PERFORMANCE EVALUATION OF SA-LA ROUTING PROTOCOL FOR WSN INTEGRATED IOT

Chettan Rajan Dongarsane[1,*], D. Mahesh Kumar[2] and Swati Sankpal[3]

Received: June 09, 2021; Revised: December 23, 2021; Accepted: September 27, 2022

Abstract

WSN is considered one of the prominent technology due to the different kinds of operations they are involved in. Secured and energy-efficient data routing is very important in the WSN framework. The main aim of this research is to evaluate the performance of a secured and energy-efficient routing protocol named Self Adaptive-Lion Algorithm (SA-LA) in WSN, as well as in WSN assisted IoT framework. This protocol is evaluated by means of different parameters like residual energy, delay, network lifetime, Node Trust Factor (NTF), Interference factor (IF), throughput and security risk probability. Achieved improved outcomes as network lifetime rose up to 14% also risk probability decreased marginally through 18% compared to previous methods.

Keywords: WSN, IoT, Self Adaptive-Lion Algorithm, Packet Drop Rate, and Node Trust Factor

Introduction

IoT is considered as the network which can generate, interchange, and utilize the data with fewer people involved. To interchange data for storage, it incorporates a huge amount of sensing devices into a single device that communicates with one another in the whole network (Kalkan 2020). Besides, the storage, size, energy capacity, and power of these gadgets are varied with one another (Harbi *et al.*, 2019). Smart homes, healthcare, agriculture, and so on are related to IoT which is used in everyday life (Baig *et al*., 2020). With the limited number of sources, WSNs are assumed as future contributors to IoT. With specific conditions, a huge number of sensors in WSN are scattered randomly in isolated and dangerous locations to collect the data also, the position of the sensor is not defined in advance. Sound, pressure, motion, quake, and temperature-related information are collected by these sensors. Scalability on deployment, low-priced sensors, and heterogeneity are some exclusive features present in WSN (Tewari and Gupta, 2020).

Routing in WSN plays an important role in which data transmission nearly consumes 70% of energy from total energy between the wide varieties of routing protocols. For that reason, it is very essential to design energy-efficient routing protocols that conserve less energy and enhance the network lifetime. Conversely, application-specific design, limited resource sensors, and lack of global addressing policy make challenging issues in routing. In addition to that, security is considered as

[1] *Sanjeevan Engineering and Technology Institute, Kolhapur, Maharashtra, India. E-mail: chetanndongarsane@gmail.com*
[2] *JSS Academy of Technical Education, Bengaluru, Karnataka, India. E-mail: dmkjssate@gmail.com*
[3] *D.Y. Patil College of Engineering & Technology. E-mail: Maharashtra, India. E-mail: sankpal1987@gmail.com*
[*] *Corresponding author*

another critical problem as sensors are deployed in unprotected atmospheres in which they are vulnerable to security attacks. Generally, security goals like integrity, confidentiality, and authenticity of transmitted data are provided by integrating security algorithms with routing protocols. These kinds of security goals are accomplished with the help of conventional routing protocols which execute different security mechanisms and any conflicts between those measures may generate vulnerabilities in the network. Also, due to limited power, bandwidth, mobility, storage, and sensing bottlenecks, smart devices in IoT are susceptible to attacks. Subsequently, secured data transmission is considered as one security risk in which safeguarding the data transmission against the attack is considered as another issue with secrecy (Bhoyar *et al*., 2018). In the IoT environment, plenty of researchers analyze new techniques and effective methods to improve secure communication. Conversely, privacy and security issues are considered a great deal in IoT settings due to the quick enlargements in information technology (Moin *et al*., 2019; Kandi *et al*., 2020). In order to achieve energy efficiency as well as security, it is very essential to develop both energy efficiency and security protocols in WSN assisted IoT framework.

Survey of Energy Efficient Routing Protocol

Muhammad Aslam et al. had introduced a HADCC (Hybrid Advance Distributed Centralized Clustering) approach for an energy-effective route scheduling algorithm (Muhammad Aslam *et al*., 2014) To execute the proposed model, high-level network geography is introduced. The entire system area is separated into two actual stages. The principal actual level comprises a roundabout locale, homogeneous typical nodes, and exceedingly significant BSs. The second actual level is the external area of the circle that contains progressed heterogeneous nodes. HADCC drags out the network lifetime for both homogeneous and heterogeneous WSNs when contrasted with existing progressed clustering routing procedures. Furthermore, Ali and Ghaffari were described energy-efficient routing algorithm (EERP) has been developed for WSNs with the help of the A-star process. (Ghaffari Ali., 2014) The developed routing plan expands the system life by transferring information parcels by means of the ideal briefest way. The ideal way can be found as to the greatest leftover energy of the following, bounce sensor hub, high connection quality, support inhabitancy, and smallest jump tallies. The outcomes display that the suggested method increases network lifespan.

Moreover, Abhilasha et al. were introduced fuzzy logic tools for the energy-effective routing protocol. (Abhilasha *et al*., 2019) The proposed fuzzy logic tools and fuzzy decision rules select the CH and select the efficiency path for the BS. The results of the proposed approach are equated with existing procedures. The outcomes illustration that the suggested procedure gives improved performance than existing protocols for energy consumption. Furthermore, Liu et al. were introduced the IEE-LEACH (improved energy-effective LEACH) protocol (Liu *et al*., 2019) considered by the remaining SN energy and the normal vitality of the systems. To accomplish acceptable execution and lessen the node energy utilization, the IEE-LEACH was utilized. It represents the quantities of the ideal CHs and precludes SNs which are closer to the BS. Besides, the IEE-LEACH utilizes another edge for choosing CHs between the SNs and utilizes solitary bounce, multi-jump, and crossover correspondences to additionally increase the energy effectiveness of the systems.

Moreover, Kavita Jaiswal and Veena Anand were explained an EOMR (energy-efficient optimal multi-path routing) to increase the QoS in WSN (Kavita Jaiswal and Veena Anand., 2020) The proposed system consists of three-factor to choose the ideal path. The three factors are lifetime, dependability, and the traffic force at the following jump hub. The approach is simulated by NS-2. Additionally, the execution of the suggested approach is contrasted with other current procedures. The outcomes display that the suggested procedure achieves improved delay, energy-saving, PDR, and system lifespan contrasted with different procedures. Table 1 illustrates the evaluation of energy efficiency models.

Table 1. Comparison of Energy-aware Protocols

Method/Algorithm	Objective	Merits	Demerits
Swarm Clustering Algorithm	Energy-efficient in large scale network	Energy consumption is less	Delays the death time of the nodes
HADCC	Introduce the energy effective path scheduling process	Stability and Network lifetime	To enlarge the energy effectiveness in smaller system
Fuzzy Routing Protocol	Enhances the network life cycle	Throughput	-
IEE-LEACH	To increase the energy effectiveness of the networks	Reduces the energy utilization	High cost
EOMR	To increase the QoS in WSN	Energy-saving, PDR, and system lifespan	Delay in constrained applications

Table 2. Evaluation of security protocols in WSN

Method/Algorithm	Objective	Merits	Demerits
Key management protocol[116]	Analyzing the security issues and security requirements	Accuracy in security	Large number of nodes
ECDSA[117]	Safeguarding information on SNs for the duration of transmission in WSNs	Authentication, Session key arrangement, Secrecy, Un-traceability.	Survivability
Novel security Protocol[118]	Security for application, physical, network, data link, and service layers.	Network resiliency and reliability.	Jamming
Multi-factor confirmation systems[119]	Forward secrecy for actual information access in WSN	Accuracy	Limited Energy
Three-factor authentication[120]	A Secure and efficient protocol for WSN	Efficient security for attacks	High Cost

Survey of Security Protocols in WSN

Kumar et al. (Kumar *et al*., 2019) was explained security issues, security necessities, and examined and deliberated about particular key administration procedures for the secure communication of data, and contrasted them based on execution. It has given a detailed explanation of the WSN-related data to incredibly comprehend the idea of the system. Moreover, Rosheen Qazi et al. was introduced an Elliptic Curve Digital Sigquality (ECDSA) cryptographic plan to give a suitable component to estimating key management time, the tally of his message, and bundle size (Rosheen Qazi *et al*., 2020) Moreover, the Algorithm for Wireless Secure Communication (ASCW) likewise gives key administration adequate key length. Also, ASCW helps in getting the correspondence on node-level which helps in getting the entire network in a superior and proficient way. ASCW likewise decreases the expense of danger and security dangers on the network with the assistance of a validation component. A physical testbed has planned dependent on gadgets and sensor bits as per the necessary particulars. The proposed arrangements have been assessed regarding key management time, a few hi messages, and size of information parcels. In WSNs, the security problems were developed by Abdullah et al. along with agreeable correspondence on every layer of the OSI model (Abdullah *et al*., 2020) Various layers such as network, service, physical, application, and data link layers are considered. The main task is described for every layer and determines the fundamental assaults and dangers. Moreover, essential security methods are introduced to solve the new challenges and problems that can support valuable communications. In addition, particular assaults are described that utilizing valuable communication and it enhances the system's versatility and dependability. Wang et al presented an effective multi-factor authentication process that employs the unfair computational superiority of the RSA (Wang *et al*., 2020) It is valuable for circumstances, here SNs are the main energy blockage. Correlation outcomes show the prevalence of the plan. Apparently, it is the initial two-factor verification that conspires for continuous information access in WSNs that can fulfill each of the 12 standards of the current assessment metric beneath the severest for design. Lee et al. were introduced a secure and effective confirmation protocol dependent on three-factor verification by exploiting biometrics (Lee *et al*., 2020) In the interim, the suggested procedure utilizes a honey-list method to secure against savage power and taken smartcard assaults. By utilizing the honey-list method and three variables, undermined. Moreover, propose a productive protocol utilizing just hash capacities barring the public key-based elliptic bend cryptography. For security assessment of the projected validation protocol, the casual security examination, Real-Or-Random (ROR) model-based, and Burrows Abadi Needham (BAN) rationale based proper security examination are executed. Table 2 shows the comparison of security protocols in WSN.

The main contribution of this paper is to evaluate the performance of a novel energy-efficient and Secured protocol SA-LA (Dongarsane *et al*., 2021) for IoT with respect to security attacks, varied packet size, and the number of simulations by considering parameters like security risk probability, delay, residual energy hence network lifetime, IR and node trust factor (NTF).

Motivation

At present, there are several authenticity and encryption algorithms for the data in use on the internet but it will be essential to check their transferability to the internet of things. If a wireless sensor network (WSN) is integrated into the internet as a part of the Internet of things (IoT), there will appear new challenges, such as setup of a secure channel between a sensor node and an Internet host, energy-efficient routing of data to maximize WSN network lifetime. Hence such issues are still open for research in IoT.

Proposed Methodology

In this method, energy-efficient as well secured data transmission is done with the help of the SA-LA technique in the WSN-IoT framework. Different kinds of constraints like residual energy, delay, NTF, interference factor (IF), and security risk probability are considered as the objective function to perform an efficient routing. In order to obtain this efficient routing, developed an improved SA-LA algorithm also, Interference rate (IR) and Packet Drop Rate (PDR) are calculated to estimate the IR as well as PDR between every single node. Finally, different kinds of performance parameters are considered to obtain the efficiency of the proposed method by varying simulation ranges, attack ratios, and packet sizes.

System Model

The structure of secured energy-efficient protocol in the WSN-IoT system is displayed in Figure 1. Constraints like residual energy proposed IR and delay, NTF, and security risk probability are considered to select an optimal route for data transmission. During simulation, energy is uploaded in IoT in which energy in IoT is exploited in the initial stage. PDR and IR estimations are estimated in every single node to calculate IR and PDR. It is said that the value of PDR should be close to 1 and the value of IR should be adjacent to 0. SA-LA algorithm is utilized in the optimal path selection process in which routes with the shortest path are optimally selected by this algorithm.

Methodology

Creation of Nodes

In starting stage, the source node, destination node, other nodes, and their location, PDR, energy, and security are determined to generate nodes in the workspace. To resolve the interference problem, the interference ratio is estimated for every single link among the nodes. For normal nodes, the PDR value is set as one, and IR is set as 0 whereas the PDR value is set as 0.7 and IR is set as 0.1 for attacker nodes in the proposed framework. PDR is directly proportional to the security level of every node

Objective Function for Optimal Route Selection via SA-LA

Energy consumption, security risk probability, delay, interference factor, and node factor are considered as important objectives in the secured energy-efficient routing protocol

Node Trust Factor

Path confidentiality is estimated with the help of NTF (Othman *et al*., 2014). When complex data is stolen by a passive attacker, confidentiality tends to be nominal. Equation (1) represents this in a mathematical form where, count of packets received by every node in the path is mentioned N_P^R count of packets transmitted by the source, and the number of nodes in the path is denoted as N_P^S and N_p respectively.

$$NTF = \frac{\sum_{node} N_p^R}{N_p * N_p^S} \tag{1}$$

Proposed IF

Interference defines the capability to transmit the packets in a given period of time. Expression (2) is used to calculate the interference factor in which N_P^T mentions the number of packets to be forwarded and N_P^F denotes the number of forwarded packets.

$$IF = \frac{N_p^F}{N_p^T} \tag{2}$$

Conversely, an attacker means that the number of packets must be forwarded after dropping the number of packets as per PDR. Hence, packets

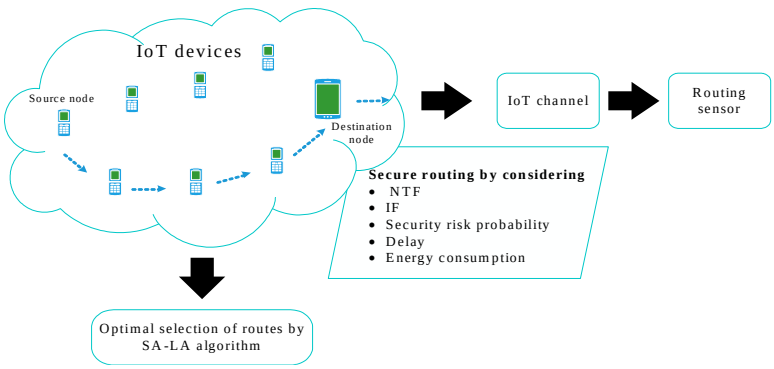

Figure 1. System model of the proposed technique in WSN-IoT framework

forwarded by the attacker must be equal to the packets to be forwarded as genuine. Therefore, Expression (3) defines the proposed IF in which packets forwarded by the previous node is mentioned as N_P^P and node count is signified as N.

$$IF = \frac{\frac{N_p^F}{N_p^T} \times \frac{N_p^T}{N_p^P}}{N} \tag{3}$$

Security Risk Probability

For secure data transmission, security risk (Liu *et al*., 2012) should be minimum. Secure mode, risky mode, and γ-risky mode are considered as security (*Se*) parameters.

Secure mode: This mode is selected when the security of the node is fulfilled by itself. In this mode, S_r and S_d The Development and is considered as a security requirement associated with nodes and security rank respectively. It is said to be secure, when the node reaches the state $s_d \le s_r$.

Risky mode: Node which takes all the feasible risks is named as risky mode and the mode is mentioned as aggressive in path selection.

γ-risky mode: It is defined as that the node that tolerates utmost all γ-risk. Accordingly, γ signify probability measures with values $\gamma = 0$ and $\gamma = 1$ (i.e., 100%) like the security and risky mode. Secure mode is considered an inexpensive one and the most employed mode is *γ-risky mode* between three modes (Liu *et al*., 2012). Very low (assigned as 1), low (assigned as 2), medium (assigned as 3), high (assigned as 4), and very high (assigned as 5) are 5 security levels assigned in Fuzzy scale. Equation 4 specifies the probability for security measures.

$$b_{risk} = \begin{cases} 0 & if \quad s_d - s_r \le 0 \\ 1 - e^{\frac{(s_d - s_r)}{2}} & if \quad 0 < s_d - s_r \le 1 \\ 1 - e^{\frac{3(s_d - s_r)}{2}} & if \quad 1 < s_d - s_r \le 2 \\ 1 & if \quad 2 < s_d - s_r \le 5 \end{cases} \tag{4}$$

Risk becomes less than 50% when the selected node reaches to state $S_d > S_r$. The selection process is completed when it reaches $0 < s_d - s_r \le 1$ and delay occurs in the selection process when $1 < s_d - s_r \le 2$.

Energy Consumption / Dissipation Ratio

In IoT, energy consumption is considered a big problem while transferring information. Furthermore, consumed energy must not be recharged and the transmission must fail due to the low battery in the node. Different functions like sensing, aggregating, transmitting, and receiving must captivate additional energy in the whole network. Equation 5 represents the energy requirement used in the data transmission. Where, $E_T(Qv)$ mentions the total used energy required to transmit Q bytes of packets at distance v and electronic energy depends on diverse constraint is mentioned as. E_g Expression (6) signifies the electronic energy in which utilized energy during data aggregation is mentioned as E_d. Equation (7) signifies the total utilized energy required to get Q bytes of packets at distance v and energy essential for amplification is explained by Equation (8).

$$E_T(Q:v) = \begin{cases} E_g * Q + E_f * Q * v^2, if \ v < v_0 \\ E_g * Q + E_p * Q * v^2, if \ v \ge v_0 \end{cases} \tag{5}$$

$$E_g = E_T + E_d \tag{6}$$

$$E_R(Q:v) = E_g Q \tag{7}$$

$$E_a = E_f v^2 \tag{8}$$

$$v_o = \sqrt{\frac{E_f}{E_p}} \tag{9}$$

In Expression (5), v_o is estimated based on equation (5), the energy of power amplifier is signified as E_p and E_f denotes the needed energy while developing a free space model. Expression (10) signifies the whole network energy in which energy required during the idle state is denoted as E_{id}, and cost of energy during sensing process is mentioned as E_{sen}. Based on Expression (10), it is a must to reduce total energy utilization.

$$E_{tot} = E_T + E_R + E_{id} + E_{sen} \tag{10}$$

Proposed Delay

While data transmission, delay metric is used to measure the average end-to-end delay (e2e). The function of hop count and distance is represented as a delay. Expression (11) is used to compute this in which path hub is signified as P_{Hub}, the number of nodes is denoted as N, the distance between source and destination is mentioned as Dis and PS mentions the propagation speed of light.

$$D = \frac{P_{Hub}}{N} * \frac{Dis}{PS} \quad (11)$$

Objective Function

Primary constraints like IF, security risk probability, delay, NTF, and energy consumption are considered to recognize the optimal route for data transmission. Thus, Equation (13) signifies all the constraints into a single objective function.

$$F = \begin{bmatrix} w_1 * (1 - NTF) + w_2 * (1 - IF) + \\ w_3 * Se + w_4 * (1 - E) + w_5 * D \end{bmatrix} \quad (12)$$

$$OB = \min(F) \quad (13)$$

Route Selection Phase

The routing server has no attacker data at simulation $t = 1$ so, IR is set as zero, and PDR is set as one for all nodes. Consequently, IR is 0 and PDR is 1 for initial data transmission. PDR and IR are calculated for additional data transmission through nodes (from $t = 2,..T; T = 10$) and data transmission takes place with calculated PDR and IR values.

PDR Valuation

With the selected route, each node forwards their packets and received packets from previous nodes. Equation (14) is used to calculate PDR in which packets forwarded by node i is mentioned as P_i^F and packets received by node i is mentioned as P_i^R

$$PDR = \frac{P_i^F}{P_i^R} \quad (14)$$

IR valuation: Equation (15) is used to estimate the IR among every single node in which P_{i+1}^R mentions the packets received by the next node $i+1$

$$PDR = \frac{P_{i+1}^R}{P_i^F} \quad (15)$$

Expressions (14) and (15) are used to calculate PDR and IR among every node from $t = 2,...T$ to transfer the data.

Solution Encoding

As per Figure 2, nodes expect source and destination are taken as input solutions to the adopted model. A hundred nodes are taken for the evolution while source and destination are not considered as solutions so, the number of nodes is set as 98. Here, $N = 2,3,4,...99; N \in (0,1)$, in which binary variable is mentioned as N. Accordingly, nodes with 1's are selected for data transmission and remaining nodes with 0's are dropped.

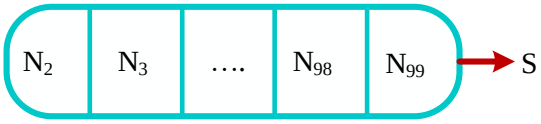

Figure 2. Solution encoding

Proposed SA-LA model

In this chapter, optimal route selection is done with the help of a novel SA-LA technique. In out-dated optimization techniques, self-enhancement is considered as a promising one (Rajakumar, 2013a; Rajakumar, 2013b; Swamy *et al*., 2013; George and Rajakumar, 2013; Rajakumar and George, 2012). Cub generation, pride generation, territorial takeover and territorial defense are four different phases in the proposed technique (Rajakumar, 2012). In this algorithm, the solution vector is signified as S which is represented as $S = [s_1, s_2, ...s_{\hat{m}}]$.

Generation of pride: Pride initialization takes place with a lioness S^{fem}, nomadic lion S^{nd} and territorial lion S^{mal}. Here, s_{len}^{fem}, s_{len}^{mal} and s_{len}^{nd} are random integers which lie in the within the limits when $\hat{m} > 1$ and $len = 1,2,..., Len$. Equation (16) defines the length (Len) of lion in which $\hat{n}$ and $\hat{m}$ signifies the variable. Expressions (17) and (18) are satisfied once $\hat{m}$ becomes one and Equation (19) specifies $V(s_{len})$

$$Len = \begin{cases} \hat{m}; & \hat{m} > 1 \\ \hat{n}; & otherwise \end{cases} \quad (16)$$

$$V(s_{len}) \in (s_{len}^{\min}, s_{len}^{\max}) \quad (17)$$

$$\hat{n}\%2 = 0 \quad (18)$$

$$V(s_{len}) = \sum_{len=1}^{Len} s_{len} 2^{\left(\frac{Len}{2} - len\right)} \quad (19)$$

Calculation of fertility: Here, S^{fem} and S^{mal} can reach local or global optimum once they get saturated but can't achieve the best solution. Laggard is observed as S^{mal} and La_r is mentioned as laggardness rate while $q(S^{mal})$ is far from q^r which is represented as fitness value. Sterility rate St_r specifies the fertility of S^{fem} whereas St_r is superior to tolerance St_r^{max} and Equation (20) is used to update S^{fem}. In Expression (20) and (21), S_d^{fem} and S_{len}^{fem+} are assumed as d^{th} and len^{th} vector components of S^{fem+}

$$s_{len}^{fem+} = \begin{cases} s_d^{fem+} & if\ \ len = d \\ s_{len}^{fem} & otherwise \end{cases} \quad (20)$$

$$s_{len}^{fem+} = \min[\, s_d^{\max}, \max(s_d^{\min}, \nabla d)] \quad (21)$$

$$\nabla d = \left\lfloor s_d^{fem} + (0.1\breve{r}_2 - 0.05)(s_d^{mal} - \breve{r}_1 s_d^{fem}) \right\rfloor \quad (22)$$

Here, arbitrary parameters are mentioned as $\breve{r}_1$ and $\breve{r}_2$ which ranges between (0, 1), female lion update is signified as ∇ and parameter d lies between $[1, len]$.

Mating: In the mating stage, crossover and mutation are assumed as an initial processes after that gender-oriented clustering is performed. Cubs are generated by the crossover and mutation function in which S^{cubs} and S^{new} indicates that the cubs are generated from crossover and mutation operation. During pregnancy time four cubs are generated and the other four cubs are produced from the crossover. Additionally, to produce four new cubs, the mutation is applied over those four cubs.

Lion operators: Survival fight generates the coalition update which signifies the territorial defence. The territorial defence is addressed by survival fight, which produces coalition updates. Expressions (23) to (25) are performed to select S^{e-nd}.

$$q(S^{e-nd}) < q(S^{mal}) \quad (23)$$

$$q(S^{e-nd}) < q(S^{mal\_cub}) \quad (24)$$

$$q(S^{e-nd}) < q(S^{fem\_cub}) \quad (25)$$

Proposed Nomad lion Update: Update of nomad lion takes place based on the proposed SA-LA technique. Based on Equation (26), nomadic lion update occurs when the trail is greater than the maximal age of cubs $A^{\max}$ otherwise, Equation (27) is used to update the nomadic lion position.

$$S^{nomad} = (0.5S^{mal}) + (0.25S^{mal\_cub}) + (0.25S^{mal}) \quad (26)$$

$$S^{nomad} = (0.5S^{fem}) + (0.25S^{fem\_cub}) + (0.25S^{fem}) \quad (27)$$

If S^{mal_cub} and S^{fem_cub} gets matured then territorial takeover helps to update S^{mal} and S^{fem}, that is cub's age is superior to $A^{\max}$.

Termination: After obtaining Equations (28) and (29), the model gets stopped. Besides, generation count is signified as it.

$$it > it_{\max} \quad (28)$$

$$h(S^{mal}) - h(S^{opt}) \le er_{th} \quad (29)$$

Here, $it_{\max}$ and er_{th} mentions the threshold and maximal generations for error respectively and optimal solution is signified as S^{opt}.

Results and Discussions

Experimental Setup

MATLAB R2018b tool was used to perform a secured energy-efficient routing protocol and simulation results were obtained from that tool. Intel i3 processor PC with 6/500 GB memory machine is used for simulation. In simulations, a 100m size sensor field is created. Where sensor nodes (100) have essential energy E_0 are subjectively positioned to examine SA-LA protocol. The table below shows the simulation parameters considered to create WSN.

Accordingly, the performance of adopted work was compared over the other approaches like CSSA (Vinitha *et al*., 2019) GAOC (Verma *et al*., 2019); DSOT (Meenaakshi Sundhari and Jaikumar, 2020), and MOFL (Bhardwaj and Kumar, 2019). Here, validation was carried out with respect to varied measures like residual energy, delay, network lifetime, and throughput (Alazzawi and Elkateeb, 2008). The study was carried out for a varied attack ratios that range from 5, 10, 15, 20, and 25 then for varied packet sizes of 100, 150, 200, 250, and 300 and results were observed as well as for a varied number of simulations.

Performance Analysis with respect to Attack Ratio

When compared to existing methods, the residual energy is higher for our proposed method which confirms that the proposed algorithm achieves additional energy with every node in WSN. As shown in Figure 3(a) the proposed method obtains 0.476 as residual energy at attack ratio 15 which is 27.38%, 29.55%, 27.38%, and 60.56% higher than MOFPL, DSOT, GAOC, and CSSA methods. With attack ratio 20, the proposed method obtains minimum delay as in Figure 3(b) in which the existing methods like CSSA, GAOC, DSOT, and MOFPL come with 30.95%, 55.62 %, 56.64%, and 71.43% higher delay respectively. Network lifetime based on this energy utilization of nodes. As shown in Figure 3(c) the proposed method obtains extended network life time for attack ratio of 2 as well as 5 but in some places, it is reduced also.

Throughput analysis with respect to different attack ratios is illustrated in Figure 3(d). When compared to existing methods, the proposed one is 44.92%, 42.37%, 40.68%, and 40.68% greater than MOFPL, DSOT, GAOC, and CSSA at attack ratio 10. Overall, the proposed methodology outperforms all existing methods in terms of different attack ratios.

Performance Evaluation with respect to Packet size

This subsection explains the performance comparison of NTF, IF, throughput, delay, network lifetime, security, and residual energy by means of varying packet sizes like 100, 150, 200, 250, and 300. In Table 3, the proposed method obtains a higher network lifetime for all packet sizes in which the existing methods obtain less network lifetime. With packet size 100, the performance of the proposed method is 3.49%, 4.71%, 14.1%, and 1.14% greater than MOFPL, DSOT, GAOC, and CSSA algorithms. The proposed method obtains 0.297 as residual energy at 200 packet size which is 27.38%, 29.55%, 27.38%, and 60.56% higher than

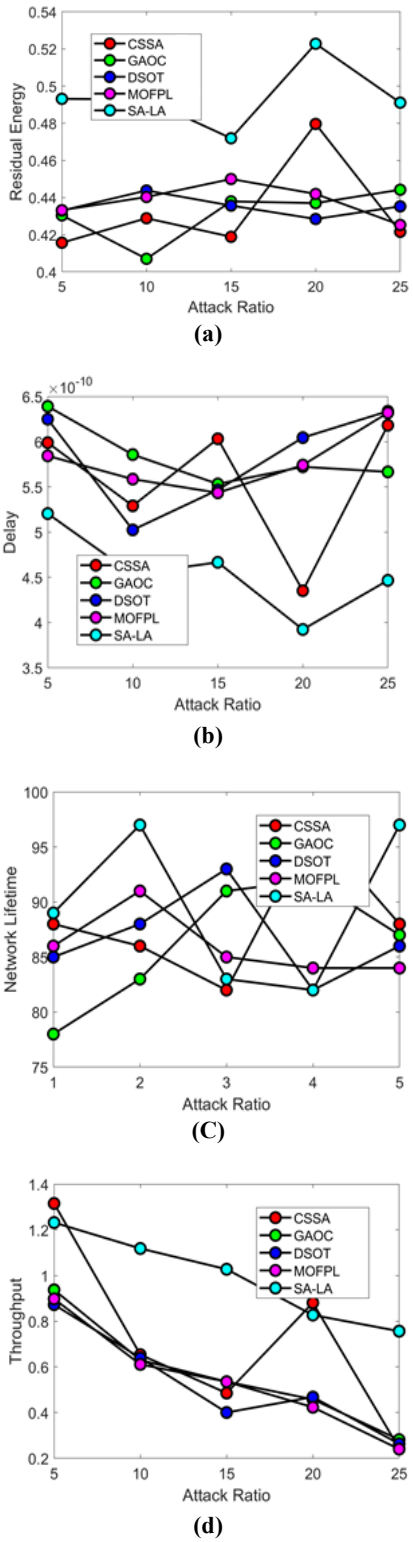

Figure 3. Analysis on (a) Residual Energy (b) Delay (c) Network lifetime and (d) Throughput attained by the implemented model over existing models with respect to attack ratio

MOFPL, DSOT, GAOC, and CSSA methods. When compared to conventional approaches, delay and security risk is lower for the proposed method with all packet size which confirms that the proposed method is the superior one.

At packet size 100, the proposed method obtains 5.2054×1010 as minimal risk probability which is 10.92%, 16.71%, 18.55%, and 13.09% superior to MOFPL, DSOT, GAOC, and CSSA methods. From all analysis, we can say that the proposed method is reliable to perform an efficient secured data routing in the WSN-IoT framework.

Performance Evaluation with respect to no of simulation

Table 3.1 shows the performance evaluation of NTF, IF, Security risk probability, and Table 3.2 shows residual energy, delay and network lifetime in terms of a varying number of simulations. The simulation number is varied from 1 to 10. In this analysis, the performance of the SA-LA method is compared with existing methods like CSSA, GAOC, DSOT, and MOFPL. At simulation number 2, the proposed method, as well as existing methods, achieve 1 as trust factor but in simulation number 4, the proposed method achieves 1 as trust factor while CSSA, GAOC, DSOT, and MOFPL achieves 0.65, 0.78, 0.8, and 0.8 as trust factor which is less than proposed methodology. When compared to all existing methods, the proposed SA-LA technique achieves a trust factor as one in every simulation. In IF analysis, the proposed SA-LA method obtains 1 as IF while conventional approaches like CSSA, GAOC, DSOT, and MOFPL achieve 0.989,1, 0.995, 1, and 1 as IF in simulation 4. GAOC and MOFPL approach achieve the same IF as the proposed SA-LA method. But in simulation 6, CSSA, GAOC, DSOT, and MOFPL accomplishes 0.995, 0.998, 0.994, and 0.994 as inference rate while the proposed achieves 1 as IF. Overall, the proposed SA-LA method is better in terms of IF. In security risk probability analysis, proposed SA-LA achieves

Table 3. Performance analysis of proposed SA-LA over existing algorithms for varied packet sizes

Network lifetime					
Methods	CSSA (35)	GAOC (37)	DSOT (36)	MOFPL (39)	SA-LA
Packet=100	88	78	85	86	89
Packet=150	33	43	46	43	58
Packet=200	14	24	26	24	45
Packet=250	9	10	17	13	61
Packet=300	10	14	11	8	33
Residual Energy					
Packet=100	0.41572	0.43044	0.43301	0.43322	0.49314
Packet=150	0.2796	0.32145	0.3213	0.32995	0.40254
Packet=200	0.18498	0.23316	0.22925	0.23358	0.297
Packet=250	0.15326	0.16433	0.19342	0.17257	0.33757
Packet=300	0.073875	0.10106	0.083451	0.062445	0.19218
Delay					
Packet=100	5.9896×10^{10}	6.3912×10^{10}	6.2494×10^{10}	5.8437×10^{10}	5.2054×10^{10}
Packet=150	5.2543×10^{10}	4.947×10^{10}	4.8586×10^{10}	5.0054×10^{10}	4.0475×10^{10}
Packet=200	4.597×10^{10}	4.6577×10^{10}	4.4255×10^{10}	4.4608×10^{10}	3.3774×10^{10}
Packet=250	3.9412×10^{10}	3.8882×10^{10}	3.7825×10^{10}	3.7842×10^{10}	2.5742×10^{10}
Packet=300	3.9228×10^{10}	3.9318×10^{10}	3.8201×10^{10}	4.079×10^{10}	3.2552×10^{10}
Security (risk probability)					
Packet=100	5.9896×10^{10}	6.3912×10^{10}	6.2494×10^{10}	5.8437×10^{10}	5.2054×10^{10}
Packet=150	5.2543×10^{10}	4.947×10^{10}	4.8586×10^{10}	5.0054×10^{10}	4.0475×10^{10}
Packet=200	4.597×10^{10}	4.6577×10^{10}	4.4255×10^{10}	4.4608×10^{10}	3.3774×10^{10}
Packet=250	3.9412×10^{10}	3.8882×10^{10}	3.7825×10^{10}	3.7842×10^{10}	2.5742×10^{10}
Packet=300	3.9228×10^{10}	3.9318×10^{10}	3.8201×10^{10}	4.079×10^{10}	3.2552×10^{10}
Trust factor					
Packet=100	0.89579	0.92961	0.87337	0.91573	1
Packet=150	0.92406	0.94989	0.88074	0.90547	1
Packet=200	0.95571	0.95058	0.96062	0.94404	1
Packet=250	0.95836	0.97088	0.97056	0.97268	1
Packet=300	0.96698	0.96165	0.97995	0.92787	1
Interference factor					
Packet=100	0.99594	0.99733	0.9955	0.99671	1
Packet=150	0.99682	0.99766	0.99344	0.99612	1
Packet=200	0.99685	0.9933	0.99631	0.99424	1
Packet=250	0.98697	0.99263	0.99281	0.98762	1
Packet=300	0.9932	0.99075	0.99572	0.99371	1
Throughput					
Packet=100	1.3157	0.9373	0.8727	0.89784	1.232
Packet=150	0.9413	1.0109	0.95215	0.99631	1.3466
Packet=200	1.0294	1.0695	1.1485	1.0944	1.2238
Packet=250	1.1533	1.066	1.1712	1.0781	1.5684
Packet=300	1.0283	1.1213	1.1046	1.0293	1.4136

less risk probability as 0.04 while CSSA, GAOC, DSOT, and MOFPL obtain 0.25, 0.24, 0.24, and 0.25 as risk probability which is greater than the proposed one at simulation 2. In the 10th simulation, CSSA and the proposed method obtain almost the same risk probability while GAOC, DSOT, and MOFPL obtain 0.35, 0.39, and 0.25 values as risk probability. In residual energy comparison, the proposed method consumes 0.35% energy while existing like CSSA, GAOC, DSOT and MOFPL consume 0.25, 0.22, 0.23, and 0.23 at simulation 10. When compared to existing methods, the proposed method consumes less energy. The proposed SA-LA method takes 5.65×10^{10} seconds to complete the routing process whereas CSSA, GAOC, DSOT, and MOFPL take 3.99×10^{-10}, 6.59×10^{-10}, $5.98\times10^{-10}$and 6.25×10^{-10} seconds to complete the process at simulation number 10. This is comparatively less for the proposed method. In terms of network lifetime, the proposed method achieves a better network lifetime when compared to existing methods in all simulations. Overall, the proposed method outperforms all existing methods by means of security risk probability

Statistical Significance

The statistical significance of the proposed SA-LA protocol is shown in the following tables using t-test method. We Considered all the required performance parameters one by one and represented them in comparison with similar methods. So, we can observe the performance of SA-LA is always superior as compare to others for all test conditions.

Table 3.1 Performance evaluation of NTF, IF, and Security risk probability against no of simulation in SA-LA method

NTF					
No of simulation	2	4	6	8	10
CSSA	1	0.65	0.9	0.82	1
GAOC	1	0.78	1	0.7	0.8
DSOT	1	0.8	0.84	0.9	0.7
MOFPL	1	0.8	0.85	0.74	0.91
SA-LA	1	1	1	1	1
IF					
No of simulation	2	4	6	8	10
CSSA	1	0.989	0.995	0.992	1
GAOC	1	1	0.998	1	1
DSOT	1	0.995	0.994	0.993	0.992
MOFPL	1	1	0.994	0.995	0.993
SA-LA	1	1	1	1	1
Security					
No of simulation	2	4	6	8	10
CSSA	0.25	0.23	0.24	0.32	0.09
GAOC	0.24	0.15	0.34	0.24	0.35
DSOT	0.24	0.23	0.3	0.36	0.39
MOFPL	0.25	0.26	0.23	0.26	0.25
SA-LA	0.04	0.05	0.06	0.07	0.09

Table 3.2 Performance evaluation of delay, network lifetime and residual energy against no of simulation in SA-LA method

Residual energy					
No. of simulation	2	4	6	8	10
CSSA	0.65	0.53	0.38	0.3	0.25
GAOC	0.65	0.50	0.40	0.33	0.22
DSOT	0.65	0.48	0.40	0.33	0.23
MOFPL	0.65	0.50	0.40	0.30	0.23
SA-LA	0.66	0.55	0.48	0.42	0.35
Delay					
No of simulation	2	4	6	8	10
CSSA	$7.45\text{x}10^{-10}$	$6.58\text{x}10^{-10}$	$7.88\text{x}10^{-10}$	$4.00\text{x}10^{-10}$	$3.99\text{x}10^{-10}$
GAOC	$6.44\text{x}10^{-10}$	$5.89\text{x}10^{-10}$	$7.26\text{x}10^{-10}$	$6.59\text{x}10^{-10}$	$6.59\text{x}10^{-10}$
DSOT	$5.56\text{x}10^{-10}$	$9.88\text{x}10^{-10}$	$7.96\text{x}10^{-10}$	$5.59\text{x}10^{-10}$	$5.98\text{x}10^{-10}$
MOFPL	$6.56\text{x}10^{-10}$	$6.56\text{x}10^{-10}$	$4.98\text{x}10^{-10}$	$5.89\text{x}10^{-10}$	$6.25\text{x}10^{-10}$
SA-LA	$4.3\text{x}10^{-10}$	$6.32\text{x}10^{-10}$	$4.98\text{x}10^{-10}$	$5.51\text{x}10^{-10}$	$5.65\text{x}10^{-10}$
Network lifetime					
No of simulation	2	4	6	8	10
CSSA	100	100	100	98	88
GAOC	100	100	100	95	78
DSOT	100	100	100	96	84
MOFPL	100	100	100	97	85
SA-LA	100	100	100	100	89

Network Lifetime:

	CSSA	GAOC	DSOT	MOFPL	SA-LA
Best	100	100	100	100	100
Worst	88	78	85	86	89
Mean	97.8	96	97.1	97.9	98.6
Median	100	100	100	100	100
STD	3.9101	7.5277	5.2799	4.4833	3.5024

Residual Energy:

	CSSA	GAOC	DSOT	MOFPL	SA-LA
Best	0.65161	0.65367	0.65161	0.65161	0.65984
Worst	0.24696	0.21813	0.23048	0.22534	0.32418
Mean	0.41572	0.43044	0.43301	0.43322	0.49314
Median	0.38956	0.42972	0.42663	0.42663	0.49356
STD	0.14338	0.1442	0.14222	0.14176	0.11373

Delay:

	CSSA	GAOC	DSOT	MOFPL	SA-LA
Best	1.5803×10^{-10}	5.6311×10^{-10}	5.094×10^{-10}	4.1297×10^{-10}	4.2784×10^{-10}
Worst	8.6058×10^{-10}	7.3248×10^{-10}	8.5117×10^{-10}	6.7932×10^{-10}	6.2761×10^{-10}
Mean	5.9896×10^{-10}	6.3912×10^{-10}	6.2494×10^{-10}	5.8437×10^{-10}	5.2054×10^{-10}
Median	6.5032×10^{-10}	6.4838×10^{-10}	5.9597×10^{-10}	6.1515×10^{-10}	5.2392×10^{-10}
STD	2.1793×10^{-10}	5.4279×10^{-10}	1.1227×10^{-10}	7.8948×10^{-10}	7.2734×10^{-10}

Security:

	CSSA	GAOC	DSOT	MOFPL	SA-LA
Best	0.098367	0.15976	0.20424	0.16923	0.011573
Worst	0.32062	0.35432	0.3829	0.30953	0.087132
Mean	0.23933	0.23751	0.2683	0.24196	0.052776
Median	0.24508	0.22561	0.24373	0.24678	0.056143
STD	0.057015	0.063472	0.062136	0.038517	0.02339

Node Trust Factor:

	CSSA	GAOC	DSOT	MOFPL	SA-LA
Best	1	1	1	1	1
Worst	0.65448	0.70065	0.70558	0.74038	1
Mean	0.89579	0.92961	0.87337	0.91573	1
Median	0.89751	1	0.86009	0.95761	1
STD	0.11399	0.11638	0.12208	0.1046	0

Interferance Factor:

	CSSA	GAOC	DSOT	MOFPL	SA-LA
Best	1	1	1	1	1
Worst	0.98966	0.98696	0.98605	0.99167	1
Mean	0.99594	0.99733	0.9955	0.99671	1
Median	0.995	1	0.99467	0.99712	1
STD	0.0038493	0.0046279	0.0045926	0.0035345	0

Throughput:

	CSSA	GAOC]	DSOT	MOFPL	SA-LA
Best	5.3262	1.2248	1.2879	1.2487	1.3712
Worst	0.43917	0.50262	0.60938	0.56015	0.90523
Mean	1.3157	0.9373	0.8727	0.89784	1.232
Median	0.86216	0.9877	0.84514	0.87881	1.2846
STD	1.449	0.20169	0.19504	0.21188	0.16031

Conclusion

Energy consumption and security are integrated in this paper to develop a novel secure and efficient routing protocol based on the SA-LA algorithm in the WSN-IoT framework. In the proposed SA-LA method, security risk probability, IF, NTF, delay, and residual energy are considered as objective functions to select an optimal route for data transmission. IR and PDR calculations are done to find the IR and PDR between every single node respectively. At long last, different performance metrics are taken to evaluate the efficiency of the proposed methodology by varying attack ratio, packet size, and simulation range. With packet size 100, the network lifetime of the proposed model is 3.49%, 4.71%, 14.1%, and 1.14% higher than existing MOFPL, DSOT, GAOC, and CSSA methods. The proposed model obtains 0.297 as higher residual energy which is 27.38%, 29.55%, 27.38%, and 60.56% greater than MOFPL, DSOT, GAOC, and CSSA by means of packet size 200. So at the end of the statistical analysis, we can say that when compared with the previous methods the proposed method obtains better performance in different parameters which assures secured (low risk) and energy-efficient (extended network lifetime) routing technique for WSN's on IoT platform. The overall computational complexity of Novel SA-LA is on quite higher side as the objectives function includes a large number of computations. In the future, a varying number of cluster analysis are performed in the data routing protocols to enhance the optimal level of hierarchy in the WSN framework. So, we can analyze how the lifetime of the network is reduced with a particular level of hierarchy and how the increasing number of cluster affect the lifetime of the network. Some sensor nodes in WSN misused the energy of its own by relying on others' data rather than utilizing its own data. So, it is also considered as another future area in which it must find any other way to limit the energy of the nodes.

Nomenclature

Abbreviation	Description
CSSA	Cat Salp Swarm Algorithm
DSOT	Dynamic Stochastic Optimization Technique
DTLS	Datagram Transport Layer Security
IoT	Internet of things
IR	Interference Ratio
GAOC	Genetic Algorithm-based Optimized Clustering
LT-SMM	Logical Tree-Based Secure Mobility Management Scheme
MOFPL	Multi-objective Fractional Particle Lion Algorithm
PDR	Packet Drop Rate
RRCB	Rectangular Rationale Correlated Bayesian
STO	Stochastic Optimization
SAKA	Secure Authentication and Key Agreement
WSNs	Wireless Sensor Networks
SA-LA	Self-Adaptive Lion Algorithm

References

Al Hayajneh, Abdullah, Md Zakirul Alam Bhuiyan, and Ian McAndrew. (2020). A novel security protocol for wireless sensor networks with cooperative communication, Computers, 9(1):4. https://doi.org/10.3390/computers9010004

Alazzawi L. and Elkateeb A. (2008). Ali. performance evaluation of the wsn routing protocols scalability. Journal of Computer Systems, Networks, and Communications, 1-10. https://doi.org/10.1155/2008/481046

Aslam, Muhammad, Ehsan Ullah Munir, Muhammad Bilal, Muhammmad Asad, Asad Ali, Tauseef Shah, and Syed Bilal. (2014). HADCC: hybrid advanced distributed and centralized clustering path planning algorithm for WSNs., In 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, 657-664. https://doi.org/10.1109/AINA.2014.81

Baig, Z.A., Sanguanpong, S., Firdous, S.N., Vo, V.N., and So-In, C. (2020). Averaged dependence estimators for DoS attack detection in IoT networks. Future Generation Computer Systems, 102:198-209. https://doi.org/10.1016/j.future.2019.08.007

Bhardwaj, R. and Kumar, D. (2019). MOFPL: Multi-objective fractional particle lion algorithm for the energy-aware routing in the WSN. Pervasive and Mobile Computing, 58:1-16. https://doi.org/10.1016/j.pmcj.2019.05.010

Bhoyar, P., Sahare, P., Dhok, S.B. and Deshmukh, R.B. (2018). Communication technologies and security challenges for internet of things: A comprehensive review. AEU - International Journal of Electronics and Communications, 99:81-99. https://doi.org/10.1016/j.aeue.2018.11.031

Dongarsane C.R., Maheshkumar D., Aravind H.S., Mallikarjunaswamy S., and Sankpal S.V. (2021). Design of Energy Efficient and Secured Routing Protocol for WSN in IoT. Design Engineering, 3,936-3,953.

George, A. and Rajakumar, B.R. (2013). APOGA: An adaptive population pool size based genetic algorithm, AASRI Procedia - 2013 AASRI Conference on Intelligent Systems and Control (ISC 2013), 4:288-296. https://doi.org/10.1016/j.aasri.2013.10.043

Ghaffari, Ali. (2014). An energy-efficient routing protocol for wireless sensor networks using A-star algorithm. Journal of applied research and technology, 12(4):815-822. https://doi.org/10.1016/S1665-6423(14)70097-5

Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., and Bentaleb, A. (2019). Enhanced authentication and key management scheme for securing data transmission in the internet of things. Ad Hoc Networks, 94:101948. https://doi.org/10.1016/j.adhoc.2019.101948

Jain, Abhilasha, and Ashok Kumar Goel. (2019). Energy-efficient fuzzy routing protocol for wireless sensor networks. Wireless Personal Communications, 110(3):1,459-1,474. https://doi.org/10.1007/s11277-019-06795-z

Jaiswal, Kavita and Veena Anand (2020). EOMR: An energy-efficient optimal multi-path routing protocol to improve QoS in wireless sensor network for IoT applications. Wireless Personal Communications, 1-23. https://doi.org/10.1007/s11277-019-07000-x

Kalkan, K. (2020). SUTSEC: SDN Utilized Trust-based Secure Clustering in IoT, Computer Networks, In press. journal pre-proof Available online, 107328. https://doi.org/10.1016/j.comnet.2020.107328

Kandi, M.A., Lakhlef, H., Bouabdallah, A, and Challal, Y. (2020). A versatile Key Management protocol for secure Group and Device-to-Device Communication in the Internet of Things. Journal of Network and Computer Applications, 150:102480. https://doi.org/10.1016/j.jnca.2019.102480

Kumar, Ranjit, Sachin Tripathi, and Rajeev Agrawal (2019). An analysis and comparison of security protocols on wireless sensor networks (WSN). In Design Frameworks for Wireless Networks, Springer, Singapore. 3-21. https://doi.org/10.1007/978-981-13-9574-1_1

Lee, Joonyoung, Sungjin Yu, Myeonghyun Kim, Youngho Park, and Ashok Kumar Das (2020). On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks. IEEE Access 8, 107046-107062. https://doi.org/10.1109/ACCESS.2020.3000790

Liu, H., Abraham, A., Snášel, V. and McLoone, S. (2012). Swarm scheduling approaches for work-flow applications with security constraints in distributed data-intensive computing environments. Information Sciences, 192. https://doi.org/10.1016/j.ins.2011.12.032

Liu, Yang, Qiong Wu, Ting Zhao, Yong Tie, Fengshan Bai, and Minglu Jin. (2019). An improved energy-efficient routing protocol for wireless sensor networks. Sensors, 19(20):4,579. https://doi.org/10.3390/s19204579

Meenaakshi Sundhari, R.P.and Jaikumar, K. (2020). IoT assisted Hierarchical Computation Strategic Making (HCSM) and Dynamic Stochastic Optimization Technique (DSOT) for energy optimization in wireless sensor networks for smart city monitoring. Computer Communications, 150:226-234. https://doi.org/10.1016/j.comcom.2019.11.032

Moin, S., Karim, A., Safdar, Z., Safdar, K. and Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Generation Computer Systems, 100:325-343. https://doi.org/10.1016/j.future.2019.05.023

Othman, S.B., Bahattab, A.A., Trad, A. and Yousse, H. (2014). Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption. Wireless Personal Communications, 80:867-889. https://doi.org/10.1007/s11277-014-2061-z

Qazi, Rosheen, Kashif Naseer Qureshi, Faisal Bashir, Najam Ul Islam, Saleem Iqbal, and Arsalan Arshad. (2020). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 547-566. https://doi.org/10.1007/s12652-020-02020-z

Rajakumar, B.R (2012). The Lion's Algorithm: A New Nature-Inspired Search Algorithm, Procedia Technology-2nd International Conference on Communication. Computing and Security, 6:126-135

Rajakumar, B.R and George, A. (2012). A New adaptive mutation technique for genetic algorithm, In Proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). 1-7 https://doi.org/10.1016/j.protcy.2012.10.016

Rajakumar, B.R. (2013a). Impact of static and adaptive mutation techniques on genetic algorithm. International Journal of Hybrid Intelligent Systems, 10(1):11-22. https://doi.org/10.3233/HIS-120161

Rajakumar, B.R.(2013b). Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis. International Journal of Computational Science and Engineering, 8(2):180-193. https://doi.org/10.1504/IJCSE.2013.053087

Swamy, S.M., Rajakumar, B.R, and Valarmathi, I.R. (2013). Design of hybrid wind and photovoltaic power system using opposition-based genetic algorithm with cauchy mutation IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), Chennai, India. https://doi.org/10.1049/ic.2013.0361

Tewari, A. and Gupta, B.B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoT) framework. Future Generation Computer Systems, 108:909-920. https://doi.org/10.1016/j.future.2018.04.027

Verma, S., Sood, N. and Sharma, A.K. (2019). Genetic Algorithm-based Optimized Cluster Head selection for single and multiple data sinks in Heterogeneous Wireless Sensor Network. Applied Soft Computing, 85:1-21. https://doi.org/10.1016/j.asoc.2019.105788

Vinitha, A., Rukmini, M.S.S. and Dhirajsunehra (2019). Secure and energy-aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm, Journal of King Saud University - Computer and Information Sciences, in press)

Wang, Ding, Ping Wang, and Chenyu Wang (2020). Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. ACM Transactions on Cyber-Physical Systems, 4(3):1-26. https://doi.org/10.1145/3325130