021), application troubleshooting, network planning, network designing, hardware validation, protocol modelling, and traffic modelling, OPNET is capable of simulating given network components, protocols, nodes, and architectures in a real-world network environment. Using OPNET, fundamental network performance parameters for varied timestamps and varying numbers of nodes may be simulated, including throughput, communication latency, packet delivery rate, energy consumption, and security. The extensive built-in OPNET, The network module library, supports numerous cutting-edge network communication devices in the IoT and WSN categories. A network's edges can execute business logic thanks to the improved sensor and device capabilities, allowing some existing company procedures to be decentralised for better efficiency, scalability, and local decision-making.

In order to identify the first indications of issues or worsening of the condition, algorithms could be employed, for instance, to make intelligent decisions based on actual time inputs from sensors that are used to monitor the health of patients or the state of cars. The IoT suggests a symbiotic relationship between the physical and digital worlds:

physical objects have digital equivalents and virtual representations; objects acquire context awareness and can detect, interact, communicate, and share data, information, and knowledge. Based on the most recent data gathered about real things and taking into account patterns in the past information, either for the same entity or similar entities, sophisticated decision-making techniques in software applications enable the right rapid responses to physical phenomena. These open up new possibilities for meeting business needs, developing new services based on real-time data from the physical world, understanding intricate relationships and processes, handling incidents, addressing environmental degradation, keeping an eye on human activity, strengthening infrastructure integrity, and dealing with energy efficiency issues.

The IoT will unite everything, including people, groups, communities, items, products, data, services, and processes. In the IoT, networking will become a commodity freely accessible to everyone at incredibly low prices. The necessary scenario-aware development environment will be required in this situation to encourage the development of services and appropriate intelligent middleware for understanding and interpreting the information, ensure prevention from deception and hostile strikes, and assure privacy.

A dedicated user interface (UI) is designed using Visual Studio Integrated Development Environment (Wikipedia Contributors, 2023; OPNET Projects, 2023), and the communication scripts are coded using C++20.0 (Shreelatha and Kavyashree, 2023; Visual Studio, 2022) programming language. The UI loads network environments into the OPNET, feeding details of the network components, protocols, key establishment and security mechanisms. The UI is also designed to receive output from OPNET for generating simulation results and plotting graphs based on the results. Several 100 to 1,000 nodes are randomly deployed in a 10,000 square metre simulation environment. ESP-32, ESP-8266, NodeMCU and LoRa IoT types nodes are used for the simulation. The simulation is performed for 168 real-world hours for the nodes with RF range from 100 to 1,000 metres. Our everyday routines have significantly changed due to the growing use of IoT technologies and gadgets. Semantic feature recovery experiments and appliances, which include web-based gadgets, home automation systems, and trustworthy energy management systems, are an example of IoT advancement. The semantic feature recovery experiment is yet another significant IoT accomplishment.

To support human health, it includes small, intelligent tools and devices. These gadgets can be used inside and outside to examine and monitor various health conditions, fitness levels, calories expended in a gym, etc. Additionally, it monitors severe medical conditions in hospitals and trauma centres. Thus, enabling it with cutting-edge technology and smart devices has altered the entire landscape of the medical sphere. IoT developers and academics are also actively working to improve the quality of life for seniors and individuals with disabilities. IoT has dramatically improved in this field, giving such people's daily lives a new direction. Most people use these tools and equipment because they were developed at a very low cost and are readily available within a reasonable price range. The semantic feature recovery experiment has revealed improvements that will increase effectiveness, comfort, and dependability. At numerous signalised junctions across major cities, intelligent sensors and drone gadgets are now managing traffic flow.

Additionally, new cars are coming off the assembly line with sensors pre-installed that can detect impending large traffic jams on a map and propose an alternate route with less congestion. IoT can therefore be very useful in many areas of life and technology.

We can conclude that the semantic feature recovery experiment has much potential for improving technology and helping humanity.

6 Results and analysis

Important network performance metrics such as throughput, end-to-end delay, latency, packet delivery ratio (PDR), average energy consumption and security are measured during the simulation process for 100 to 1,000 nodes in step 100. This section analyses and compares the performance evaluations of existing and proposed methods.

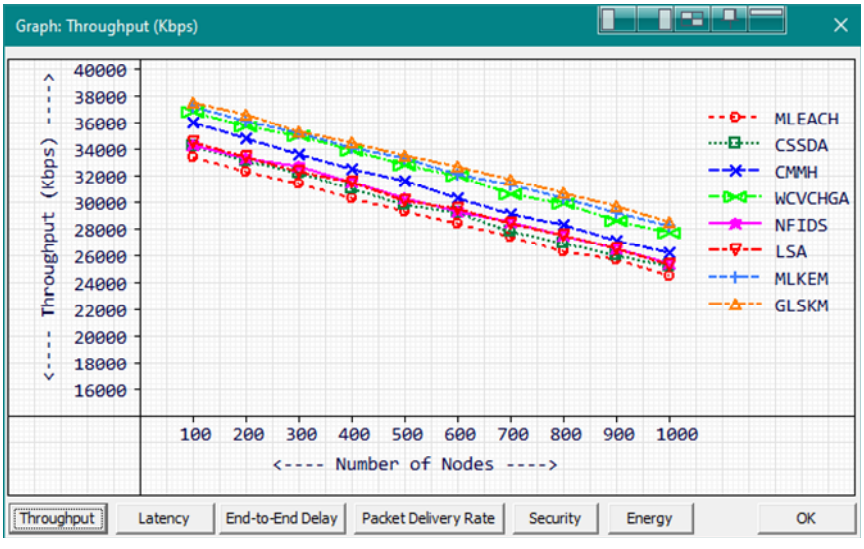
6.1 Throughput

Throughput is the primary network evaluation parameter which is the highest depending factor for overall user experience. The rate of data communication messages transferred from a source to a destination through a communication channel is shortly referred to as the throughput. It is measured using the 'bits-per-second' (bps) unit. A good network should support higher throughput rates for an improved user experience. Measured throughput values during the simulation are listed in Table 3. Based on the observed results, the maximum throughput values are achieved while the number of nodes is 100. It is understood that the higher node density increases network traffic, which increases the data packet drops. The highest achieved throughput is 37,597 kbps, achieved by the GLSKM method during the simulation with 100 nodes. During the simulation with the highest node density, GLKEM achieved a throughput of 28,577 kbps which is also higher than the other comparison methods. As per the experiment, it is observed that the proposed GLKEM method outperforms in terms of throughput values. A comparison graph is given in Figure 6 for ease of data visualisation.

Table 3 Throughput (kbps)

Nodes	*MLEACH*	*CSSDA*	*CMMH*	*WCVCHGA*	*NFIDS*	*LSA*	*MLKEM*	*GLSKM*
100	33,439	34,285	36,054	36,800	34,369	34,536	37,278	37,597
200	32,375	33,186	34,895	35,700	33,311	33,452	36,151	36,661
300	31,481	32,226	33,684	35,020	32,747	32,333	35,246	35,353
400	30,391	31,064	32,558	33,917	31,514	31,538	34,110	34,560
500	29,399	29,834	31,657	32,874	30,399	30,197	33,391	33,501
600	28,443	29,286	30,307	32,027	29,351	29,567	32,162	32,770
700	27,413	27,876	29,169	30,605	28,568	28,415	31,396	31,727
800	26,373	26,970	28,308	29,974	27,548	27,539	30,366	30,753
900	25,744	26,083	27,147	28,650	26,586	26,563	29,240	29,720
1,000	24,536	25,278	26,249	27,749	25,426	25,314	28,254	28,577

Figure 6 Throughput (see online version for colours)



6.2 *Latency*

Latency refers to the communication delay between the source and the destination one-way trip time duration. Latency is measured in millisecond (ms) units. High latency increases the end-to-end communication delay, which refers communication degradation. Good network architecture should have low latency durations to maintain good network quality. Measured latency values during the experiment for the compared methods are listed in Table 4.

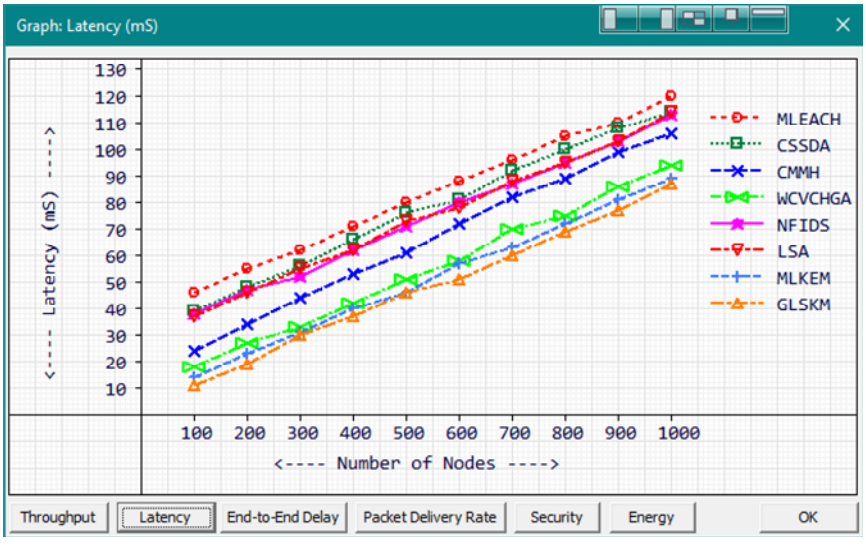
Table 4 Latency (ms)

Nodes	*MLEACH*	*CSSDA*	*CMMH*	*WCVCHGA*	*NFIDS*	*LSA*	*MLKEM*	*GLSKM*
100	46	39	24	18	38	37	14	11
200	55	48	34	27	47	46	23	19
300	62	56	44	33	52	55	31	30
400	71	66	53	42	62	62	40	37
500	80	76	61	51	71	73	46	46
600	88	81	72	58	80	78	57	51
700	96	92	82	70	87	88	63	60
800	105	100	89	75	95	95	72	69
900	110	108	99	86	103	103	81	77
1,000	120	114	106	94	113	114	89	87

Based on the observed results, the GLSKM method causes very little latency when comparing the other methods. The range of GLSKM latency values ranges from 11 ms to 87 ms with an average of 48.7 ms. GLSKM method managed to keep down the latency of

87 ms even for the highest network density with 1,000 nodes. The comparison graph is given in Figure 7.

Figure 7 Latency (see online version for colours)



6.3 End-to-end delay

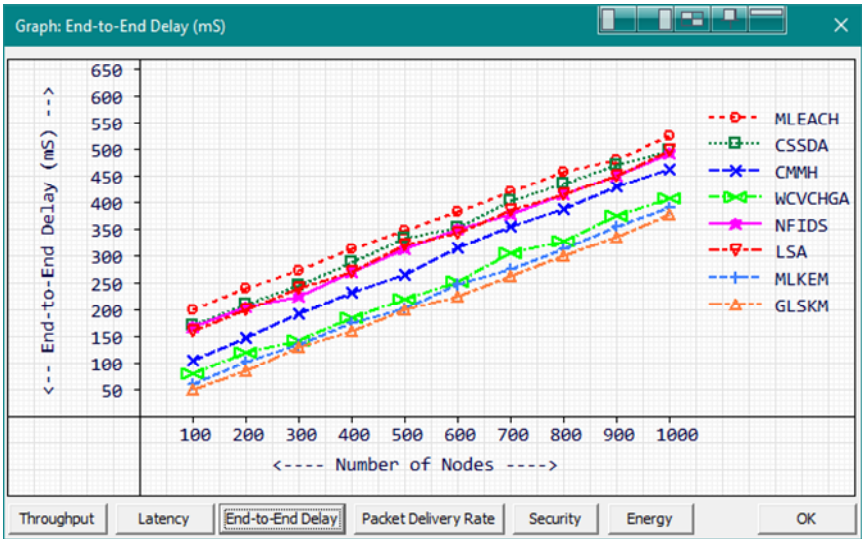
End-to-end delay is the accumulated duration that includes IP delay, communication delay and jitter for a data packet to transfer from source to destination. A good network infrastructure should maintain this end-to-end delay in control to avoid communication lagging. The measured end-to-end delay values are given in Table 5.

Table 5 End-to-end delay (ms)

Nodes	*MLEACH*	*CSSDA*	*CMMH*	*WCVCHGA*	*NFIDS*	*LSA*	*MLKEM*	*GLSKM*
100	202	171	107	80	168	162	62	51
200	241	211	149	120	207	201	103	85
300	273	246	193	144	227	242	136	132
400	313	288	234	185	272	271	177	161
500	349	333	267	222	313	320	204	200
600	384	353	316	253	351	343	248	226
700	421	404	357	305	379	385	276	264
800	459	437	389	328	416	417	314	300
900	482	470	431	376	451	452	355	337
1,000	526	499	464	409	494	498	391	379

The end-to-end delay range of GLSKM is only from 51 ms to 379 ms with an average of 213.5 ms which is comparatively lower than all other compared methods. Measured end-to-end values are plotted as a graph in Figure 8.

Figure 8 End-to-end delay (see online version for colours)



6.4 *Packet delivery ratio*

PDR is an important parameter to measure a communication network's quality. The PDR can be calculated using the formula. $\frac{\sum_{i=1}^{n}\delta_r}{\sum_{i=1}^{n}\delta_t}\times 100$, where n is the total number of packets, δ_r refers to the number of packets successfully received and δ_t refers to the number of packets transferred. Higher PDR refers to the higher quality of the network (Table 6).

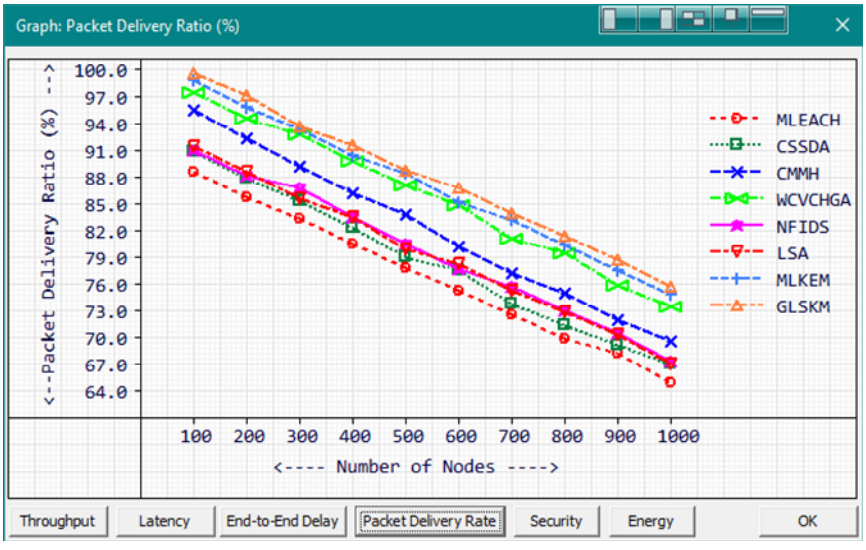
Table 6 Packet delivery ratio (%)

Nodes	*MLEACH*	*CSSDA*	*CMMH*	*WCVCHGA*	*NFIDS*	*LSA*	*MLKEM*	*GLSKM*
100	88.6356	90.8781	95.5671	97.5445	91.1008	91.5434	98.8116	99.6571
200	85.8153	87.9650	92.4950	94.6288	88.2964	88.6701	95.8242	97.1761
300	83.4456	85.4204	89.2851	92.8263	86.8014	85.7040	93.4254	93.7090
400	80.5564	82.3403	86.3004	89.9027	83.5331	83.5967	90.4142	91.6070
500	77.9269	79.0800	83.9122	87.1380	80.5776	80.0422	88.5084	88.8000
600	75.3929	77.6274	80.3338	84.8929	77.7997	78.3723	85.2507	86.8624
700	72.6627	73.8900	77.3173	81.1237	75.7242	75.3187	83.2203	84.0977
800	69.9060	71.4885	75.0351	79.4511	73.0206	72.9967	80.4901	81.5160
900	68.2388	69.1373	71.9576	75.9416	70.4706	70.4097	77.5055	78.7778
1,000	65.0368	67.0036	69.5773	73.5534	67.3959	67.0990	74.8919	75.7481

The OPNET simulator has a facility to measure the individual energy consumption of the network nodes involved in the simulation (Figure 9). The experimental results show that MLKEM and GLSKM methods score higher PDRs. The highest PDR, 99.66%, is

achieved by GLSKM during the simulation with 100 nodes. GLSKM is also sustained, with an average PDR score of 87.79% during the simulation.

Figure 9 Packet delivery ratio (see online version for colours)



6.5 *Energy*

Since the IoT-based WSN nodes are mostly battery-powered devices, energy efficiency is vital in determining the overall network lifetime. Energy is measured in Joule (J) units, and the electrical energy of 1 watt is equal to 1 Joule per second. The average energy consumption of the simulated nodes is measured during the simulation, and the values are given in Table 7.

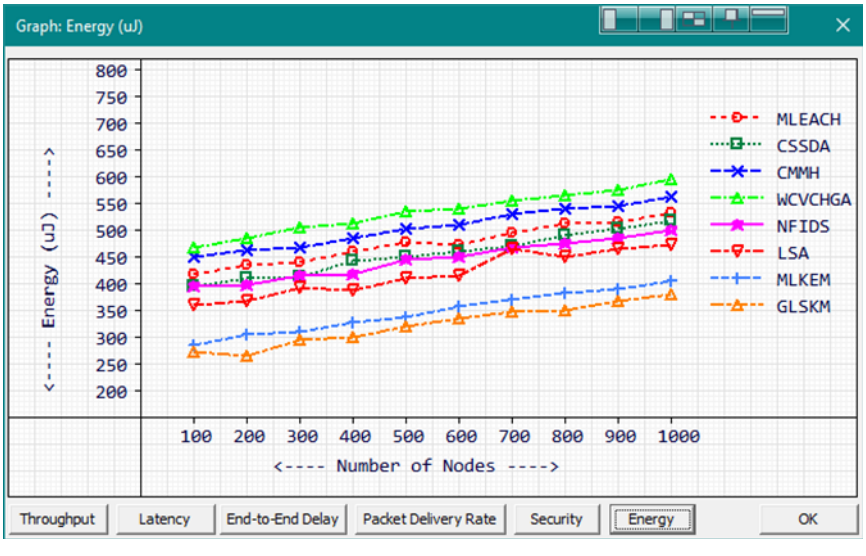
Table 7 Average energy consumption (uJ)

Nodes	*MLEACH*	*CSSDA*	*CMMH*	*WCVCHGA*	*NFIDS*	*LSA*	*MLKEM*	*GLSKM*
100	419	395	452	469	395	361	287	273
200	435	411	463	487	398	369	307	267
300	442	413	469	506	416	393	311	295
400	462	443	486	513	419	388	328	300
500	479	452	504	537	447	410	338	320
600	474	462	511	542	451	416	359	336
700	495	472	530	557	469	467	371	349
800	513	490	540	565	477	451	384	351
900	516	504	545	577	487	466	390	369
1,000	533	519	564	596	501	474	406	380

The energy efficiency of the LSA, MLKEM, and GLSKM methods is relatively higher than the other compared methods, according to observations made during the trials. The GLSKM approach has demonstrated maximum energy efficiency by using the least

energy during the evaluation process. When simulating a low-density network with 100 nodes, GLSKM uses extremely little energy (267 uJ). When simulating with 1,000 nodes, GLSKM uses a maximum of roughly 380 uJ of energy. In addition to the strategies mentioned above, techniques for post-processing exist that lessen the complexity of the model and hence computational expense. Few studies that are related to this topic used after-processing reduction algorithms. These advancements showed that a model's richness might be reduced while performance is hardly affected. IoT is a pruning procedure based on the Taylor series extension of a cost function that was used to reduce the model for semantic data. This method has some drawbacks, such as a loss of accuracy. Instead of applying transfer learning on top of a network that has already been trained, it produces better outcomes when training from scratch. When ranked from best to worst, the average network density usage of energy for GLSKM, MLKEM, and LSA is 324 uJ, 348.1 uJ, and 419.5 uJ, respectively. As a result, it is claimed that the proposed GLSKM method's energy efficiency is poorer than all other compared approaches. Using GLSKM, the network will last longer with the lowest energy use. Figure 10 shows a comparison graph of the measured energy values for each method.

Figure 10 Energy consumption (see online version for colours)



6.6 Security

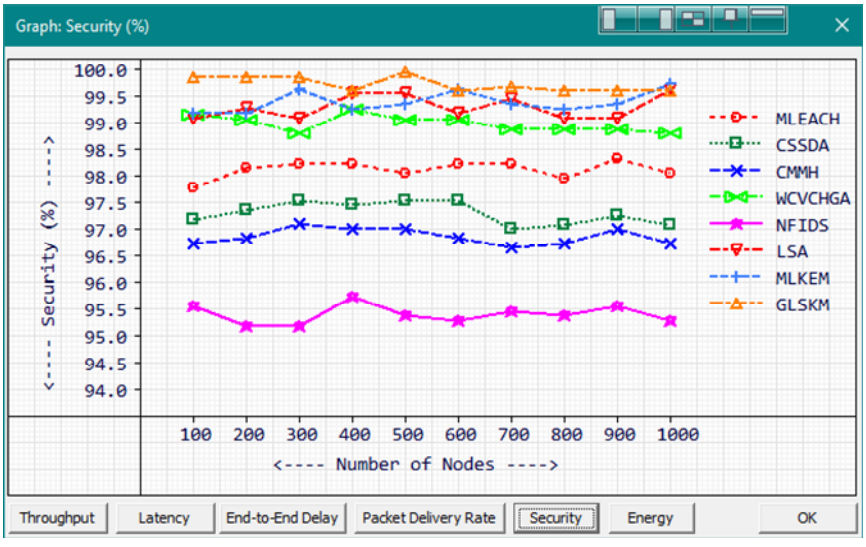
Security is the preeminent parameter in IoT-based WSN security due to its vast application area. A weakened node may collapse the purpose of the entire network. Security can be calculated by $\frac{\delta_r}{\delta_t} \times 100$ where δ_r refers to the rigid data packets, and δ_t refers to the total number of data packets transferred. The security level values are logged during the experiment and enumerated in Table 8.

Table 8 Security (%)

Nodes	*MLEACH*	*CSSDA*	*CMMH*	*WCVCHGA*	*NFIDS*	*LSA*	*MLKEM*	*GLSKM*
100	97.7900	97.1818	96.7418	99.1636	95.5636	99.1000	99.1800	99.8745
200	98.1536	97.3636	96.8327	99.0727	95.2000	99.2818	99.1800	99.8745
300	98.2445	97.5455	97.1055	98.8000	95.2000	99.1000	99.6345	99.8745
400	98.2445	97.4545	97.0145	99.2545	95.7455	99.5545	99.2709	99.6018
500	98.0627	97.5455	97.0145	99.0727	95.3818	99.5545	99.3618	99.9655
600	98.2445	97.5455	96.8327	99.0727	95.2909	99.1909	99.6345	99.6018
700	98.2445	97.0000	96.6509	98.8909	95.4727	99.4636	99.3618	99.6927
800	97.9718	97.0909	96.7418	98.8909	95.3818	99.1000	99.2709	99.6018
900	98.3355	97.2727	97.0145	98.8909	95.5636	99.1000	99.3618	99.6018
1,000	98.0627	97.0909	96.7418	98.8000	95.2909	99.6455	99.7255	99.6018

The observations show that the security level averages for GLSKM, MLKEM and LSA are 99.72%, 99.39% and 99.31%, respectively. The highest security index, 99.96%, is achieved by the GLSKM method. During the entire simulation, the GLSKM method can manage a security level not below 99.60%, showing the rigidity of the method in terms of security. The comparative graph for measured security values of included methods is plotted as a graph in Figure 11.

Figure 11 Security (see online version for colours)



7 Conclusions

Providing high security without affecting performance is an intelligent and vital task in IoT-based WSNs. A GLSKM is established in this work, and the accomplishment towards overall network performance and high-security index with the least energy

utilisation is evaluated. The recorded results disclose that the proposed GLKEM work has gained advantages in preferred network parameters. The consummated benefits of GLSKM stipulate a key to the applicability of this method in real-time generic IoT-based WSN environments. The system's permanent incentive is ensured after the crowdsourcing problem is solved. This study also tests the efficacy of this mechanism using an evolutionary game. Through financial incentives, the suggested GLKEM incentive system could direct employees to consistently raise their level of effort. The thorough simulation studies show that the suggested algorithms can direct employees to maintain high effort and the long-term motivation of mobile sourcing systems.

7.1 Future work

The relevance of the performance of the proposed GLSKM method in a vast network environment with a supplementary number of nodes is not examined in this work, which could be accomplished in future works. The advantage of GLKEM in the future is that more potent models can now be used in contexts with strict constraints. Given the wide range of IoT use cases in contexts with limited resources, we consider this important, including semantic and convolution-based deployments, healthcare evaluation, and convolution analysis. Additionally, lighter and speedier models let researchers develop concepts more quickly and with less money. In subsequent studies, we will delve deeper into issues relating to privacy protection and other aspects of service quality among transactions in GLKEM. We further enhance the incentive system based on game theory to resolve the conflict between safeguarding personal information loss and service excellence. Extensions of our research may involve leveraging augmentation techniques described in similar works like GLKEM to boost performance even more. These techniques will be especially useful for unbalanced datasets like GLKEM. Using machine learning and variable quantisation approaches, we also intend to investigate hyper-parameter fine-tuning to further minimise the proposed architectural storage footprint.

References

Adame, T., Carrascosa-Zamacois, M. and Bellalta, B. (2021) 'Time-sensitive networking in IEEE 802.11be: on the way to low-latency WiFi 7', *Sensors*, Vol. 21, No. 15, p.4954, Basel, Switzerland, DOI: 10.3390/s21154954.

Aldabbagh, G., Dimitriou, N., Alkhuraiji, S., Bamasak, O. and Babrouk, S. (2022) 'Internet of mobile things: reliability and security issues and solutions', *IJCSNS*, Vol. 22, No. 3, pp.687–695.

Alotaibi, M. (2021) 'Improved blowfish algorithm-based secure routing technique in IoT-based WSN', *IEEE Access: Practical Innovations, Open Solutions*, Vol. 9, pp.159187–159197, DOI: 10.1109/access.2021.3130005.

Anajemba, J.H., Tang, Y., Iwendi, C., Ohwoekevwo, A., Srivastava, G. and Jo, O. (2020) 'Realizing efficient security and privacy in IoT networks', *Sensors*, Vol. 20, No. 9, p.2609, Basel, Switzerland, DOI: 10.3390/s20092609.

Anandhavalli, M.A. and Bhuvaneswari, D.A. (2019) 'Lightweight security algorithm on PMIPv6 protocol for IoT based wireless sensor networks', *International Journal of Innovative Technology and Exploring Engineering*, Vol. 8, No. 12, pp.1790–1799.

Cang, S., Kang, Z. and Wang, Z. (2021) 'Pseudo-random number generator based on a generalized conservative Sprott-A system', *Nonlinear Dynamics*, Vol. 104, No. 1, pp.827–844, DOI: 10.1007/s11071-021-06310-9.

Dagdeviren, Z.A. (2021) 'Weighted connected vertex cover based energy-efficient link monitoring for wireless sensor networks towards secure internet of things', *IEEE Access: Practical Innovations, Open Solutions*, Vol. 9, No. 1, pp.10107–10119.

Fascista, A. (2022) 'Toward integrated large-scale environmental monitoring using WSN/UAV/ crowdsensing: a review of applications, signal processing, and future perspectives', *Sensors*, Vol. 22, No. 5, p.1824, Basel, Switzerland, DOI: 10.3390/s22051824.

Ghayvat, H., Mukhopadhyay, S., Gui, X. and Suryadevara, N. (2015) 'WSN- and IoT-based smart homes and their extension to smart buildings', *Sensors*, Vol. 15, No. 5, pp.10350–10379, Basel, Switzerland, DOI: 10.3390/s150510350.

He, Y., Nie, D., Wan, Q. and Hang, L. (2021) 'Construction of open-pit mine environmental monitoring system based on wireless sensor network', *IOP Conference Series, Earth and Environmental Science*, Vol. 784, No. 1, p.12012, DOI: 10.1088/1755-1315/784/1/012012.

Huang, X., Han, D., Cui, M., Lin, G. and Yin, X. (2021) 'Three-dimensional localization algorithm based on improved A* and DV-hop algorithms in wireless sensor network', *Sensors*, Vol. 21, No. 2, p.448, Basel, Switzerland, DOI: 10.3390/s21020448.

Hussein, S.M., López Ramos, J.A. and Ashir, A.M. (2022) 'A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks', *Electronics*, Vol. 11, No. 17, p.2721, DOI: 10.3390/electronics11172721.

Khan, F.A., Abubakar, A., Mahmoud, M., Al-Khasawneh, M.A. and Alarood, A.A. (2019) 'Cotton crop cultivation oriented semantic framework based on IoT smart farming application', *International Journal of Engineering and Advanced Technology*, Vol. 8, No. 3, pp.480–484.

Khasawneh, A.M., Altalhi, M., Kumar, A., Aggarwal, G., Kaiwartya, O., Khalifeh, A., Al-Khasawneh, M.A. and Alarood, A.A. (2021) 'An efficient void aware framework for enabling internet of underwater things', *Journal of Marine Science and Engineering*, Vol. 9, No. 11, p.1219.

Lanzolla, A. and Spadavecchia, M. (2021) 'Wireless sensor networks for environmental monitoring', *Sensors*, Vol. 21, No. 4, p.1172, Basel, Switzerland, DOI: 10.3390/s21041172.

Lloret, J., Sendra, S., Garcia, L. and Jimenez, J.M. (2021) 'A wireless sensor network deployment for soil moisture monitoring in precision agriculture', *Sensors*, Vol. 21, No. 21, p.7243, Basel, Switzerland, DOI: 10.3390/s21217243.

Mast, N., Khan, M.A., Uddin, M.I., Ali Shah, S.A., Khan, A., Al-Khasawneh, M.A. and Mahmoud, M. (2021) 'Channel contention-based routing protocol for wireless ad hoc networks', *Complexity*, Vol. 2021, No. 1, pp.1–10.

OPNET Projects (2023) [online] https://opnetprojects.com/ (accessed 1 July 2023).

Paul, A., Sinha, S., Shaw, R.N. and Ghosh, A. (2021) 'A neuro-fuzzy based IDS for internet-integrated WSN', in *Studies in Computational Intelligence*, pp.71–86, Springer, Singapore.

Priscila, S.S., Rajest, S.S., Tadiboina, S.N., Regin, R. and András, S. (2023) 'Analysis of machine learning and deep learning methods for superstore sales prediction', *FMDB Transactions on Sustainable Computer Letters*, Vol. 1, No. 1, pp.1–11.

Rani, R., Kumar, S., Kaiwartya, O., Khasawneh, A.M., Lloret, J., Al-Khasawneh, M.A., Mahmoud, M. and Alarood, A.A. (2021) 'Towards green computing oriented security: a lightweight postquantum signature for IoE', *Sensors*, Vol. 21, No. 5, p.1883, Basel, Switzerland.

Rani, S., Maheswar, R., Kanagachidambaresan, G.R. and Jayarajan, P. (2020) *Integration of WSN and IoT for Smart Cities*, Springer Nature, Cham, Switzerland.

Salim, A., Ismail, A., Osamy, W. and Khedr, A.M. (2021) 'Compressive sensing based secure data aggregation scheme for IoT based WSN applications', *PloS One*, Vol. 16, No. 12, p.e0260634.

Santi, S., Lemic, F. and Famaey, J. (2022) 'Location-based discovery and network handover management for heterogeneous IEEE 802.11ah IoT applications', *IEEE Transactions on Network and Service Management*, Vol. 19, No. 3, pp.3154–3162, DOI: 10.1109/tnsm.2022.3159839

Shahidinejad, A., Ghobaei-Arani, M., Souri, A., Shojafar, M. and Kumari, S. (2022) 'Light-edge: a lightweight authentication protocol for IoT devices in an edge-cloud environment', *IEEE Consumer Electronics Magazine*, Vol. 11, No. 2, pp.57–63, DOI: 10.1109/mce.2021.3053543.

Sharma, P.K. and Sharma, S. (2021) 'Prevalent fixed point theorems on MIFM-spaces using the (CLR_SR) property and implicit function', *Journal of Mathematics and Computer Science*, Vol. 25, No. 4, pp.341–350.

Shreelatha, G.U. and Kavyashree, M.K. (2023) 'IEEE 802.11g wireless protocol standard: performance analysis', in *IoT Based Control Networks and Intelligent Systems*, pp.67–79, Springer Nature, Singapore.

Springer, J.M. and Kenyon, G.T. (2021) 'It's hard for neural networks to learn the game of life', *2021 International Joint Conference on Neural Networks*, IEEE.

Ullo, G.R.S.L. (2020) 'SinhaAdvances in smart environment monitoring systems using IoT and sensors', *Sensors*, Vol. 20, No. 11, p.3113.

Vayadande, K., Riteshpokarne, M. and Phaldesai, T. (2022) 'Simulation of Conway's game of life using cellular automata', *International Research Journal of Engineering and Technology*, Vol. 9, No. 1, pp.326–331.

Visual Studio (2022) [online] https://visualstudio.microsoft.com/vs/ (accessed 1 July 2023).

Wikipedia Contributors (2023) *Op Amp Integrator*, Wikipedia, The Free Encyclopedia, 24 June [online] https://en.wikipedia.org/w/index.php?title=Op_amp_integrator&oldid=1161725062 (accessed 5 January 2023).