Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.020973
Article

Tech Science Press

Cellular Automata Based Energy Efficient Approach for Improving Security in IOT

P. Hemalatha[1,*] and K. Dhanalakshmi[2]

[1]Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India
[2]Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India
*Corresponding Author: P. Hemalatha. Email: hemalathaphd12@gmail.com

Received: 17 June 2021; Accepted: 20 July 2021

Abstract: Wireless sensor networks (WSNs) develop IoT (Internet of Things) that carry out an important part and include low-cost intelligent devices to gather information. However, these modern accessories have limitations concerning calculation, time taken for processing, storage capacity, and vitality sources. In addition to such restrictions, the foremost primary challenge for sensor networks is achieving reliable data transfer with the secured transmission in a hostile ambience containing vulnerable nodes. The proposed work initially analyses the relation between deployment configuration, lifetime of the deployed network, and transmission delay with this motivation. Besides, it also introduces a new cellular automata-based scheme for improving the security of the network. Each device has a unique id based on its properties (or random number with timestamp). While initializing the communication, they will broadcast their id to all neighbour nodes; to pair with other nodes, they should exchange their unique id. The main advantage of this work is the infinitive states' existence, i.e., the encoded codes generated by cellular automata are infinite. Besides, a modern approach named Fast Particle Swarm Optimization is used to collect data for nodes ar away from the sink and slow data collection for nodes Close to the Sink (FPSO-FSC). Hence the proposed energy-efficient method reduces the end-to-end delay. Comparison studies report that the performance of FPSO-FSC outperforms the previously proposed methods.

Keywords: Energy efficiency; relay selection; delay; duty cycle; lifetime; cellular automata; fast particle swarm optimization; sink

1 Introduction

Internet of Things (IoT) is an emerging technology comprised of networking enables devices, sensors, and tools to process information [1,2]. The primary objective of the IoT is to enable connectivity among the devices connected anywhere containing homogenous objects. At the outset, Radio Frequency Identification (RFID) is the technology accepted for transmitting the electromagnetic waves from the reader to the outer world. This process is completed with the help of wireless connectivity devices. The RFID system mainly consists of two main parts: Radio signal transponder (tag) and tag readers. RFID tags principally comprise information stored electronically meant for classification, tracking and monitoring. Also, the tags provide the instant location tracking when gets attached to any object. Wireless sensor networks (WSNs) [3,4] is another advanced technology for IoT, comprising smart objects called sensor nodes. For the past few recent decades, Wireless Sensor Networks(WSN) [5,6] stood witnessed as a new horizon for sensing the environmental matter using tiny devices called as sensors. It is one of the key enabling technologies of IoT. Usually, the deployment is in an unstructured manner to capture information restricted by resources like vitality, speed of calculation, internal memory backup, and energy consumed for processing. Consecutively, enabling security for the IoT devices also a difficult task constrained due to the factors which includes, reduced memory backup, network hackers and various sensor node limitations.

However, due to the WSN structural complexity and restrictions on sensor nodes, security in IoT is yet challenging with the variety of attacks in networks which disrupts communication [7,8]. IoT-based WSN is used in various situations like contaminated air, assessing water quality status, smart cities, etc., which can be both attended and unattended environments. Improving the efficiency of energy is another crucial aspect [9,10] besides reliable data forwarding. Researchers have defined transmission delay as the totality of the time needed for performing the data transmission from the source node to the sink [11]. In the process of routing [12], a single-hop delay can be formulated as the amount of time taken for receiving the data from one end and successfully transferring it to the next hop.

Accumulation of the data residing any one hop is caused by propagation delay in the routing process due to the gap of the source node which is directly proportional distance of the sink node from any nodes. The presence of umpteen count of hops on the routing path causes a more significant propagation delay. Hence transmission delay is effectively reduced by reducing the multiple paths. Delay that is produced by the single hop is influenced by various components [13]. Once a data packet is received, a specific period is required for the node in order for receiving and processing the data from the receiving end before it enters into the queue meant for sender. Subsequently, concerning the transport protocol, the hop next to the sender transfers the data till the next-hop node accepts it [14]. The process flow comprising of time for processing the data, queuing, and then sending it decides the delay in the network. Depending on the transport protocol, the data will be sending numerous times.

Among these delay periods, node processing data time is the least, which can be excluded in future during the data transmission in a strategic wireless environment. The waiting time of the packets in the queue is conditioned depending upon a nodes' hindrance. More critical data that the network transmits, longer the waiting time of the packets. Leading to stopping in transmission in the event, making the queuing columns complete [15]. The sending time of data depends on the data transport protocol and other network factors. But it usually differs according to the transport protocol used. Data sending time is directly proportional to the transport protocol and other network parameters. The duty cycle mechanism used by WSNs is highly responsible for affecting delay. Limited node energy in WSNs causes the continuation of a lifetime, which is found to be very critical while designing a network with minimal energy consumption.

Energy consumed by the sensor nodes during communication can be significantly minimized by the duty cycle mechanism [16]. For reducing the energy utilized by the nodes in the network, some nodes are left in an idle state when not in function. It results in the duty cycle mechanism. It is a regular alteration of nodes between its awake and state. Generally, the cycle frequency is comparatively high concerning the duty cycle, whereas the time cycle of physical events is extensive. Therefore, using the duty cycle mechanism, the sensor nodes can save energy while meeting the monitoring requirements. However, receiving and sending data is not possible in a numbed state. In case of transmitting the sender's data, the next-hop nodes are set in a numbed state to make the nodes active before starting up a data communication. Thus, reducing the sleep delay in data routing forms a significant cause to minimize propagation delay.

Detection delay is another delay related to the duty cycle. Data packets are not be detected in a sleep state. While sending a packet when the node is at a waiting state is essential, the node wakes before the packet can perform perceiving and receiving. Delay for detection is the time lag that is measured from the time taken by the node that is intended to start up the communication to the other end which is receiving it. The duty cycle is directly proportional to the node's energy consumption. Thus, when the duty cycle increases the energy consumed by the node also gets increases which in turn minimizes the node's life time. Due to this circumstance, no further mechanisms have been employed to maintain a high lifetime and minimized delay. This work is a modern method to successfully decrease the delay and guarantee a lifetime more than the earlier used methods. The major innovations of this study are.

Development of wireless sensor networks management scheme based cellular automata (CA). This suggested scheme enables pre-loaded CAs to form pair wise keys at any given stage of network operation. A local modern method named Fast Particle Swarm Optimization is designed to reduce the energy consumption in addition to diminish the end-to-end delay. It works by collecting data for nodes far away from the sink and facilitates slower data collection for nodes close to the Sink (FPSO-FSC). This work proposing Particle Swarm Optimization (PSO) for on optimizing network lifetime and transmission and obtaining relationships between the transmission range r, the minimum per-hop forwarding distance r_0, the node density ρ and duty cycle affecting the load of the node and network lifetime and network delay.

The paper is organized in a following manner. Section II provides the related works prevailed in this area. Section III outlooks the proposed methodology, Section IV presents the experimental results and comparison charts. Section V concludes the work with future enhancements.

2 Literature Survey

Industrial manufacturing utilizes a huge number of sensor nodes, leading to the formation of the Industrial Internet of Things (IIoTs). In these corresponding situations, data gathered from the sensors is valid at the instances whenever the sensor data reaches the sink node at the given threshold time. Sensor nodes delivered alarm information must be particularly transported at the earliest, or else industrial manufacturing will face great damage and disaster [17,18]. The transmission node selection approach is proposed for networks based on sleep-wake cycle sensors [19]. This approach aims to minimize the delay by selecting the appropriate transmission node from the next-hop nodes. Naveen and Kumar came up with a design that considers that the next-hop node which is deployed nearer to the sink remains to be in the actual state by selecting the transmission node. The originating node now holds dual chances: the first is waiting for waking state of the node which resides very close to the sink. And the next is, making the next hop as the node meant for transmission provided it is awake with far away from the sink.

Simultaneously, whenever the sender is waiting for the node which is nearer to the sink gets wake up, it will result in a decreased number of hops required for routing, and due to waiting, the hop's delay will increase. If the awake node is selected as a transmission node, the delay will not be necessarily slight because the number of hops will increase. The faraway sink approach is used for quick FFSC approach-a slow data collection for the node propounded to outlook the efficient vitality parameters in addition with minimizing the lagging time taken for transmitting the data from originating end to the destination end [20]. Normally, the FFSC approach is applicable for the deployed region which is farthest from the sink. Here, the adoption strategy includes the forwarding of data only if the adjacent node is alive. Eventually, the node in this region completely utilizes the remaining energy. In the nodes closer to the sink, maintaining a high network lifetime and saving energy is possible by selecting optimized transmission nodes before forwarding. Hence, overall, the FFSC approach improves energy-efficient utilization and minimizes network delay. High versatility in networking applications is one of the routing-based method’s advantages for reducing the transmission delay. Also, downside of this design method is its complexity and limited performance. The primary cause of the delay is desynchronized nodes. When transmitting data, the forwarding nodes are not necessarily awake, which causes a long delay.

Chen et al. [21] put forward an innovative design to change the duty cycle and reduce delay. In this work, it is found that the nodes present nearer to the sink needs high energy with the nodes far away from the sink consumes minimal energy. Hence, there is a less amount of energy depleted from the nodes. Researches state that to reduce delay, a large duty cycle is adopted by the near-sink nodes. The far sink nodes acquire a small duty cycle to make sure longer network lifetime. This causes a reduction in the overall delay and high lifetime maintenance. In [22], authors proposed a technique to use nodes’ traffic to adjust the duty cycles, also called as Adaptable Wakeup Period (AWP). It is found that production in the network and duty cycle are interrelated. For example, an increase occurs at the duty cycle raises the success ratio of delivery rate with the considerable decrease in the return rate of the data. According to this approach, a node’s duty cycle is reduced to save energy if the node's traffic is negligible. It will enable saving energy without performance network reduction. When the node has more extensive traffic, its duty cycle is more to meet the network’s performance demands. Also, this system minimizes the energy consumed by the nodes in the network excluding the property of minimizing the network performance. The aforesaid property is carried out by making the network as the synchronous network [23]. The synchronous network is another type of network in which nodes follow a clock frequency; this causes the nodes to be in waken up state only when it is working and remains to be in sleep state other times.

Here, energy is effectively saved by making the nodes that are needed to be in active state only at the time of active data transmission. This system needs exact synchronization, thus limiting the scaling of the system. Applications in wireless sensor networks mainly adopt asynchronous operations because it is difficult to synchronize in a large-scale network. Thus, every node must choose its working slots independently without synchronizing to maximize its application. However, generally, WSNs are not proven to be beneficial when operating in the asynchronous mode in synchronous mode. In this scenario, TDMA-MAC which is an incompetent protocol usually employed [24].

According to this protocol, a work slot is assigned to each node by a system. Each node has to wake up in the organized pattern, perform the required data function then switch back to sleep. It is an energy-efficient technique. In Xu et al. [25] provides the theoretical evidences that shows the propounded algorithm delivers an effective plan with the upper bound of the delay. It is often used for data fusion in wireless sensor nodes, especially in which “n” packets are combined into a single packet. The limitation of this method is that nodes’ performance in the network is decided before in advance. While calculating the time slots of the nodes, it is to be followed that the constant sequence throughout the network. Therefore, this technique applies to the networks in which data functions can’t decide in advance. However, this method is not likely to be adopted in most cases because sensor nodes should be aware of unexpected events in industrial applications, so work slots can’t determine in advance.

This research focuses mainly on WSNs with packet loss and low duty cycles. Therefore, the complexity of research has exceeded the previous ones, significantly to minimize delay and propagation times simultaneously without shortening lifetime. Also, researchers are being conducted in various fields like Secured WSN, Sensor Node authentication, Integrity management and Node management.

3 Proposed Methodology

The network model of this study is similar to the model in [26]. Beneficially, this framework necessitates environmental monitoring, pollution monitoring and continuous monitoring of nuclear radiation by employing N sensor nodes over a radius of region R. The sensor node has an embedded processor and storage system. Unlike the conventional wireless network, WSN sensor devices are battery-driven because of their limited energy and limited calculation and communication potentials. Sensor nodes are capable of collecting the data, analysing them, and sending them to a destination. The sensor field is the domain of the sensor nodes. They usually use a wireless connection to communicate with each other as well as with their neighbouring parts. These sensors are assumed to be non- tamper-resistant. Any action like capturing or compromising the sensor will give the attacker access to data like security information.

Cellular Automata-Based Key management Scheme (CABKMS) is used to avoid such situations. Therefore, a sensor is used to locate its neighbours and obtain CA information through the local wireless network. Once the event is identified, the nodes which are in active state periodically sends the data finally to the sink. Active packets get eventually transmitted to the sink node prevailed in WSNs. The proposed mechanism also assesses the relationship between the system administration and the existence of the network with the delay after CABKMS. An approximate optimization approach, proposed using Particle Swarm Optimization (PSO), is used to minimize the transmission delay with decreased configuration complexity. In some instances, in which the network lifetime is constantly more significant than the described target value, a local contemporary method called nodes Fast Particle Swarm Optimization data collection for far-sink nodes, and slow data collection for near-sink nodes (FPSO-FSC) is suggested. Fig. 1 illustrates the architecture diagram of the CABKMS-FPSO-FSC enabled efficient energy data transmission in the Internet of Things (IoT).

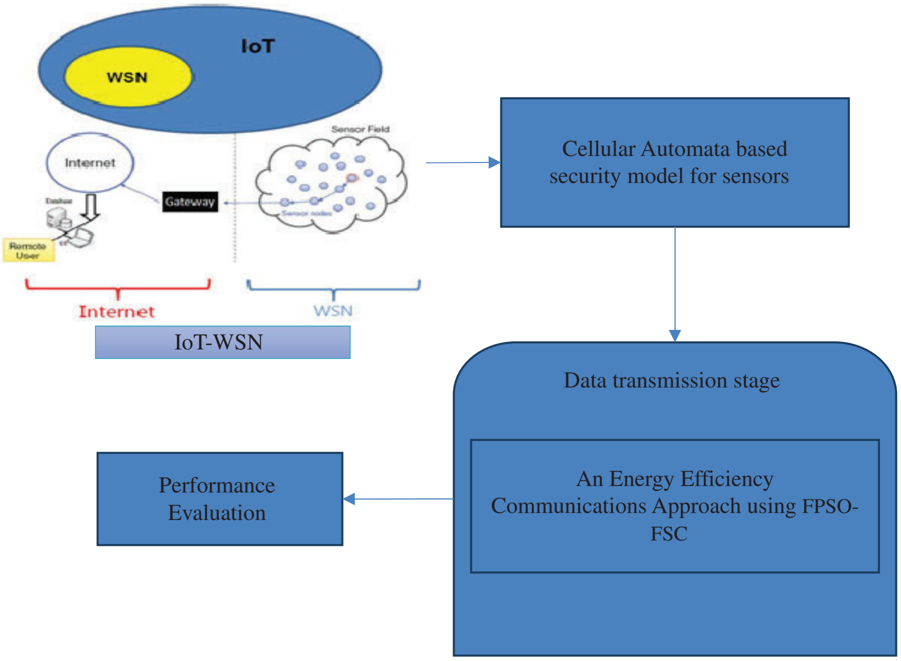

Figure 1: Architecture diagram of CABKMS-FPSO-FSC approach in IoT

3.1 Cellular Automata Based Key Management Scheme (CABKMS)

In CABKMS, each sensor is pre-loaded with a small number of CAs. Additionally, the certificate authorities generate the pair wise keys arbitrarily among the participating nodes employing OR and XOR operations. Each pair of sensors use different key generation methods. Furthermore, it enables the discovery of the unique keys which are quasiall-pairwise. Also, CABKMS attains the resilience with the quasi-perfect property. It also facilitates the acquirement of preloaded shared key structures in the global key schemes. More significantly, the sensor nodes shared a common certificate authority key in the event of computing the key values. This feature facilitates CABKMS in providing inherent support for rekeying activities.This section comprising of three sections which includes CA preloading, shared key deriving and rekeying. At the outset, every node is equipped with the set of CAs that are generated. In the second phase, neighbouring sensors use a shared CA to compute a shared key. Finally, the currently shared keys are refreshed by the rekeying process, and pairwise keys are deployed between sensors in different phases.

CA Pre-Loading: comprises of three offline steps:

Step 1: It is then followed by producing the sets of CAs expressed as C with the corresponding identifiers for every CAs. These CAs are required to be efficient of generating the output data which shows good accurate randomness. Due to the huge pool of CAs, definitely for the formation of CA collection, various types of CAs may be required.

Step 2: In order to build the sub category of preloaded CAs assigned to a sensor, randomly drawing r CAs from the collection C without replacing them. CA selection process needs to be performed carefully in case numerous CA types, say m, are available. It then allows the sensor nodes to generate a set of CAs of r numbers to constitute a full size with same similarities. A simple agenda is considering collection of CAs comprised of m subpools. In this instance, every sensors node can be provided with CAs of range ⌊r/m⌋ taken from the subsets of pools.

Step 3: Memory of each sensor is loaded with CAs and their identifiers. As explained below steps, the underlying phase makes that a minimum CA count are pre-loaded into each sensor and made sure that at least one CA is shared by two sensors with a specified probability.

i) The degree of the probability of CAs being overlapped as the two subsets determines the key establishment in CABKMS.

ii) Network topology have to be considered as the random graph where the network connectivity can be analysed by adopting the randomized graph theoretic models.

iii) Hence, the other existing pre-distribution schemes are dependable to the probability of key sharing. Also, the results generated after the data transfer are built based on the node's key sharing in the random graph. For instance, with a collection of $C = 20,000$ CAs and preloading each sensor with $r = 250$ CAs, the probability p of two nodes sharing at least 1 CA is $p = 1 - \frac{((C-r)!)^2}{(C-2r)!C!} = 1 - \frac{((19750)!)^2}{(19500)!20000!} \approx 90\%$.

iv) It is noted that even if same quantity of information is stored in sensor's memory. The memory overhead of each node may get varied as it directly relies on the CAs and the memory overhead of each may be varied.

Shared Key Derivation: This encompasses two steps that are exchange CA data and key calculation.

CA information Exchange: CA data is exchanged by Sensors and corresponding immediate (i.e., 1-hop) neighbours after deployment process. This can be easily accomplished by enabling sensors to carry out a local broadcast with its own CA identifiers. It's important to note that attack opportunity is not given by this approach to an adversary which already exists because keys are never transmitted. Furthermore, if a node is captured by an adversary, only the CAs that is stored in the node memory can be obtained. Same CA used by other node pairs likely selects different initialization and round numbers. Therefore, other keys computed with the same CA will not be familiar to the adversary.

Key Computation: A common CA is selected by two sensors, once the list of CAs owned by neighbouring nodes is processed. Then, the sensors select two parameter values for configuring their common CA. At the outset, the CAs are selected by the deployed sensor node and the successive rounds for rule enforcement. All such variables are then utilized for generating the session key. All such variables are then utilized for generating the session key.

An example for CA rule is given in the below shown equation:

$$c_i' = c_{i-1} \oplus (c_i \text{ OR } c_{i+1}) \quad (1)$$

The rule implicates the following:

The value of the cellc_i at the starting state is denoted by c_i'. The rule denotes that the new cell value will be the XOR of the left neighbours' cell value (c_{i-1}) and the current cells and right neighbour's (c_{i+1}) OR value. It's worth to observe that the addition of supplementary variables while reducing a session, the main aspect varies from assessing a key based on incomplete information. This results in, sharing multiple pairs of nodes highly depending on arbitrary CA output values which is coupled with the independent starting variables making it doubtful to share the same key. Thus, CABKMS enables achieving the unique keys that are shared between the dual set of sensors that are quasi-all pairwise.

In the instances where the adjacent nodes not sharing the CA, path key establishment phase can be used to obtain common neighbour for transmitting key related information. Intermediate node has only one constraint that to establish a key it must share a key with the neighbouring nodes. The key pre-distribution schemes adopt path-key establishment procedure. Hence, clarification of this step is omitted, and the interested reader is referred to any the other work during this phase.

Rekeying: Rekeying can be decided by nodes for many causes, e.g., prudent key refreshment, possible key disclosure, or newly allocated sensors. In CABKMS, foundation of the rekeying process is based on the top level of randomness obtainable from CAs. This enables rekeying by the nodes at any time during the network lifetime. This also doesn't dependent on any of the preceding rekeying phase. This quality is important for dependability and durability of networks containing This quality is important for dependability and durability of networks containing the nodes which have limited resources. For examples where the sensors having limited battery power will reduce n world-wide data communication till the restoration is done. Flexibility provided to the network controller is other good characteristics of CABKMS's rekeying capability.

Specifically, for the initial sensor deployment it is not necessary to know the number of phases (or "generations") of node placements beforehand. For rekeying purpose, two nodes sharing a CA have to agree on a new initial configuration. And the number of iterations can be determined using CA rule. Arbitrary decision is taken to decide node responsible for initiation process. In case rekeying takes place among two nodes previously sharing a key with the added protection can be encrypted for the rekeying specifications agreed upon by the nodes. Transmission of these parameters can be secured by the to-be-refreshed key. Existing sensors do not share keys with new ones in phase deployment. Therefore, plaintext is used to transmit rekeying parameters. Session key establishment is performed by sensors that are newly deployed which are supplied with CAs that are derived from the same CA collection similar to previously deployed sensors. Although, one can argue that CAs can be replaced by one-way functions in the rekeying process. But, CAs are most suitable option due to the below mentioned reasons.

- Expensive instructions like modular multiplications are needed for most of these purposes and their co related approach (e.g., one-way hash chains). Hence the overhead implementation essential to these functions may not be suitable for devices having constrained resources.
- One-way functions or compression functions work by mapping a greater arbitrary input size into a compact fixed-size output. Behaviour exhibited by CA is exactly opposite of this. To be more specific, a few initial bits are used by CAs for generating arbitrarily long (and variable) length keys.

The rekeying information like the initial configuration value or round number does not compulsorily be preserved by the current shared key. By enforcing the ad-hoc connectivity, the sensors are able to make such a functional decision. Unless time consumed by the two nodes using the CA is not compromised, passive listener won't be able to conclude the current establishment key over any rekey eavesdropped key. The authentication procedure experiences a small quantity of ambiguity (i.e., the cost of a simple XOR operation), so that the sensors nodes take the shared key that are recently shared in the instances of protecting the rekeying parameters. Therefore, keying parameters continue to stay secure even though CA is being hacked, still the preliminary positions in addition with the iteration numbers of the CA rule is not detected.

3.2 An Energy Efficiency Communications Approach Using FPSO-FSC

The main idea is to maximize the network lifetime L by introducing optimized parameters in the hotspot regions by using a PSO method similar to Algorithm 1 with an effort to detect the parameters resulting in the lowest delay in the non-hotspot regions. Considering a network with a duty cycle τ. Then, method to select a suitable r_0 and network lifetime L and a delay, D_min , under such a parameter separately in both hotspot and non-hotpot regions. The core of the FFSC design consists of 2 parts:

The optimum parameters use node non-hotspot regions to minimizes the delay without considering energy consumption. Considering the vitality parameters is not needed fir the nodes as it performs relaying the data due to the extensive volumes of the dissipated energy prevailed in the regions that are non-hotspot; Hence, optimal network parameters can be used to reduce delay effectively.

Optimal parameters capable of reducing the energy consumption are utilized for data relay in hotspot region. Energy consumption of the hotspot regions mainly relies in the lifetime of the deployed network. Also, this life time inversely proportional to the energy consumed. It optimizes the parameters across the region using the PSO mechanism. By enumerating two factors, FPSO-FSC is employed to minimize the packet transmission delay which in turn preserves the life time.

Algorithm 1: Optimal Parameters of Duty cycle τ, transmission radius r using PSO

```
Input: Network lifetime $L_\Delta$ and radius $r$ needed for application
Output: Optimal parameters to reduce the network delay, duty cycle τ, and relay node with the smallest r0
Initialization: For a network where the lifetime $L$ and radius $r$ are needed by the application, give the optimized duty cycle τ and the minimum reward $r_0$ by PSO for a relay node that minimize the delay while keeping the lifetime greater than $L_\Delta$, number of sensors as particles as $N$.
1: Assign initial values $\tau = \tau_0$, $D^{min} = \infty$, $r_0 = 0$; //τ0 is a relatively small initial value and D is the overall network delay
2: Calculate the maximum energy consumption $E_{min}^{r_0}$ based on theorem 7 [20] to obtain the network lifetime $L = \frac{E_{init}}{E_{min}^{r_0}}$
3: While $L < L_\Delta$ Do PSO algorithm procedure //Look for optimal parameters for the least delay until lifetime meets the requirements
(1) Set the values as in step 1 and the particle number, and determine the scope of each dimension of network and maximal speed of particle.
(2) At the outset, set the PSO population with the dual dimensions and declare the position and wavelength of every particle.
(3) By considering the present position, set the personal extreme of particle followed by computing the fitness value of every particle. Global extreme is defined by the personal extreme which possess the best fitness value among all particles.
```

(Continued)

Algorithm 1 (continued)

```
4) Perform the iteration till the final outcome modifies or attains the maximal reach.
5) Assign the speed and location of the particle by the following formulae.
$v_{id}(t+1) = w \times v_{id}(t) + c_1 \times rand_1($ב$) \times [p_{id}(t) - x_{id}] + c_2 \times rand_2$ $($ב$) \times [p_{gd}(t) - x_{id}],$ ב ε $[0, 1]$
$x_{id}(t+1) = x_{id}(t) + v_{id}(t+1) 1 \leq i \leq N, 1 \leq d \leq D$
Where $v_{id}$ and $x_{id}$ are the dth speed component and location component of $i$th particle. $c_1$ and $c_2$ are acceleration coefficients and they denote the weights of statistical acceleration items in approaching to $P_{id}$ and $P_{gd}$ of a particle and $w$ is inertia coefficient and it make particles keeping fly inertia.
6) Find the fitness value of particle and if the value of the newer position is optimal than the value of the extreme, then the obtained location replaces the personal extreme location.
7) When the obtained particle founds optimal and better than the better extreme, then the former is replaced with the global extreme.
8) Return the optimal τ and $r_0$.
4: For each $\tau$ , $r_0 = 0$, the minimum delay $D^{min} = \infty$
5: While $r_0 < r$ Do // Explore different r0 and computing $D^{r_0}$ by Eq. (16) in Theorem 5 [20] and also calculate the delay of the current lifetime $L = \frac{E_{init}}{E_{min}^{r0}}$
8: If $D^{r_0} < D^{min}$ min and $L < L_\Delta$ then
Choose the optimal values which meet the requirements of the intended application
9: The current minimum delay as $D_{min} = D^{r_0}$
10: Record the optimal duty cycle and $r_0$ found now as $\tau_o = \tau$, $r_{op} = r_0$ //op is described as optimal;
11: End if
12: The $r_0$ reduced by $\Delta_r$ as $r_0 = r_0 + \Delta_r$
13: End while
14: τ = Δτ
15: End while
16: Return the PSO based optimal parameter values as $r_{0p} = r_0$.
```

4 Experimental Results and Discussion

The proposed CABKMS-FPSO-FSC is described with respect to probability of key sharing, node capture resilience, computational overhead, expense for communication, overhead storage, and ability to rekey. Furthermore, certain unique features of CABKMS are explained and its co relation with the overall performance. In case of unspecified parameters, the network parameters are set to: R = 500 m and r = 80 m. A novel FPSO-FSC method is designed to improve efficiency of energy while decreasing the transmission delay. In previous routing methods, smaller node loads present in the regions away the sink disabled using large amount of surplus energy. From an overall perspective analysis based on parameters such as End-to-end delay, Energy Consumption, Packet Delivery Ratio, Attack Detection Accuracy, and Communication overhead, the CABKMS-FPSO-FSC approach results in an effectively improved energy utility rate thereby reducing network delay than the tradition FFSC method [20] and direct forwarding strategy approach. The main system model parameters used in this study are similar to those in [27].

4.1 End-to-End Delay

Fig. 2 shows the comparison result of transmission delay from the proposed CABKMS-FPSO-FSC, and the existing FFSC and direct forwarding strategy. It is noted that the proposed CABKMS-FPSO-FSC attains greater throughput when compared to existing methods. The performance of End-to-End delay by distance is observed to be still lower for further increasing distance too. Relative to the direct forwarding strategy, the CABKMS-FPSO-FSC approach can effectively decrease transmission delay by 7.56%–23.16%, while compared to the FFSC strategy; reduces the transmission delay by 4.16%–9.79% while keeping network lifetime constant.

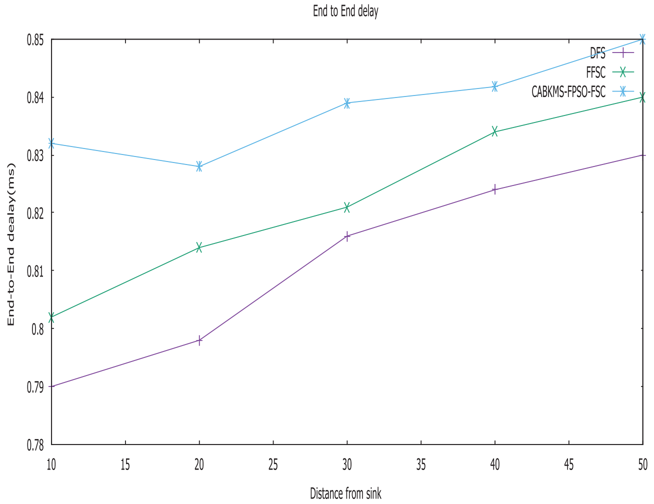

Figure 2: End-to-end delay *vs*. distance from sink (m)

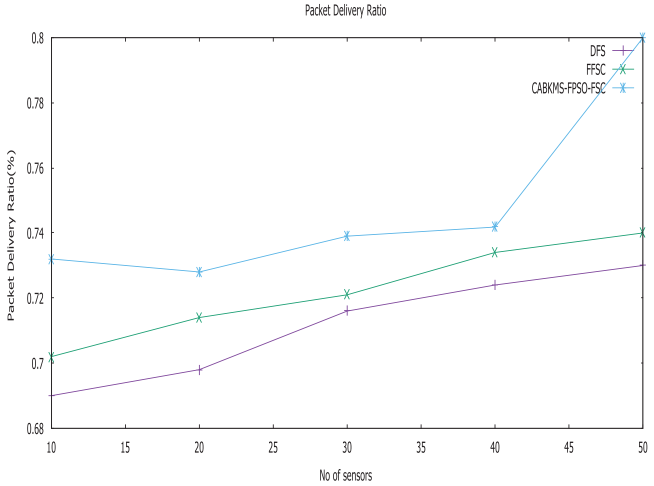

Figure 3: Packet delivery ratio *vs*. no. of sensors

4.2 Packet Delivery Ratio (PDR)

Delivery ratio usually portrays the state of message sent to the destination node. It can be said that proposed CABKMS-FPSO-FSC approach reports enhanced ration of data transmission when compared to the FFSC and direct forwarding strategy approach shown in Fig. 3.

$$PDR = \frac{\sum P_{ST}}{\sum P_T} = \frac{Total\ Packet\ successfully\ delivered\ to\ sink\ node}{Total\ packets\ transmitted} \tag{2}$$

From the figure, when number of nodes increases the appropriate delivery ration also increases gradually. The proposed CABKMS-FPSO-FSC has high delivery ratio compared to the existing methods. The reason being that, trustworthy sensors can be identified by the proposed work with the help of CABKMS.

4.3 Attack Detection Accuracy

Fig. 4 shows the attack detection accuracy of TAODV, AODV and CABKMS-FPSO-FSC scheme. It is obvious that the detection accuracy of CABKMS-FPSO-FSC is greater than FFSC and direct forwarding strategy scheme when exposed to several attacks. From Fig. 2, we can see that the average DA reduces when the number of attackers increases in the network. When trust management system is implemented, the average detection accuracy of CABKMS-FPSO-FSC, FFSC and direct forwarding strategy, are 97.95%, 96.95% and 95.97% respectively. Improve the reliability of route discovery compared to the traditional trust mechanism is the main reason.

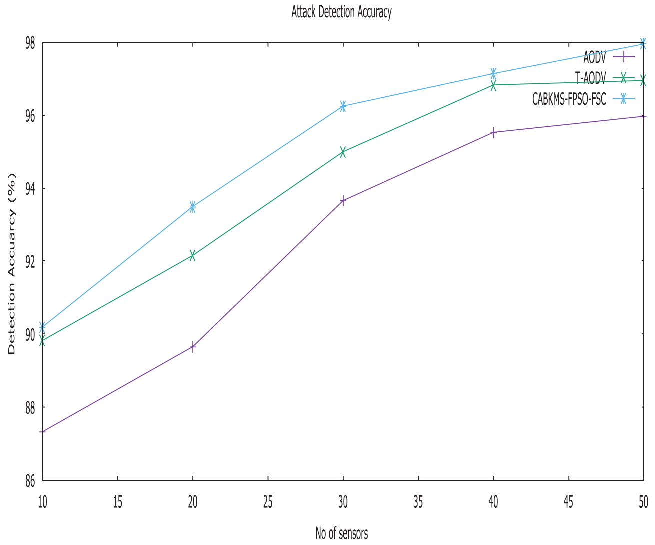

Figure 4: Attack detection accuracy *vs*. no. of sensors

4.4 Energy Consumption

Fig. 5. illustrates the Energy consumption of three techniques when plotted against the distance from the sink. It is possible to say that the CABKMS-FPSO-FSC approach consumes less energy than the other FFSC and direct forwarding strategy approach. The initial energy possess by the sensor nodes are 500Joules. In the given figure, the value of energy will reduce significantly when malicious nodes initiate attacks in WSN. CABKMS-FPSO-FSC increases energy value compared to FFSC and direct forwarding strategy. Since explicit trust is considered, indirect trust and incentive factor can resist detecting error effectively. We observe from the figure that while using the CABKMS-FPSO-FSC, most of the used energy is relatively equal to other designs such as FFSC and direct forwarding strategy. It implies that network lifetime does not decrease while using the unused node energy in non-hotspot areas. It reports the efficacy of CABKMS-FPSO-FSC.

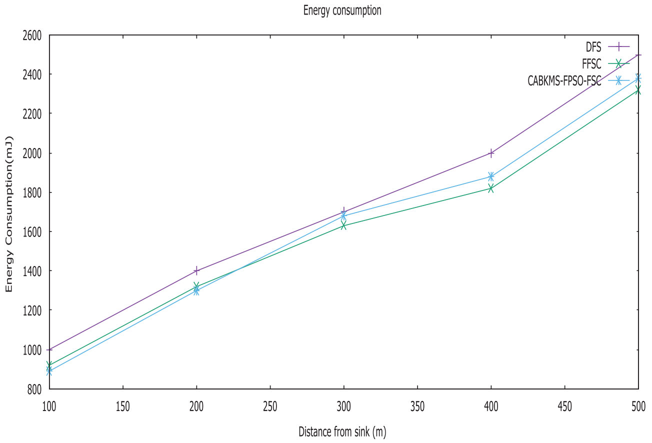

Figure 5: Energy consumption *vs*. distance from sink

4.5 Network Lifetime

Fig. 6. illustrates the relationship of the network lifetime based on the number of nodes. It is considered that the CABKMS-FPSO-FSC approach has a high network lifetime when compared with the other FFSC and direct forwarding strategy design. Compared to the direct forwarding concept, the lifetime network of the CABKMS-FPSO-FSC design stays unchanged. Even though the no-wait feature is present in the direct forwarding strategy, it can cause more hops than the other techniques. In such a scenario, it is proven that the outcome has a shorter lifetime than CABKMS-FPSO-FSC.

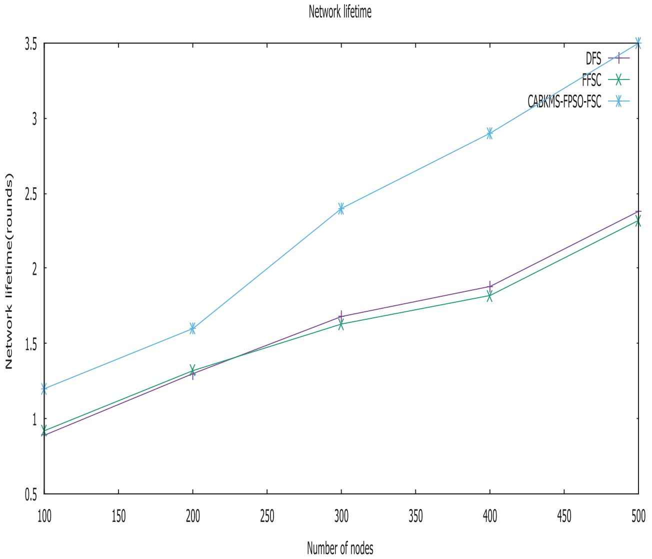

Figure 6: Network lifetime *vs*. distance from sink

4.6 Communication Overhead

The graph Fig. 7. shows the communication overhead of CABKMS-FPSO-FSC, FFSC, and direct forwarding strategy plotting against the number of sensor nodes. The nodes deployed in the region make the average route hop of CABKMS-FPSO-FSC greater than FFSC and direct forwarding strategy because nodes will select a relatively long path than selecting an untrusted next-hop node in other existing methods. Although CABKMS-FPSO-FSC superior to FFSC and a direct forwarding strategy as it can eliminate malicious nodes from the routing paths. Our ideas are confirmed by these results and show a positive tendency for the CABKMS-FPSO-FSC strategy.

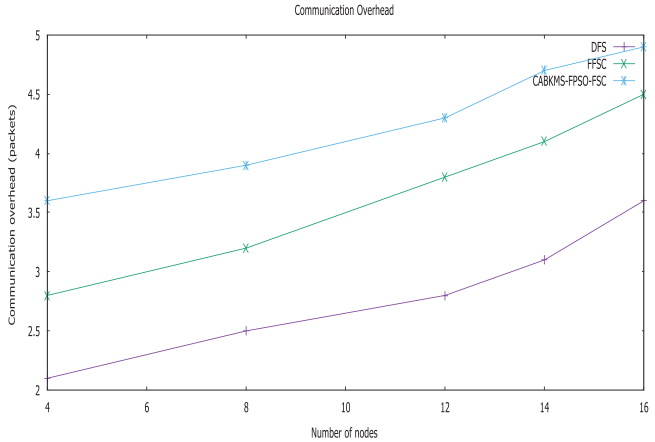

Figure 7: Communication overhead *vs*. no of nodes

5 Conclusion and Future work

WSNs primarily function with Green communications. It includes challenges like transferring data to the sink at the earliest while maintaining efficient energy. This work develops a key management scheme built on cellular automata for wireless sensor networks. These functions set up pairwise keys among neighbouring sensors at different functional phases in a sensor-based network. In this proposed system, sensors are preloaded with several CA rules. Subsequently, the determination of pairwise keys by the sensors with its neighbours is performed after deploying by using some primary parameters or variables to their shared CAs. Then, PSO algorithm is proposed as an optimization algorithm that can to optimize minimum per-hop forwarding distance $\mathbf{r_0}$, and also involving optimization of transmission range $\mathbf{r}$ as well as the duty cycle. Based on this experimental analysis, FPSO-FSC further reduces the end-to-end delay. As a future enhancement focused on attack detection in the IoT-based WSN, it will profoundly impact our lives in terms of having a deep economy and commercial and social lives. The nodes participating in IoT networks are mostly resource-constrained, making them luring targets for attacks.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, “Internet of things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computing System*, vol. 29, pp. 1645–1660, 2013.

[2] D. Uckelmann, M. Harrison and F. Michahelles, An architectural approach towards the future internet of things. In: *Architecting the Internet of Things*. Heidelberg, Germany: Springer, pp. 1–24, 2011.

[3] J. D. Downie, L. Nederlof, J. S. Sutherland, R. E. Wagner, D. A. Webb *et al.,* "Radio frequency identification (RFID) connected tag communications protocol and related systems and methods," U. S. Patent No. 9, 652, 707, 2017.

[4] M. J. Koch, C. B. Swope and B. J. Bekritsky, "System for, and method of, accurately and rapidly determining, in real-time, true bearings of radio frequency identification (RFID) tags associated with items in a controlled area," U.S. Patent 9,773,136, 2017.

[5] K. Muthumayil, T. Jayasankar, N. Krishnaraj, M. Sikkandar, P. N. Balasubramanian *et al.,* "Maximizing throughput in wireless multimedia sensor network using soft computing techniques," *Intelligent Automation & Soft Computing*, vol. 27, no. 3, pp. 771–784, 2021.

[6] N. Krishnaraj, M. Elhoseny, M. Thenmozhi, M. M. Selim and K. Shankar, "Deep learning model for real-time image compression in internet of underwater things (IoUT)," *Journal of Real-Time Image Processing*, vol. 17, no. 6, pp. 2097–2111, 2020.

[7] H. Ning, H. Liu and T. Yang, "Cyberentity security in the internet of things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[8] S. Pirbhulal, H. Zhang, M. E. E. Alahi, H. Ghayvat, S. C. Mukhopadhyay *et al.,* "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, no. 1, pp. 69–78, 2017.

[9] N. Sharma and A. K. Sharma, "Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network," *Sādhanā*, vol. 41, pp. 283–288, 2016.

[10] K. Wang, Y. Wang, Y. Sun, S. Guo and J. Wu, "Green industrial Internet of things architecture: An energy-efficient perspective," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 48–54, 2016.

[11] H. Teng, X. Liu, A. Liu, H. Shen, C. Huang *et al.,* "Adaptive transmission power control for reliable data forwarding in sensor based networks," *Wireless Communications and Mobile Computing*, vol. 2018, no. 2068375, pp. 1–23, 2018.

[12] H. Dai, G. Chen, C. Wang, S. Wang, X. Wu *et al.,* "Quality of energy provisioning for wireless power transfer," *IEEE Transaction Parallel Distribution System*, vol. 26, no. 2, pp. 527–537, 2015.

[13] T. Wang, J. Zhou, M. Huang, M. Z. A. Bhuiyan Liu, W. Xu *et al.,* "Fog-based storage technology to fight with cyber threat," *Future Generation Computing System*, vol. 83, no. 14, pp. 208–218, 2018.

[14] A. Liu, W. Chen and X. Liu, "Delay optimal opportunistic pipeline routing scheme for cognitive radio sensor networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, pp. 1–13, 2018.

[15] Y. Liu, K. Ota, K. Zhang, M. Ma and N. Xiong, "QTSAC: An energy efficient MAC protocol for delay minimized in wireless sensor networks," *IEEE Access*, vol. 26, no. 6, pp. 8273–8291, 2018.

[16] K. P. Naveen and K. Anurag, "Relay selection for geographical forwarding in sleep-wake cycling wireless sensor networks," *IEEE Transaction Mobile Computing*, vol. 12, no. 3, pp. 475–488, 2013.

[17] Z. Chen, A. Liu, Z. Li, Y. J. Choi and J. Li, "Distributed duty cycle control for delay improvement in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 10, no. 3, pp. 559–578, 2017.

[18] M. Dong, K. Ota and A. Liu, "RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 511–519, 2016.

[19] K. P. Naveen and A. Kumar, "Relay selection for geographical forwarding in sleep-wake cycling wireless sensor networks," *IEEE Transaction. Mobile Computing*, vol. 12, no. 3, pp. 475–488, 2013.

[20] Y. Liu, A. Liu, Y. Hu, Z. Li, Y. J. Choi *et al.,* "An energy efficiency communications approach for delay minimizing in internet of things," *IEEE Access*, vol. 4, pp. 3775–3793, 2016.

[21] Z. Chen, A. Liu, Z. Li, Y. J. Choi and J. Li, "Distributed duty cycle control for delay improvement in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 10, no. 3, pp. 559–578, 2017.

[22] J. H. Lee, "A traffic-aware energy efficient scheme for WSN employing an adaptable wakeup period," *Wireless Personal Communication*, vol. 71, no. 3, pp. 1879–1914, 2013.

[23] C. J. Liu, P. Huang and L. Xiao, “TAS-MAC: A traffic-adaptive synchronous MAC protocol for wireless sensor networks,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 12, no. 1, pp. 1–30, 2016.

[24] X. Liu, Y. Liu, H. Song and A. Liu, “Big data orchestration as a service networking,” *IEEE Communication Management*, vol. 55, no. 9, pp. 94–101, 2017.

[25] X. H. Xu, X. Y. Li, X. Mao, S. Tang, S. G. Wang *et al.,* “A delay-efficient algorithm for data aggregation in multihop wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 1, pp. 163–175, 2011.

[26] M. Zorzi and R. R. Rao, “Geographic random forwarding (GeRaF) for ad hoc and sensor networks: Multihop performance,” *In IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 337–348, 2003.

[27] P. Medagliani, J. Leguay, G. Ferrari, V. Gay and M. Lopez-Ramos, “Energy-efficient mobile target detection in wireless sensor networks with random node deployment and partial coverage,” *Pervasive Mobile Computing*, vol. 8, no. 3, pp. 429–447, 2012.