International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6585
Article Received: 14 February 2023 Revised: 28 March 2023 Accepted: 09 April 2023

Secure Cluster-based Routing using TCSA and Hybrid Security Algorithm for WSN

M.Supriya[1], Dr. T. Adilakshmi[2]
[1]HOD, Dept of Information Technology
Swami Vivekananda Institute of Technology, JNTUH
Secundrabad, India
supriyasamuel@yahoo.com
[2]Head, Dept of Computer Science and Engineering
Vasavi College of Engineering, Ibrahimpatnam , Osmania University
Hyderabad,India
t_adilakshmi@staff.vce.ac.in

Abstract— Wireless Sensor Network (WSN) is operated as a medium to connect the physical and information network of Internet-of-Things (IoT). Energy and trust are two key factors that assist reliable communication over the WSN-IoT. Secure data transmission is considered a challenging task during multipath routing over the WSN-IoT. To address the aforementioned issue, secure routing is developed over the WSN-IoT. In this paper, the Trust-based Crow Search Algorithm (TCSA) is developed to identify the Secure Cluster Heads (SCHs) and secure paths over the network. Further, data security while broadcasting the data packets is enhanced by developing the Hybrid Security Algorithm (HSA). This HSA is a combination of the Advanced Encryption Standard (AES) and Hill Cipher Algorithm (HCA). Therefore, the developed TCSA-HSA avoids malicious nodes during communication which helps to improve data delivery and energy consumption. The performance of the TCSA-HSA method is analyzed using Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), energy consumption, End to End Delay (EED), and throughput. The existing methods namely Optimal Privacy-Multihop Dynamic Clustering Routing Protocol (OP-MDCRP) and Secure and Energy-aware Heuristic-based Routing (SEHR) are used to evaluate the TCSA-HSA performances. The PDR of TCSA-HSA for 100 nodes is 99.7449%, which is high when compared to the OP-MDCRP and SEHR.
.

Keywords Secure Cluster Head, Packet Loss Ratio, hybrid Security algorithm, trust-based crow search algorithm, End to End delay, wireless sensor network.

I. INTRODUCTION

WSN is considered an integral part of the large-scale and effective installation of Internet-of-Things (IoT). The WSN is a set of a huge amount of sensor nodes and base station/ sink whereas the sensors have restricted storage, processing, and communication abilities [1]. In recent times, real-world objects and numerous network edge devices are combined with wireless sensors for collecting and monitoring real-time data. Accordingly, this structure has varied with the development of IoT [2]. IoT is one of the power system architectures that integrate the physical and the virtual worlds by utilizing the web as the mode for transmitting information between the physical and the virtual worlds [3]. The IoT has a huge number of objects such as sensors, RFID tags, mobile devices, and actuators which are linked to the internet over a wired/wireless connection [4]. Nowadays, internet devices exist in everyday human life such as real-time equipment monitoring, industrial supply chain management, safety production management, and environmental monitoring. It predicted that each person has connected to the internet with more than ten devices in the year 2050 [5] [6].

In WSN, rapid energy consumption is considered a primary problem due to limited battery levels. The sensing process of the nodes and the data transmitted over the nodes are affected when the node exhausts their energy in the network [7] [8]. Generally, the forwarding methods are categorized into two categories such as structure-free and structure-based approaches. In a structure-free approach, the sensor data is gathered without any fixed architecture, and accomplishes the data collection according to the partial information. On the contrary, the network is separated into various files namely clusters in the structure-based approach which helps to preserve the energy of the nodes [9] [10]. The sensors are formed into groups by a clustering process that gathers and transmits the data to the chosen Cluster Head (CH). Subsequently, the CH collects the data and broadcasted it to the BS that act as a bridge between the network and the end user [11] [12]. The sensors are generally located in the open and remote environment which creates the devices susceptible to security threats, specifically when malicious node attacks are occurring in the network [13]

[14]. Therefore, a secure routing approach is required to be developed to enhance the reliability during the data broadcasting over the network [15].

II. RELATED WORK

Kavitha, V [16] developed The Optimal Privacy-Multihop Dynamic Clustering Routing Protocol (OP-MDCRP). It improves data privacy and energy-efficient routing for the heterogeneous network and uses clustering and multi-hop communication to reduce the energy consumption of sensor nodes and increase the lifetime of WSN. The source nodes in the random network are classified into clusters according to the region. Strong data privacy is also provided by the system's use of the Elliptic Curve Integrated Encryption-Key Provisioning Mechanism (ECIES-KPM).

Karunkuzhali, D. et al. [17] implemented An ideal QoS-aware routing approach for smart cities using wireless sensor networks with IoT capabilities (OQR-SC). During the proposed system's data-gathering phase, the improved differential search serving as the cluster leader. The data transmission phase of an internet-of-things sensor pair is where data encryption is first shown. The optimal decision-making (ODM) method is then used in an IoT platform to find the best path between the source and destination.

Gali, S. and Nidumolu, V [18] developed a novel chaotic bumble bee mating optimization (CBBMO) technique named CBBMOR-TSM model for safe data transport. The BBMO is sparked by the bumble bee swarm's affinity for mating. The classic BBMO approach is combined with the chaotic idea in the CBBMO model to speed up the convergence of the BBMO a novel chaotic bumble bee mating optimization (CBBMO) technique named CBBMOR-TSM model for safe data transport technique. The suggested model's objectives are to develop a trust sensing model and carry out secure routing utilizing the CBMO algorithm.

Haseeb, K *et al.* [19] said Detecting and preventing data compromise with effective performance is the goal of the secure and energy-conscious heuristic-based routing (SEHR) protocol for WSN. First, the proposed protocol uses a heuristic analysis based on artificial intelligence to create a trustworthy, clever learning scheme. To achieve security with the least amount of complexity, it also safeguards communications against malicious parties. Moreover, traffic analysis is done in the route maintenance strategy to reduce network interruptions and link failures.

Gurupriya, M. and Sumathi, A [20] a hybrid optimal multipath routing approach for WSNs (HOFT-MP). We first describe the modified teaching-learning-based optimization (MTLO) technique to efficiently cluster the sensor nodes and improve energy efficiency. To expand the search space in the network that effectively computes node location, position, and sensor node movement direction, we combine teacher learning with fish swarm optimization (FSO). To identify node issues and boost fault tolerance, the backup node for clusters is calculated using the nonlinear regression-based pigeon optimization (NR-PO) method.

III. TCSA-HSA METHOD

This TCSA-HSA approach uses the Trust based CSA to find an SCH and secure path while avoiding malicious nodes. It is necessary to remove the rogue nodes from the network since they result in excessive energy consumption and packet loss. Using the HSA also improves data security while the data packets are being transmitted. The WSN-packet IoT's delivery and energy usage are thus improved by using both the TCSA and HSA. The block diagram of the TCSA-HSA method is shown in Figure 1.

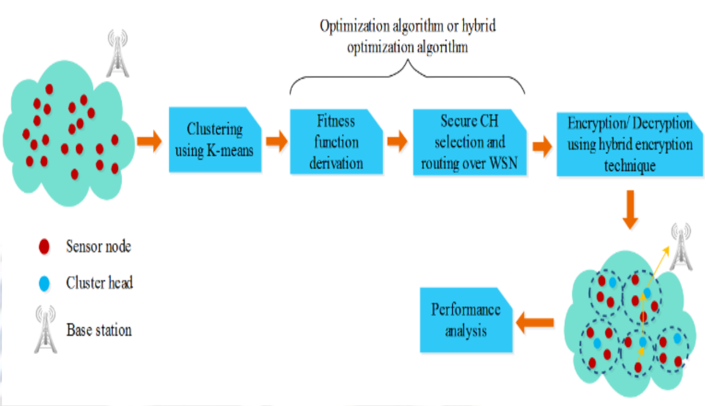

Optimization algorithm or hybrid optimization algorithm
Clustering using K-means
Fitness function derivation
Secure CH selection and routing over WSN
Encryption/ Decryption using hybrid encryption technique
Sensor node
Cluster head
Base station
Performance analysis

Fig1. Block diagram of the TCSA-HSA method

A. *K-means based clustering process*

At first, the nodes are randomly located in the WSN-IoT followed by the nodes being separated into various groups using the K-means clustering method. The Euclidian distance calculation between the nodes serves as the basic foundation for the K-means method in this instance. After network-based clustering is complete, the SCH choice and secure path discovery are carried out.

B. ***TCSA-based SCH selection***

The TCSA, which aids in mitigating malicious nodes, is used to select an ideal SCH from the clusters. Therefore, avoiding rogue nodes helps to reduce unnecessary energy usage and packet drops. A meta-heuristic algorithm called CSA(Crow Search Algorithm) [21] typically imitates the social behaviors of crows, including food-hiding, communication, and remembering. The following are the four main tenets of this CSA: Crows follow each other to carry out robberies, they live in flocks, they remember where food is hidden, they protect their caches from being stolen, and they follow each other to carry out robberies. The selection of SCH using TCSA is described as follows

***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 09 April 2023*

C. *Initialization of TCSA*

In this initialization phase, The collection of candidate nodes that must be chosen as SCH is included in TCSA's initialization. In the WSN-IoT, the total number of nodes is designated as S, and each crow is first initialized with a random node ID from 1 to S.Let, the ith crow of TCSA is $P_i = (P_{i,1}, P_{i,2}, \dots, P_{i,D})$, where D specifies the dimension of each crow (i.e., number of SCHs).

D. *Iterative process*

In TCSA, the ith crow has the capacity to follows the other jth crow for identifying the hidden food place. Here, the ith crow gradually updated the location in the searching process as well as the ith crow is required to update the food location, when it is stolen.

There are two different scenarios are accomplished in the CSA to update the location of the crows which are explained as follows:

In first scenario, the jth crow doesn't realized which is followed by ith crow. Thus, the ith crow approaches the hiding food location of jth crow. Equation (1) shows the ith crow's updated location P_i^{t+1}.

$$P_i^{t+1} = P_i^t + r_i \times fl_i^t \times (M_j^t - P_i^t) \tag{1}$$

Where, P_i^t represents the ith crow's location at iteration $t0$; fl_i^t specifies the flight length of the crow; r_i denotes the random number between 0 & 1, M_j^t denotes the memory matrix.

In the second scenario, the jth crow realized which is followed by ith crow. Thus, the jth crow betrays ith crow by moving to other random location over the search space, therefore, the ith crow's location is randomly chosen in the search space. Equation (2) shows the location updating process of scenario 1 and

$$P_i^{t+1} = \begin{cases} P_i^t + r_i \times fl_i^t \times \left(M_j^t - P_i^t\right) & if\ r_j \geq AP_i^t \\ a\ random\ location & otherwise \end{cases} \tag{2}$$

Where, the r_j denotes the random number generated within $[0, 1]$ and crow's awareness probability is denoted as AP_i^t. Equation (3) expresses the memory updating process of crows.

$$M_i^{t+1} = \begin{cases} P_i^{t+1} & if\ f(P_i^{t+1})\ is\ btter\ than\ f(P_i^t) \\ M_i^t & otherwise \end{cases} \tag{3}$$

Where, the objective function is represented as $f()$.

E. *3.2.3. How to derive the Fitness function*

When choosing the SCHs from the clusters, the TCSA takes into account the various fitness functions. TCSA takes into account four fitness measures: such as communication cost (fm_1), trust (fm_2), node degree (fm_3), and residual energy (fm_4) are considered in TCSA. The fitness function mentioned in equation (1) is expressed in the following equation (4).

$$S = \delta_1 \times fm_1 + \delta_2 \times fm_2 + \delta_3 \times fm_3 + \delta_4 \times fm_4 \tag{4}$$

Where each fitness measure has weight parameters that range from $\delta_1 - \delta_4$. The information about the fitness measures are given as follows:

- Equation(5) illustrates the necessary communication cost for interacting with the nearest node .

$$fm_1 = \frac{d_{avg}^2}{d_0^2} \tag{5}$$

Where, d_{avg}^2 represents the average distance between the sensor and the nearest node and d_0^2 is the distribution radius of the sensor. The primary goal for this CH selection is trust, as represented in equation (6). The nodes in the WSN communicate information based on a mutually trusted connection to prevent malicious assaults during data transmission. Here, the nodes' communication is used to calculate the trust. As a result,trust is defined by the packets that the node receives and the packets that the source node sends.

$$fm_2 = \frac{Packets\ received_{a,b}}{Packets\ sent_{a,b}} \tag{6}$$

Where, a and b are the example nodes.

- In addition, the node degree specifies the number of hops between the node and the CH. To achieve lower energy consumption, a lower node degree is used

$$fm_3 = \sum_{i=1}^{D} CM_i \tag{7}$$

Where, CM_i refers to the number of CMs associated to the ith CH.

- Data collection and transmission over the network are the responsibilities of the sensors. As a result, for data delivery, the node with the highest residual energy is preferred. The expression for residual energy can be seen in Equation 7.

$$fm_4 = \sum_{i=1}^{D} E_{SCH_i} \tag{8}$$

Where $E_{SCH_i}$is used to represent the ith SCH's residual energy.

The above fitness function is used to choose an appropriate Cluster Head. Due to their ability to cause packet drops throughout the network, malicious nodes are avoided using the trust model employed in fitness measurements. Then, the path with the shortest distance and lowest energy usage is determined using the communication cost. To determine if the node has enough energy to broadcast the data or not, the residual energy is analyzed. As a result, the network's packet delivery to the BS is enhanced. To reduce the nodes' energy consumption, the node degree was also taken into account.

F. Routing technique in TCSA

The route discovery is carried out utilizing the TCSA after choosing the SCH from the clusters. This TCSA uses AODV control messages like hello (HELLO), route request (RREQ), route reply (RREP), route error (RERR), and hello (RREQ) to find routes. Using the fitness function generated in the previous section and the constructed TCSA, the secure route is found. The source CH initially broadcasts the RREQ to all of the network's neighbouring CHs. The TCSA selects the best relay node to send the RREP message back to the starting CH. This process is repeated until the message reaches the destination node, BS. The secure route in the WSN was established when the source CH received the RREP message. Then the data packets are transmitted over the network. Moreover, this route discovery phase uses the HELLO and RERR for route maintenance.

G. Hybrid Security algorithm

After identifying the secure path using TCSA, the HSA is initialized for encrypting the data before transmission. The hybrid encryption technique, which combines Advanced Encryption Standard (AES) and Hill Cipher Algorithm(HCA), is used in this step to assure the security of the data. AES is one of the most secure symmetric encryption techniques generally, and the HCA further improves it. Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round-Key are some of the four main functions of the AES. The encryption is instead carried out using HCA using an invertible square matrix.

The following procedures carried out by this HSA are listed: Each byte in the block is switched using a predetermined lookup table known as the Substitution box at the beginning of the Sub-Bytes operation. Shift-Rows cyclically shift each byte in a data block by 0, 1, 2, or 3 positions. The 4 bytes in each column are then multiplied by a fixed matrix with constant entries as part of the Mix-Columns procedure. The Galois field GF(28) coefficients in this instance are multiplied and added. To create the output encrypted data, known as En, the input data is XORed with the key block cell by cell in the AddRoundKey operation. The output acquired from the AES is additionally encrypted with the HCA for improving security. Consider, the given input En is divided into two blocks as en_1 and en_2, accordingly the Key matrix is $HK_{2\times2}$. The ciphertext (En). generated by HCA (H_En) over the result of the AES encryption is expressed in equation (9)

if $En = \begin{bmatrix} en_1 \\ en_2 \end{bmatrix}$ and $HK = \begin{bmatrix} hk_{11} & hk_{12} \\ hk_{21} & hk_{22} \end{bmatrix}$ then

$$H_{En} = \begin{bmatrix} (hk_{11}en_1 + hk_{12}en_2) \ mod \ X \\ (hk_{21}en_1 + hk_{22}en_2) \ mod \ X \end{bmatrix} \qquad (9)$$

Where, the range of values given in the input is denoted as X.

H. Programming environment details:

Windows: Windows 7 ultimate
Processor: Intel (R) Core (TM) i5-3570 CPU @ 3.40GHz 3.80 GHz
RAM: 6 GB RAM
System type: 64-bit OS
Virtual machine: VMware Workstation Pro 14
Ubuntu version: ubuntu 16.04 LTS-64 bit

IV. RESULTS AND DISCUSSION

The outcomes of the TCSA-HSA method are discussed in this section.TCSA- HSA is implemented in the Network Simulator NS -2.34 using an i5 processor and 6GB RAM.
The NS-2.34 generally has two programming languages such as TCL at the front end and C++ at back whereas the network animator shows the node deployment. The simulation parameters utilized to analyze the secure data transmission using TCSA-HSA is given in the Table 1.

Parameters	Values
Simulator	NS-2.34
Area	300m × 300m
No. of nodes	50, 100, 150, 200 and 250
Initial energy	5J
Antenna pattern	Omni Antenna
Media Access Control	IEEE 802.11 DCP
Network Interface Type	WirlessPhy
Traffic source	Constant Bit Rate
Propagation model	Two-ray ground reflection

Table 1. Simulation parameters

Analysis of the TCSA-performance HSA's is done using PDR, PLR, energy use, EED, and throughput. The performance of TCSA-HSA is assessed using the SEHR [19] based routing.

A. PDR and PLR

Packet Delivery Ratio is the ratio between the number of received packets at the BS and the amount of generated packets by the source that is shown in equation (10). On the contrary, PLR is the ratio among the lost packets and sent packets which are simplified as shown in equation (11).

$$PDR = \frac{Amount\ of\ received\ packets\ at\ BS}{Amount\ of\ generated\ packets\ by\ source} \times 100 \qquad (10)$$

$$PLR = 100 - PDR \tag{11}$$

Figure 2 and 3 shows the comparison of PDR and PLR for TCSA-HSA with SEHR [19]. By changing the number of nodes, the performance is examined here. From the figures, it is known that the TCSA-HSA achieves better data delivery than the SEHR [19]. For example, PDR of the TCSA-HSA is 99.7449% for 100 nodes, whereas the SEHR [19] obtains the PDR of 91.5%. The combination of TCSA based secure routing and HSA based data security are used to avoid malicious threats while transmitting the data which is used to avoid packet loss over the WSN-IoT.

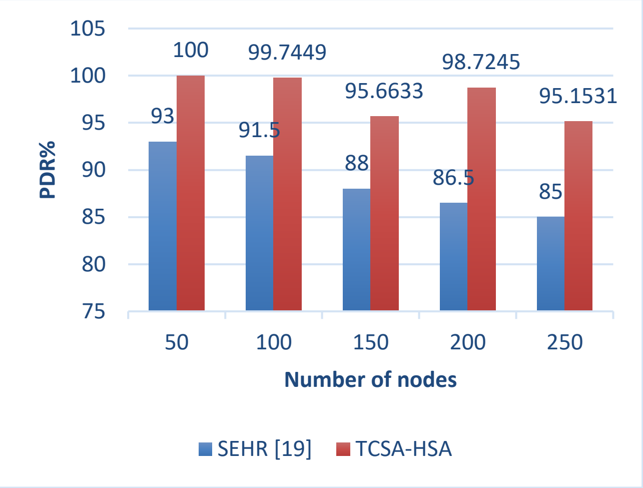


Figure2. Analysis of PDR

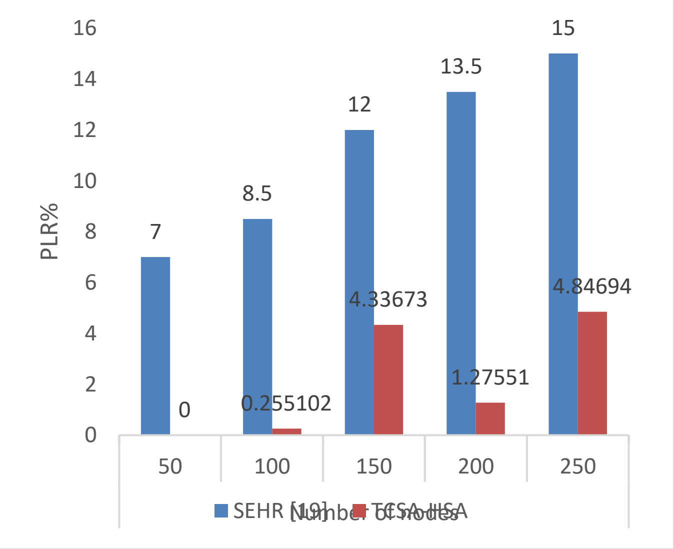


Fig 3. Analysis of PLR

B. . Energy consumption

The energy usage while transmitting and receiving the data packets are stated as the energy consumption (EC) of the WSN-IoT which is expressed in equation (12).

$$EC = E_{tr} + E_{rx} \tag{12}$$

Where, E_{tr} and E_{rx} are transmitting and receiving the energy of the nodes which are expressed in equation (13) and (14) respectively as per the energy model [19].

$$E_{tr} = \begin{cases} E_{elect} \times L + L \times E_{fs} \times d^2, & if\ d \leq d_t \\ E_{elect} \times L + L \times E_{amp} \times d^4, & if\ d > d_t \end{cases} \tag{13}$$

$$E_{rx} = E_{elect} \times L \tag{14}$$

Where, the transmission distance of the path is represented as d; the amount of consumed energy for a single bit is E_{elect}; amount of data bits is denoted as L; E_{fs} and E_{amp} denotes the free space and amplification energy, and threshold distance is represented as d_t.

The comparison of energy consumption for TCSA-HSA with SEHR [19] is shown in Figure 4. This Figure 4 shows that Less energy is used by TCSA-HSA than by SEHR [19]. In contrast to the SEHR [19], which achieves an energy usage of 0.018J, TCSA-HSA, for example, uses 0.00337J for 100 nodes. The shortest path generation and mitigation of malicious nodes using TCSA-HSA help to minimize the energy consumption of WSN-IoT.

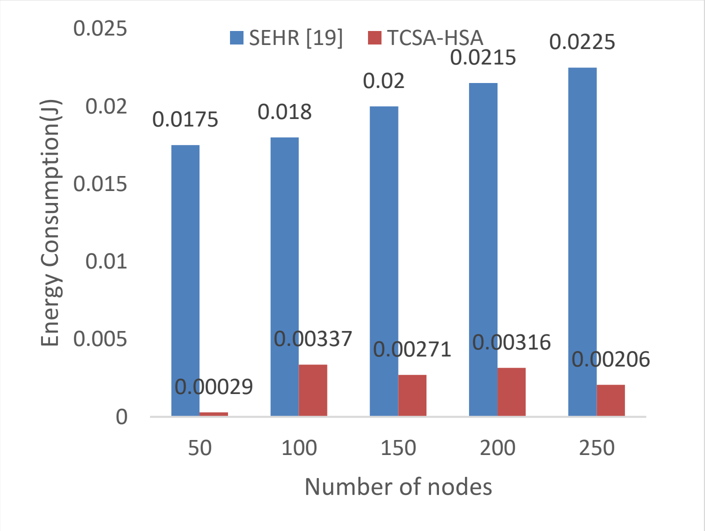


Fig 4. Energy consumption Vs No of nodes

C. End-to-end delay

According to the equation, EED is the proportion of the time needed for the sensor to send the data packet to the base station through the network (15).

$$EED = \frac{Sum\ of\ time\ taken\ to\ transmit\ packet\ to\ receiver}{Number\ of\ packet\ received\ by\ receiver} \tag{15}$$

SEHR [19] obtains the EED of 0.13ms. The TCSA with unique fitness measures is used to compute the optimal path with less amount of control packets which helps to minimize the EED.

***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 09 April 2023*

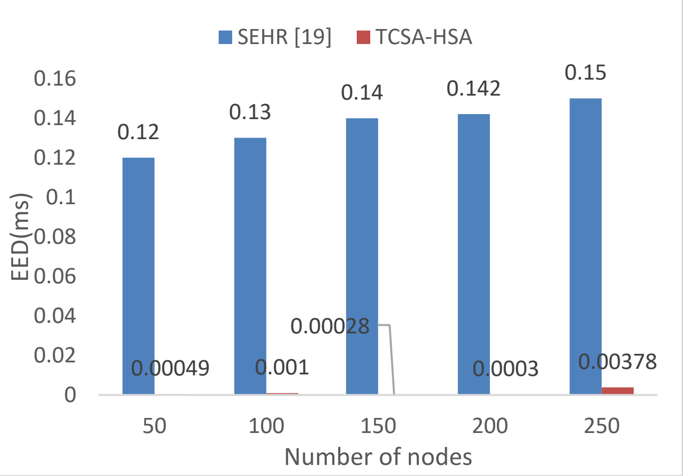


Fig 5. Analysis of EED

D. *Network throughput*

The number of packets the BS successfully receives in a certain length of time is referred to as throughput. Figure 6 illustrates the throughput comparison between TCSA-HSA and SEHR [19]. Changing the number of nodes allows for an analysis of the performance here. This Figure 6 shows that the In terms of throughput, the TCSA-HSA performs better than the SEHR [19]. For instance, SEHR [19] has a throughput of 90% while TCSA-HSA has a throughput of 99.5901 percent for 100 nodes.

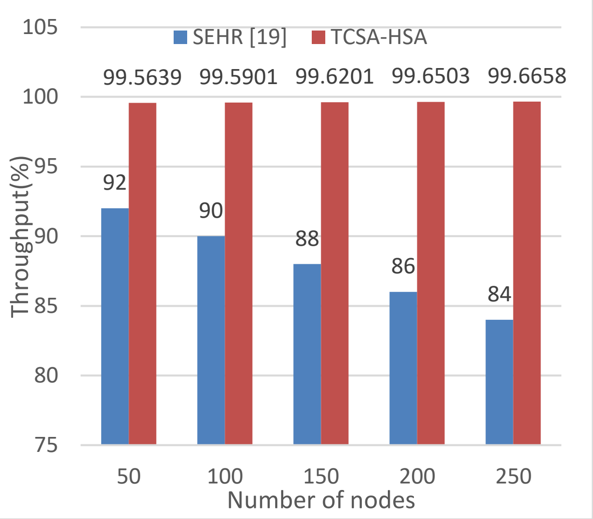
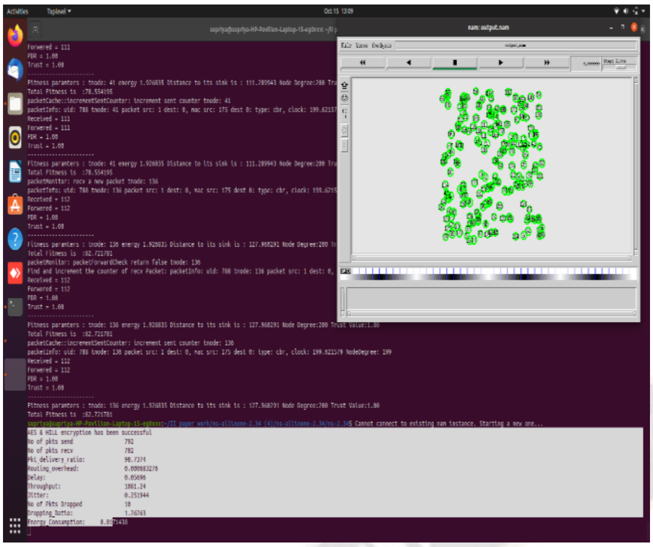


Fig 6. Analysis of throughput

and HSA improves the robustness against malicious attackers that helps to improve the successful data transmission over the WSN-IoT.

Performances	Methods	Number of nodes				
		50	100	150	200	250
PDR (%)	OP-MDCRP [16]	NA	98	NA	96	NA
	SEHR [19]	93	91.5	88	86.5	85
	TCSA-HSA	100	99.7449	95.6633	98.7245	95.1531
PLR (%)	OP-MDCRP [16]	NA	2	NA	4	NA
	SEHR [19]	7	8.5	12	13.5	15
	TCSA-HSA	0	0.255102	4.33673	1.27551	4.84694
Energy consumption (J)	SEHR [19]	0.0175	0.018	0.02	0.0215	0.0225
	TCSA-HSA	0.00029	0.00337	0.00271	0.00316	0.00206
EED (ms)	OP-MDCRP [16]	NA	0.023	NA	0.0265	NA
	SEHR [19]	0.12	0.13	0.14	0.142	0.15
	TCSA-HSA	0.00049	0.001	0.00028	0.00030	0.003780
Throughput (%)	SEHR [19]	92	90	88	86	84
	TCSA-HSA	99.5639	99.5901	99.6201	99.6503	99.6658

Table 2. Comparative analysis of TCSA-HSA



```
Forwered = 111
PDR = 1.00
Trust = 1.00
--------------------
Fitness paranters : tnode: 41 energy 1.926835 Distance to its sink is : 111.289943 Node Degree:200 Tru
Total Fitness is  :78.554195
packetCache::incrementSentCounter: increment sent counter tnode: 41
packetInfo: uid: 788 tnode: 41 packet src: 1 dest: 0, mac src: 175 dest 0: type: cbr, clock: 199.62157
Received = 111
Forwered = 111
PDR = 1.00
Trust = 1.00
--------------------
Fitness paranters : tnode: 41 energy 1.926835 Distance to its sink is : 111.289943 Node Degree:200 Tru
Total Fitness is  :78.554195
packetMonitor: recv a new packet tnode: 136
packetInfo: uid: 788 tnode: 136 packet src: 1 dest: 0, mac src: 175 dest 0: type: cbr, clock: 199.6215
Received = 112
Forwered = 112
PDR = 1.00
Trust = 1.00
--------------------
Fitness paranters : tnode: 136 energy 1.926835 Distance to its sink is : 127.968291 Node Degree:200 Tr
Total Fitness is  :82.721781
packetMonitor: packetForwardCheck return false tnode: 136
Find and increment the counter of recv Packet: packetInfo: uid: 788 tnode: 136 packet src: 1 dest: 0,
Received = 112
Forwered = 112
PDR = 1.00
Trust = 1.00
--------------------
Fitness paranters : tnode: 136 energy 1.926835 Distance to its sink is : 127.968291 Node Degree:200 Trust Value:1.00
Total Fitness is  :82.721781
packetCache::incrementSentCounter: increment sent counter tnode: 136
packetInfo: uid: 788 tnode: 136 packet src: 1 dest: 0, mac src: 175 dest 0: type: cbr, clock: 199.621579 NodeDegree: 199
Received = 112
Forwered = 112
PDR = 1.00
Trust = 1.00
--------------------
Fitness paranters : tnode: 136 energy 1.926835 Distance to its sink is : 127.968291 Node Degree:200 Trust Value:1.00
Total Fitness is  :82.721781
supriya@supriya-HP-Pavilion-Laptop-15-eg0xxx:~/II paper work/ns-allinone-2.34 (4)/ns-allinone-2.34/ns-2.34$ Cannot connect to existing nam instance. Starting a new one...
AES & HILL encryption has been successful
No of pkts send              792
No of pkts recv              782
Pkt_delivery_ratio:          98.7374
Routing_overhead:            0.000883276
Delay:                       0.05696
Throughput:                  1881.24
Jitter:                      0.251944
No of Pkts Dropped           10
Dropping_Ratio:              1.26263
Energy_Consumption:     0.0171438
```

Fig 7.Output of fitness parameters

This is the output after the calculation of Fitness parameters for every node packet farwarded.Security can be measured by using PDR and energy consumption.The metrics used for communication between nodes in the secure cluster based routing are trust, communication cost, residual energy and node degree.It also shows that AES and Hill encryption is successful,The calculation of Jitter,Delay,No of live nodes,No of packets dropped,Energy consumption is done.

V. Conclusion

This TCSA-HSA approach uses the Trust based CSA to find a SCH and safe route while avoiding malicious nodes. It is necessary to remove the rogue nodes from the network since they result in excessive energy consumption and packet loss. Using the HSA also improves data security when the data packets are being sent. The WSN-packet IoT's delivery and energy usage are therefore improved by using both the TCSA and HSA. Based on the findings, it can be said that the TCSA-HSA performs more effectively than the MDCRP and SEHR. The PDR of TCSA-HSA for 100 nodes is 99.7449%, which is high when compared to the OP-MDCRP and SEHR.

REFERENCES

[1] Hriez, S., Almajali, S., Elgala, H., Ayyash, M. and Salameh, H.B., 2021. A novel trust-aware and energy-aware clustering method that uses stochastic fractal search in IoT-enabled wireless sensor networks. IEEE Systems Journal.

[2] Ahmed, A., Abdullah, S., Bukhsh, M., Ahmad, I. and Mushtaq, Z., 2022. An energy-efficient data aggregation mechanism for IoT secured by blockchain. IEEE Access, 10, pp.11404-11419.

[3] Kala, I. and Karthik, S., 2021. Advanced hybrid secure multipath optimized routing in Internet of Things (IoT)-based WSN. International Journal of Communication Systems, 34(8), p.e4782.

[4] Shende, D.K. and Sonavane, S.S., 2020. CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. Wireless Networks, 26(6), pp.4011-4029.

[5] Zhang, Y., Ren, Q., Song, K., Liu, Y., Zhang, T. and Qian, Y., 2021. An Energy Efficient Multi-Level Secure Routing Protocol in IoT Networks. IEEE Internet of Things Journal.

[6] Gayathri, A., Prabu, A.V., Rajasoundaran, S., Routray, S., Narayanasamy, P., Kumar, N. and Qi, Y., 2022. Cooperative and feedback based authentic routing protocol for energy efficient IoT systems. Concurrency and Computation: Practice and Experience, 34(11), p.e6886.

[7] Wang, Y., Li, F., Ren, P., Yu, S. and Sun, Y., 2022. A secure aggregation routing protocol with authentication and energy conservation. Transactions on Emerging Telecommunications Technologies, 33(1), p.e4387.

[8] Hema Kumar, M., Mohanraj, V., Suresh, Y., Senthilkumar, J. and Nagalalli, G., 2021. Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. Journal of Ambient Intelligence and Humanized Computing, 12(5), pp.5287-5295.

[9] Haseeb, K., Islam, N., Almogren, A., Din, I.U., Almajed, H.N. and Guizani, N., 2019. Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. IEEE Access, 7, pp.79980-79988.

[10] Yu, X., Li, F., Li, T., Wu, N., Wang, H. and Zhou, H., 2020. Trust-based secure directed diffusion routing protocol in WSN. Journal of Ambient Intelligence and Humanized Computing, pp.1-13.

[11] Reegan, A.S. and Kabila, V., 2021. Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT. Wireless Personal Communications, 118(2), pp.1313-1329.

[12] Chouhan, N. and Jain, S.C., 2020. Tunicate swarm Grey Wolf optimization for multi-path routing protocol in IoT assisted WSN networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-17.

[13] Mon, S., Winster, S.G. and Ramesh, R., 2021. Trust Model for IoT Using Cluster Analysis: A Centralized Approach. Wireless Personal Communications, pp.1-22.

[14] Bangotra, D.K., Singh, Y., Selwal, A., Kumar, N. and Singh, P.K., 2021. A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. Wireless Personal Communications, pp.1-22.

[15] Qureshi, S.G. and Shandilya, S.K., 2021. Novel fuzzy based Crow Search optimization algorithm for secure node-to-node data transmission in WSN. Wireless Personal Communications, pp.1-21.

[16] Kavitha, V., 2021. Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment. Peer-to-Peer Networking and Applications, 14(2), pp.821-836.

[17] Karunkuzhali, D., Meenakshi, B. and Lingam, K., 2022. OQR-SC: An optimal QoS aware routing technique for smart cities using IoT enabled wireless sensor networks. Wireless Personal Communications, pp.1-28.

[18] Gali, S. and Nidumolu, V., 2021. An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things. Cluster Computing, pp.1-11.

[19] Haseeb, K., Almustafa, K.M., Jan, Z., Saba, T. and Tariq, U., 2020. Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access, 8, pp.163962-163974.

[20] Gurupriya, M. and Sumathi, A., 2022. HOFT-MP: A Multipath Routing Algorithm Using Hybrid Optimal Fault Tolerant System for WSNs Using Optimization Techniques. Neural Processing Letters, pp.1-26.

[21] AlFarraj, O., AlZubi, A. and Tolba, A., Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, (2018) 1-11.

[22] Selvakumar, K., Sairamesh, L. and Kannan, A., An intelligent energy-aware secured algorithm for routing in wireless sensor networks. Wireless Personal Communications, 96(3) (2017) 4781- 4798.

[23] Azharuddin, M., Kuila, P. and Jana, P.K., Energy-efficient faulttolerant clustering and routing algorithms for wireless sensor networks. Computers & Electrical Engineering, 41 (2015) 177-190.

[24] Rodrigues, P. and John, J., Joint trust: an approach for trust-aware routing in WSN. Wireless Networks, (2020) 1-16.

[25] Deepa, C. and Latha, B., HHSRP: a cluster-based hybrid hierarchical secure routing protocol for wireless sensor networks. Cluster Computing, 22(5) (2019) 10449-10465.

[26] Alghamdi, T.A., Secure and energy-efficient path optimization technique in wireless sensor networks using DH method. IEEE Access, 6 (2018) 53576-53582.

[27] Darabkh, K.A., Al-Maaitah, N.J., Jafar, I.F. and Ala'F, K., EA-CRP: a novel energy-aware clustering and routing protocol in wireless sensor networks. Computers & Electrical Engineering, 72 (2018) 702-718.

[28] Sureshkumar, C. and Sabena, S., Fuzzy-Based Secure Authentication and Clustering Algorithm for Improving the Energy Efficiency in Wireless Sensor Networks. Wireless Personal Communications, 112(3) (2020) 1517-1536.

[29] Logambigai, R., Ganapathy, S. and Kannan, A., Energy-efficient grid-based routing algorithm using intelligent fuzzy rules for wireless sensor networks. Computers & Electrical Engineering, 68 (2018) 62-75.

[30] Rahayu, T.M., Lee, S.G. and Lee, H.J., A secure routing protocol for wireless sensor networks considering secure data aggregation. Sensors, 15(7) (2015) 15127-15158.

[31] Ye, Z., Wen, T., Liu, Z., Song, X. and Fu, C., A security faulttolerant routing for multi-layer non-uniform clustered WSNs. EURASIP Journal on Wireless Communications and Networking, 2016(1) (2016) 1-12.

[32] Sharma, R., Vashisht, V. and Singh, U., eeTMFO/GA: a secure and energy-efficient cluster head selection in wireless sensor networks. Telecommunication Systems, (2020) 1-16.

[33] Sahoo, R.R., Sardar, A.R., Singh, M., Ray, S. and Sarkar, S.K., A bio-inspired and trust-based approach for clustering in WSN. Natural Computing, 15(3) (2016) 423-434.

[34] Pavani, M. and Rao, P.T., Adaptive PSO with optimized firefly algorithms for secure -cluster-based routing in wireless sensor networks. IET Wireless Sensor Systems, 9(5) (2019) 274-283.

[35] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H.K. and Kannan, A., An energy-aware trust-based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105(4) (2019) 1475-1490.

[36] Dhand, G. and Tyagi, S.S., SMEER: Secure multi-tier energyefficient routing protocol for hierarchical wireless compared to the SRPMA 20 (2019).

[37] Shankar, A., Jaisankar, N., Khan, M.S., Patan, R. and Balamurugan, B., A hybrid model for security-aware cluster head selection in wireless sensor networks. IET Wireless Sensor Systems, 9(2) (2018) 68-76.

[38] Sun, Z., Wei, M., Zhang, Z. and Qu, G., Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless

[39] Kavidha, V. and Ananthakumaran, S., Novel energy-efficient secure routing protocol for wireless sensor networks with mobile sink. Peer-to-Peer Networking and Applications, 12(4) (2019) 881-892.

[40] Vijayalakshmi, V. and Senthilkumar, A., USCDRP: an unequal secure cluster-based distributed routing protocol for wireless sensor networks. The Journal of Supercomputing, 76(2) (2020) 989-1004.