International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Security Aware Cluster-Based Routing Using MTCSA and HEA for Wireless Sensor Networks

M. Supriya [1], Dr. T. Adilakshmi*[2]

Submitted: 13/11/2022 **Accepted:** 15/02/2023

Abstract*:* Wireless Sensor Network (WSN) is operated as a medium to connect the physical and information network of the Internet-of-Things (IoT) for exchanging information. Energy and trust are two key factors that assist reliable communication over the WSN-IoT. Secure data transmission is considered a challenging task during the multipath routing over the WSN-IoT. To address the aforementioned issue, secure routing is developed over the WSN-IoT. In this paper, the Multiobjective Trust based Crow Search Algorithm (MTCSA) is developed to identify the Secure Cluster Heads (SCHs) and secure path over the network. Further, data security while broadcasting the data packets isenhanced by developing the Hybrid Encryption Algorithm (HEA). This HEA is the combination of Advanced Encryption Standard (AES) and Hill Cipher Algorithm (HCA). Therefore, the developed MTCSA-HEA avoids malicious nodes during the communication which helps to improve data delivery and energy consumption. The performance of MTCSA-HEA 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 MTCSA-HEA performances. The PDR of MTCSA-HEA for 100 nodes is 99.7449%, which is high when compared to the OP-MDCRP and SEHR.

Keywords: Energy *Consumption, Internet-Of-Things, Hybrid Encryption Algorithm, Multiobjective Trust Based Crow Search Algorithm, Packet Delivery Ratio, Wireless Sensor Network.*

1.Introduction

Wireless Sensor Network (WSN) is considered an integral part of the large-scale and effective installation of Internet-of-Things (IoT). The WSN isthe 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 numerousnetwork 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 architecture that integrates the physical and the virtual worlds by utilizing the web as the mode for transmitting the information between the physicaland the virtual worlds [3]. The IoT has a huge amount of objects such as sensors, RFID tags, mobile devicesand actuators which are linked to the internet over wired/wireless connections [4]. Nowadays, internet devices exist in everyday human life such as real-timeequipment monitoring, industrial supply chain management, safety production management, and environmental monitoring. It is predicted that each person has connected to the internet with more than ten devices in the year of 2050 [5] [6].

In WSN, rapid energy consumption is considered a primary problem due to the limited battery level. The sensing process of the nodes and the data transmitted over the nodes are affected when the node exhausts its energy in the network [7] [8]. Generally, the forwarding methods are categorized as structure-free and structure-based approaches. In structure-freeapproach, the sensor data is gathered without any fixed architecture and accomplishes the data collection according to the partial information. On thecontrary, 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 datato the chosen Cluster Head (CH). Subsequently, the CH collects the data and broadcasted it to the BS thatacts as a bridge between the network and the end-user [11]**[12].** The sensors are generally located in the open and remote environment that creates the devicessusceptible to security threats, specifically when there are malicious node attacks 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].

The contributions of this research are concise as follows:

- The K-means clustering and MTCSA based SCH selection are used to improve energy efficiency and security. The trust based clustering is used to avoid the malicious nodes that help to minimize the data loss over the network.
- Further, the trust based routing is performed byusing the MTCSA followed by data security is accomplished by using HEA. Hence, the MTCSA and HEA are used to minimize the energy consumption and packet drop.

1 Swami Vivekananda Institute of Technology, JNUTH, Secundrabad, Telangana– 500003, INDIA
ORCID ID: 0000-0001-6466-5843
2Vasavi College of Engineering,,Ibhrahimpatnam,Osmania University,Hyderabad,Telangana,– 500031,INDIA
ORCID ID : 0000-0002-8295-3029
Email: supriyasamuel@yahoo.com,t_adilakshmi@staff.vce.ac.in

The remaining paper is organized as follows: therelated works about secure communication over WSN-IoT are given in Section 2. A detailedexplanation of the MTCSA-HEA method is given in Section 3. The outcome of the MTCSA-HEA is provided in Section 4 whereas the conclusion is presented in Section 5.

2.Related Work

Kavitha, V [16] developed the architecture of cryptographic-based clustering which is used to protect data privacy by using the Optimal Privacy- Multihop Dynamic Clustering Routing Protocol (OP-MDCRP). In this work, the clusters were generated according to the area followed by the combination ofan elliptic curve and encryption-key provisioningwas used to ensure data privacy. The OP-MDCRP was used to minimize the energy consumption by using both clustering and multi hop communication. This work formed the clusters only according to the nodes placed in the area.

Karunkuzhali [17] implemented a routing according to the optimal quality of service for smart cities using IoT-WSN. The clusters were formed by using Chaotic Bird Swarm Optimization (CBSO). Each sensor's trust degree was computed by using the improved differential search where the node with high trust was selected as Cluster Head (CH). The lightweight encryption approach was used to ensure the data encryption followed by route between the source and destination was discovered by optimal decision-making approach. The developed CBSO was considered the only cluster center and data pointduring the optimization.

Gali, and Nidumolu, [18] developed Chaotic Bumble Bees Mating Optimization (CBBMO) to perform reliable communication along with the trust sensing model. The CBBMO was the combination ofbumble bees mating and chaotic concept. The developed CBBMO based routing achieved less energy consumption. However, the optimal route selection of CBBMO was considered only the energyand trustworthiness of the node.

Haseeb [19] presented a Secure and Energy- aware Heuristic-based Routing (SEHR) for optimizing the routing with an effective decision against malicious attackers. The hop count to BS, link integrity factors and residual energy were used in the heuristic function of SEHR. In addition, counter mode encryption was used to offer data security in IoT-WSN. Essential factors such as route maintenance, energy consumption and secure communication were concentrated to obtain reliable communication. However, this work failed to achievebetter energy efficiency.

Gurupriya and Sumathi, [20] developed a hybridoptimal fault tolerant system to perform a multipath routing in a network. An effective clustering over thenetwork was done by using modified teaching– learning based optimization. The backup node for clusters was discovered by using a nonlinear regression-based pigeon optimization that was used to maximize the fault tolerance. Further, the multipath over the network was determined by usinga deep Kronecker neural network. The data security between the network wasn't concentrated in this multipath routing.

3. MTCSA-HEA Method

In this MTCSA-HEA method, an SCH and securepath are identified by using the multiobjective CSA for avoiding malicious nodes. The malicious nodes are required to be eliminated in the network because it causes unwanted energy usage and packet drop over the network. Further, the data security while transmitting the data packets is enhanced by using theHEA. Therefore, both the MTCSA and HEA are usedto improve the packet delivery and energy. consumption of the WSN-IoT. The block diagram ofthe MTCSA-HEA method is shown in Fig. 1.

3.1 K-means based clustering process

At first, the nodes are randomly located in the WSN-IoT followed by the nodes being separated intovarious groups using the K-means clustering method.Here, the K-means method is mainly based on the Euclidian distance computation among the nodes.The SCH selection and secure path discovery are done, once the clustering is done over the network.

3.2 MTCSA-based SCH selection

An optimal SCH from the clusters is chosen by using the MTCSA which helps to mitigate the malicious nodes.

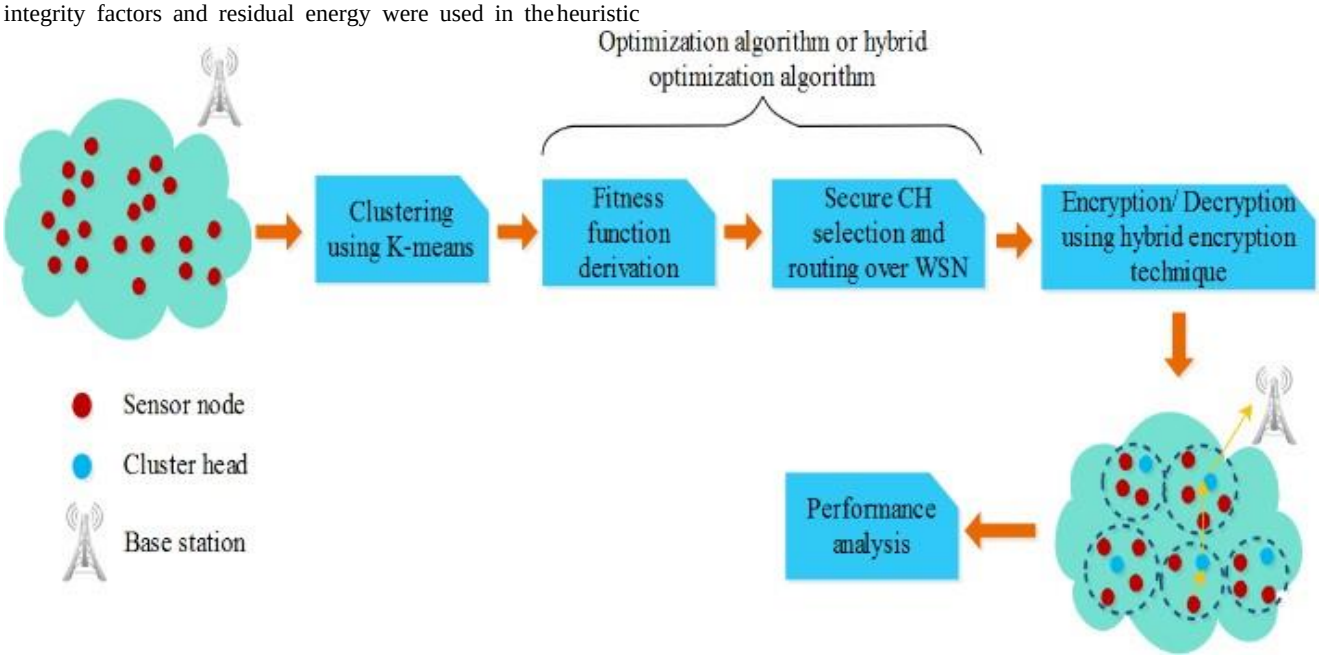

Fig. 1 Block diagram of the MTCSA-HEA method

An optimal SCH from the clusters is chosen by using the MTCSA which helps to mitigate the malicious nodes. Hence, the unwanted energy consumption and packet drop are minimized by avoiding the malicious nodes. CSA [21] is generally a meta-heuristic algorithm that mimics memory capacity, communication skills and social actions of hiding food from crows. This CSA has four keyprinciples which are mentioned as follows: 1) crows live in the flock, 2) it remembers the location of hiding food locations,

3.2.1. Initialization of MTCSA

In this initialization phase, the MTCSA is initialized with the set of candidate nodes that are required to be selected as SCH. Each crow is initialized with the random node ID among 1 to S, where total nodes exist in the WSN-IoT is denoted as S. Let, the ith crow of MTCSA is $Pi = (Pi,1, Pi,2, \dots, Pi,D)$, where D specifies the dimension of each crow (i.e., number of SCHs).

3.2.2 Iterative process

In MTCSA, 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 to the hiding food location of jth crow. Equation (1) shows the ith crow's updated location P_i^{t+1}.

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

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 and 1 and M_j^t denotes the memory matrix.

In 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 2.

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

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.

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

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

3.2.3. Derivation of fitness function

The MTCSA considers the multiple fitness functions while selecting the SCHs from the clusters. There are four fitness measures such as trust (fm_1), communication cost (fm_2), residual energy (fm_3) and node degree(fm_4) are considered in MTCSA. The fitness function mentioned in the equation (1) is expressed in the following equation (4).

$$S = \delta_1 \times fm_1 + \delta_2 \times fm_2 + \delta_3 \times fm_3 + \delta_4 \times fm_4 \quad (4)$$

Where, $\delta_1 - \delta_4$ are the weight parameters allocated to an each fitness measure. The clear information about the fitness measures are given as follows:

- Trust expressed in equation (5) is considered as the primary objective for this SCH selection. The nodes in the WSN exchanges the information based on the mutual trust relationship for avoiding the malicious attacks during data delivery. Here, the trust is computed based on the communication carried out by the nodes. Therefore, the trust is a definition of packets received by the node and packets sent by the source node.

$$fm_1 = \frac{Packets\ received_{a,b}}{Packets\ sent_{a,b}} \quad (5)$$

Where, a and b are the example nodes.

- The required communication cost for interacting with the adjacent node is shown in equation (6).

$$fm_2 = \frac{d_{avg}^2}{d_0^2} \quad (6)$$

Where, the average distance between the sensor and neighbour node is represented as d_{avg}^2 and the sensor's distribution radius is denoted as d_0^2.

- The sensors are supposed to perform data collection and transmission over the network. Therefore, the node with high residual energy is preferred for data delivery. Equation (7) shows the expression for residual energy.

$$fm_3 = \sum_{i=1}^{D} E_{SCH_i} \quad (7)$$

Where, the residual energy of ith SCH is denoted as E_{SCH_i}.

- Further, the node degree defines the number of hops connected to the CH. The lesser node degree is used to achieve the less energy consumption.

$$fm_4 = \sum_{i=1}^{D} CM_i \quad (8)$$

Where, the number of CMs connected to the ith CH is denoted as CM_i.

Therefore, an appropriate SCH is selected by using the aforementioned fitness function. The trust used in the fitness measures is used to avoid the malicious nodes, because these malicious node causes packet drop over the network. Next, the communication cost is used to identify the path with small distance that results in lesser energy consumption. The residual energy is used to identify whether the node has enough energy to broadcast the data or not. Based on this, the packet delivery to the BS is improved over the network. Further, the node degree also considered to minimize thee energy consumption of the nodes.

3.3. MTCSA-based routing

The route discovery is carried out utilising the MTCSA after choosing the SCH from the clusters. This MTCSA 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 MTCSA, the secure route is found. The source CH initially broadcasts the RREQ to all of the network's neighbouring CHs. The next step is for the best relay node determined by the MTCSA to transmit the RREP message back to the originating CH.The same procedure is continued until it reaches the destination node i.e., BS. When the source CH received the RREP message, the secure route in the WSN. After

that, the data packets are transmitted over the network. Moreover, this route discovery phase uses the HELLO and RERR for route maintenance.

3.4. Hybrid encryption algorithm

After identifying the secure path using MTCSA, the HEA is initialized for encrypting the data before transmission. The hybrid encryption technique, which combines AES and 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.The AES has four main functions such as Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round-Key. On the contrary, HCA accomplishes the encryption based on the invertible square matrix.

The following procedures carried out by this HEA are listed:

In the initial stage of the Sub-Bytes operation, each byte in the block is switched using a fixed lookup table called the Substitution box. Each byte in the data block is cyclically shifted by 0, 1, 2, or 3 places in Shift-Rows. Then, in the Mix-Columns operation, the 4 bytes in each column are multiplied by a fixed matrix with constant entries. Of this case, the coefficients in the Galois field GF(28) are multiplied and added. In the addRoundKey operation, the input data is XORed with the key block cell by cell in order to produce the output encrypted data, denoted as En. The output acquired from the AES is additionally encrypted with the HCA for improving the 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) .

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

$$H\_En = \begin{bmatrix} (hk_{11}en_1 + hk_{12}en_2)\ mod\ X \\ (hk_{21}en_1 + hk_{22}en_2)\ mod\ X \end{bmatrix} \quad (9)$$

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

4. Results and discussion

The outcomes of the MTCSA-HEA method are discussed in this section. The implementation of the MTCSA-HEA is done in the Network Simulator (NS) -2.34 where the system is operated with i5 processor and 6GB RAM. The NS-2.34 generally has two programming languages such as TCL at front end and C++ at bank whereas the network animator shows the node deployment. The simulation parameters utilized to analyse the secure data transmission using MTCSA-HEA is given in the Table 1.

Parameter	Value
Simulator	NS-2.34
Area	300mx300m
Number of nodes	50, 100,150, 200 and 250
Traffic source	CBR
Antenna pattern	OmniAntenna
MAC	IEEE 802.11 DCP
Propagation model	Two-rayground reflection
Initial energy	5J
Network interface type	WirlessPhy

Table 1: Simulation Parameters

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

4.1. Packet delivery ratio and packet loss ratio

PDR is the ratio among the amount of packets collected by the BS and amount of packets sent by source that is shown in equation (10). On the contratry, PLR is ratio among the lost packets and sent packets which is simplified as shown in equation (11).

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

$$PLR = 100 - PDR \quad (11)$$

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

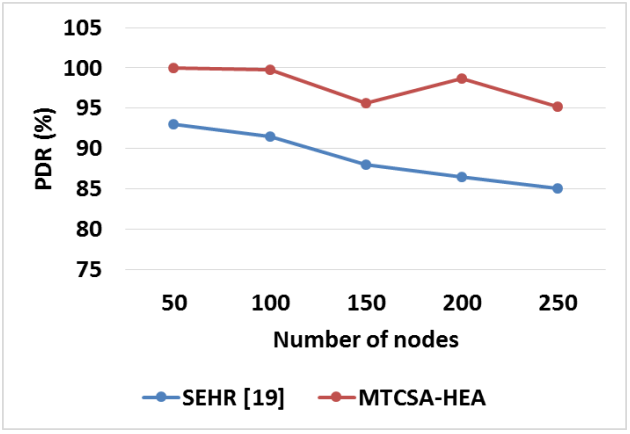

Fig 2. Analysis of PDR

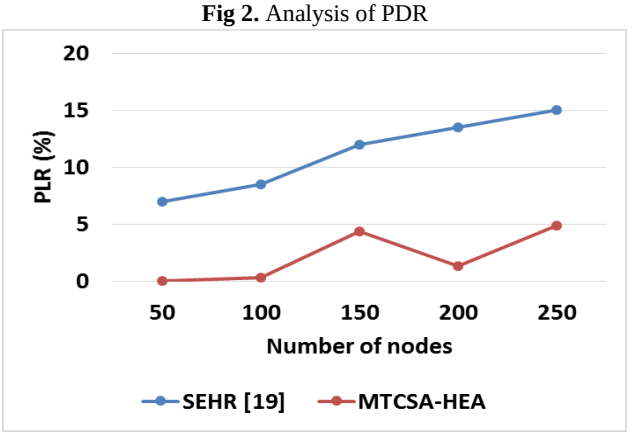

Fig 3. Analysis of PLR

4.2. **Energy consumption**

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

$$EC = E_{tr} + E_{rx} \quad (12)$$

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

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

$$E_{rx} = E_{elect} \times L \quad (14)$$

Where, the transmission distance of the path is represented as d; amount of consumed energy for a single bit is $Eelect$; amount of data bits is denoted as L; Efs and $Eamp$ denotes the free space and amplification energy, and threshold distance is represented as dt . The comparison of energy consumption for MTCSA-HEA with SEHR [19] is shown in the Figure 4. This Figure 4 shows that the MTCSA-HEA achieves lesser energy consumption than the SEHR [19]. For instance, the energy consumption of MTCSA-HEA for 100 nodes is 0.00337J whereas the SEHR [19] achieves the energy consumption of 0.018J. The shortest path generation and mitigation of malicious nodes using MTCSA-HEA helps to minimize energy consumption of WSN-IoT.

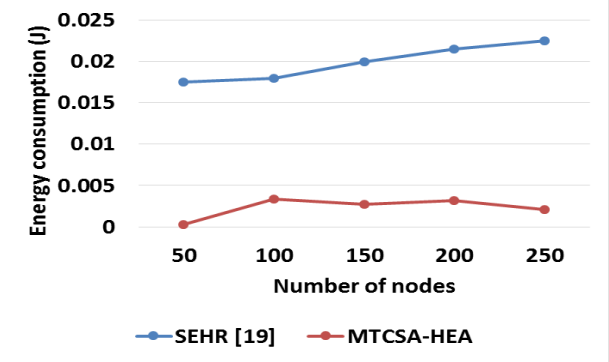

Fig 4. Analysis of energy consumption

4.3 End to end delay

EED is the ratio between the amount of time consumed by the sensor for transmitting the data packet to the BS over the network which is shown in equation (15).

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

Figure 5 shows the analysis of EED for MTCSA-HEA with SEHR [19]. By changing the number of nodes, the performance is examined here. From the Figure 5, it is known that the MTCSA-HEA achieves less EED than the SEHR [19]. For example, the EED of the MTCSA-HEA is0.001ms for 100 nodes, whereas the SEHR [19] obtains the EED of 0.13ms. The MTCSA with unique fitness measures is used to compute the optimal path with less amount of control packets which helps to minimize the EED.

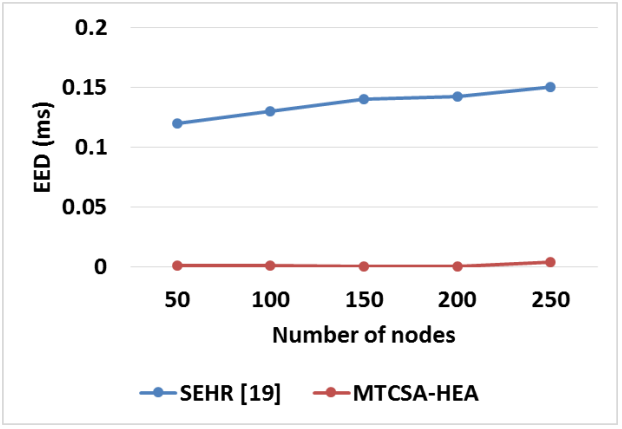

Fig 5. Analysis of EED

4.4. **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 MTCSA-HEA and SEHR [19]. Changing the number of nodes allows for an analysis of the performance here. This Figure 6 shows that the MTCSA-HEA achieves higher throughput than the SEHR [19]. For instance, the throughput of MTCSA-HEA for 100 nodes is 99.5901% whereas the SEHR [19] achieves the throughput of 90%. The trust value considered in the MTCSA and HEA improves the robustness against the malicious attackers that helps to improve the successful data transmission over the WSN-IoT.

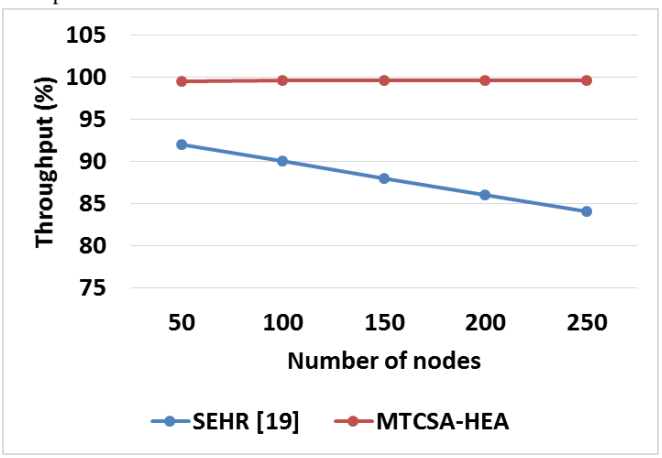

Fig 6. Analysis of throughput

Conclusion

This MTCSA-HEA approach uses the multiobjective 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 HEA also improves the 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 MTCSA and HEA. Based on the findings, it can be said that the MTCSA-HEA performs more effectively than the MDCRP and SEHR. The PDR of MCTSA-HEA for 100 nodes is 99.7449%, which is high when compared to the OP-MDCRP and SEHR.

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
	MTCSA-HEA	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
	MTCSA-HEA	0	0.2551	4.33673	1.27551	4.84694
Energy consumption (J)	SEHR [19]	0.0175	0.018	0.02	0.0215	0.0225
	MTCSA-HEA	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
	MTCSA-HEA	0.00049	0.001	0.00028	0.0003	0.00378
Throughput (%)	SEHR [19]	92	90	88	86	84
	MTCSA-HEA	99.5639	99.5901	99.6201	99.6503	99.6658

Table 2. Comparative analysis of MTCSA-HEA

Acknowledgements

This research was supported/partially supported by my SVIT institution We thank our HOD Dr.Shyamala from [Osmania University] who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank guide [Dr.T.Adilakshmi] for assistance with [MTCSA-HEA] from [VCE] for comments that greatly improved the manuscript.

Author contributions

Mrs. M.Supriya: Conceptualization, Methodology, Software, Field study , Data curation, Writing-Original draft preparation, Software, Validation., Field study

Dr.T.Adilakshmi: Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest

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] Vijayalakshmi, V. and Senthilkumar, A., 2020. USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks. The Journal of Supercomputing, 76(2), pp.989-1004.
[22] Rodrigues, P. and John, J., 2020. Joint trust: an approach for trust-aware routing in WSN. Wireless Networks, pp.1-16.
[23] Selvi, M., Thangaramya, K., anapathy, S., Kulothungan, K., Nehemiah, H.K. and Kannan, A., 2019. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105(4), pp.1475-1490.
[24] Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W. and Yang, Y., 2021. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Communications and Networks.
[25] SureshKumar, K. and Vimala, P., 2021. Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks. Computer Networks, 197, p.108250.
[26] Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J. and Song, L., 2020. Information-aware secure routing in wireless sensor networks. Sensors, 20(1), p.165.
[27] Hu, H., Han, Y., Wang, H., Yao, M. and Wang, C., 2021. Trust-aware secure routing protocol for wireless sensor networks. ETRI Journal.
[28] Shankar, A., Jaisankar, N., Khan, M.S., Patan, R. and Balamurugan, B., 2018. Hybrid Model for security-aware cluster head selection in wireless sensor networks.*IET Wireless Sensor Systems*, *9*(2), pp.68-76.
[29] Thangaramya, K., Kulothungan, K., Indira Gandhi, S., Selvi, M., Santhosh Kumar, S.V.N. and Arputharaj, K., 2020. Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. *Soft Computing*, pp.1-15.
[30] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: a survey," Security and Comm. Networks, vol. 8, pp. 1812-1827, 2015.