Received: August 25, 2022. Revised: October 4, 2022.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Adaptive Cluster based Routing Using Multi Objective-Trust based Hybrid Optimization Algorithm for CPS

Saritha Ibakkanavar Guddappa[1]* **Rajeshwari Mahabhaleshwar Hegde[2]**

[1]*Department of Electronics and Telecommunication Engineering,*
BM Sreenivasaiah Institute of Technology and Management, Bengaluru, India.
[2]*Department of Electronics and Telecommunication Engineering,*
B M Sreenivasaiah College of Engineering, Bengaluru, India.
* Corresponding author's Email: Saritha.i.g@bmsit.in

Abstract: Cyber physical system (CPS) is an engineered system that integrates the physical world with the cyber world through enhanced computation, communication and control (3C) abilities. But, the CPS's sensors are susceptible to malicious threats due to its dynamic topology and open medium of the network. Therefore, an effective secure adaptive cluster-based routing is required to be developed for improving the security of CPS. In this paper, the multi objective-trust based hybrid optimization algorithm (MO-THOA) is proposed to improve CPS security. The MO-THOA is the combination of trust based flower pollination algorithm (TFPA) and trust based ant colony optimization (TACO). In that, the TFPA is used to select a secure adaptive cluster head (ACH) and TACO is used to identify the secure routing path via ACHs. Therefore, the proposed MO-THOA improved the security against malicious attacks while broadcasting the data. The performance of the MO-THOA is evaluated using packet delivery ratio (PDR), average end to end delay (AEED) and normalized routing overhead (NRO). The existing methods namely grey-wolf updated whale optimization algorithm (GU-WOA), moving centroid based routing protocol (MCRP) and multi-objective ant colony optimization (MOACO) are used to evaluate the MO-THOA method. The PDR of the MO-THOA for 20 nodes is 0.981, it is high when compared to the GU-WOA, MOACO and MCRP.

Keywords: Cyber physical system, Malicious attacks, Multi objective-trust based hybrid optimization algorithm, Secure adaptive cluster based routing, Trust based ant colony optimization, Trust based flower pollination algorithm.

1. Introduction

CPS received huge attention in both the research and public communities because these CPSs are used to perform communications among machines, environments, humans and to a new paradigm [1, 2]. The physical objects of the CPS are incorporated with the computing devices, actuators, sensors and data transmission abilities [3]. CPS based data observing is used in different real-world applications such as social sensing, mobile event discovery, chemical explosions, military intrusion tracking, structural health monitoring and crowd sensing application [4]. The structure of the sensing layer-network layer-cognitive layer-control layer is used to obtain an effective interaction between the information and the physical world. The physical devices are included in the sensing layer which is used to observe the physical environment and characteristics while the network layer enables the connection between the information and the physical world. The cognitive layer exists in the information world and performs different evaluations on the collected data. Accordingly, this information world broadcast the results to the successive control layer where it generates an appropriate decision and provides the commands to handle the physical layer of the device to broadcast the physical world [5 - 7].

CPS is the combination of sensor networks with cyber resources which provides the intelligent response to the dynamic changes occurred in the physical world, whereas the wireless sensor network is considered one of the essential modules which

gather information from the physical environment [8]. Since, the sensors are susceptible to attacks, because those sensors are installed in a harsh/ unattended environment. Therefore, security is considered an important issue in the wide usage of CPS [9 - 11]. Generally, the attacker node interferes with the normal nodes which create a collision of traffic with packet drop or occasionally cause the data misdirection over the paths [12]. The secure service is required to provide information integrity, data confidentiality, access control, ID certification and privacy protection for CPS [13]. Therefore, secure clustering and routing are developed for improving the security of the network [14]. Node's trustworthiness is a key security parameter in network security that examines the traffic and node activities. Moreover, this trust value evaluates the risk included in the data broadcasting over the untrusted nodes [15].

The contributions of this paper are concise as follows:

- Initially, the K-means approach is used to divide the CPS into various clusters followed by secure ACH and routes are selected to accomplish the communication.
- The TFPA from the MO-THOA is used for secure ACH selection from the clusters whereas the flower pollination algorithm (TFPA) is selected because of its enhanced searching ability.
- Moreover, the TACO is used to identify the secure route via ACHs for enabling communication. Since ant colony is selected for routing purposes because of its advantage of adapting capacity to any dynamic changes in the network.

The remaining paper is arranged as follows: The related works of secure data transmission are given in section 2. Clear details about the MO-THOA are provided in section 3. Section 4 delivers the outcomes of the MO-THOA method while the conclusion is presented in section 5.

2. Related work

Kanchan [16] presented the secure and privacy-preserving SignRecryption (SPSR) approach for improving the security in vehicular CPS. The developed SPSR combined the group signature with an authentication protocol. The privacy and restriction of unauthorized access were achieved by the group signature and authentication respectively. The analysis of successful packet delivery was required to be analyzed for an effective security approach.

Adil [17] implemented the routing scheme namely Hash-media access control-destination sequence distance vector (Hash-MAC-DSDV) for enabling mutual authentication in the CPS. The DSDV was modified for accomplishing the mutual authentication through the hop count communication. Here, the secured authentication key is created by using the hash function with the MAC address. The continuous broadcasting of the authentication information was used to ensure the legitimacy of participating devices. However, the packet loss was increased when there was an increment in traffic.

Reddy [18] presented an optimal CH selection by implementing the GU-WOA. This GU-WOA was considered for various fitness functions such as delay, energy, distance, and security. But, the low energy adaptive clustering hierarchy (LEACH) was considered a basic routing algorithm for GU-WOA. Therefore, the data transmission over the network was affected because of the direct data transmission performed in the LEACH.

Wang [19] developed the MOACO for developing the node-trusted secure routing over the network. Here, the security of the nodes was evaluated based on the trust valuation model. This trust valuation mode used two types of trust such as direct and indirect trust during the security analysis. This developed secure routing was used to minimize energy consumption. The multiple objectives considered for this research are only residual energy and trust of the sensor.

Shen [20] implemented the MCRP for the cyber-physical-social distributed systems. The variable basic locations using a moving centroid were generated to use the node movement. Subsequently, the relay nodes were chosen by considering the distance and transmission probability which improved the PDR. But, the data transmission using MCRP was susceptible to malicious attacks.

3. MO-THOA method

The MO-THOA method is developed for improving the performances of CPS whereas the MO-THOA is the combination of TFPA and TACO. There are three main processes performed in this MO-THOA method such as clustering, secure ACH selection and secure adaptive route identification. In that, the TFPA is used to select secure ACH and TACO is used to identify the secure route. Therefore, the developed secure adaptive communication provides robustness against malicious nodes during data transmission. Fig. 1 shows the overall block

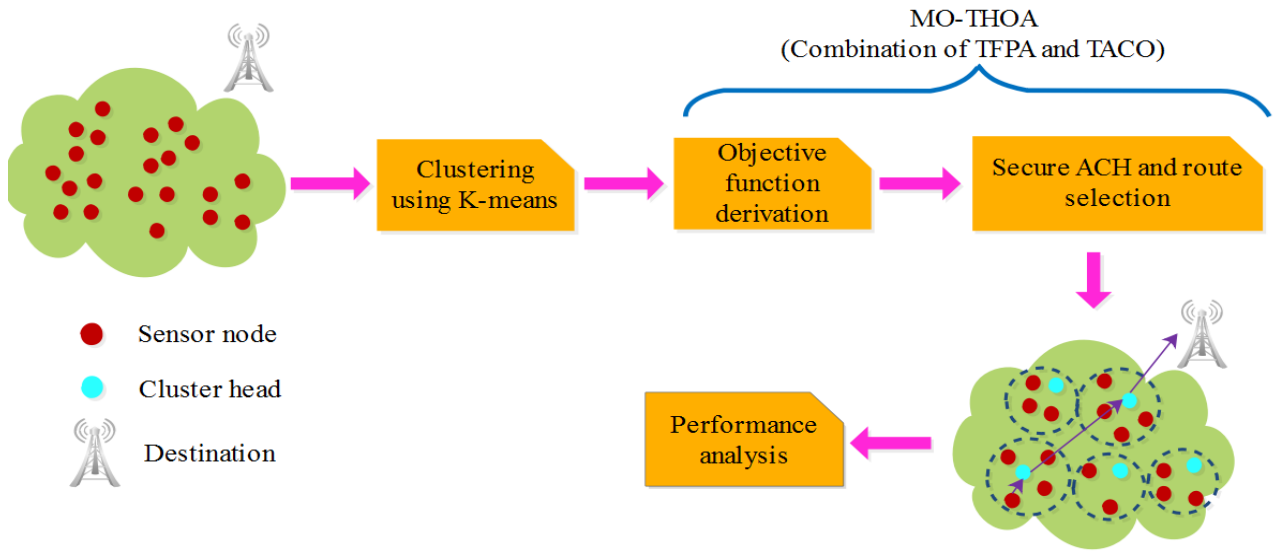

Figure. 1 Block diagram of the MO-THOA method

diagram of the MO-THOA.

3.1 Clustering process

Initially, the nodes are randomly deployed in CPS followed by the K-means approach which is used for dividing the network into various clusters. Since the K-means approach mainly depends on the Euclidian distance calculation among the nodes. The secure ACHs are identified from the cluster, once the clustering process is completed in the CPS.

3.2 Selection of secure ACH using TFPA

In this phase, TFPA is used to identify the secure ACHs from each cluster. Since the conventional FPA is a population-based optimization technique that imitates the behavior of flower pollination. The identification of secure ACH using TFPA helps to avoid the malicious nodes to be selected as ACH which helps to minimize packet loss and avoids unwanted energy consumption. The process of ACH selection from the clusters is detailed as follows:

3.2.1. Initialization

In this TFPA, the population is initialized with the candidate sensor node which is required to be chosen as ACH. The dimension of the population is identical to the number of CHs required to choose from the network. Each solution is initialized with the ID of a random sensor from 1 to NS, where NS defines the number of sensors. Consider, that the ith solution of TFPA is $x_i = (x_{i,1}, x_{i,2}, .., x_{i,NC})$, where the NC defines the number of ACHs and $1 \leq d \leq NC$ denotes the node ID among the 1 to NS.

3.2.2. Iterative process for ACH selection

The generated initial populations are updated in this iterative process that is used to obtain the adaptive CHs according to the objective function. Generally, pollination is categorized into two types such as self and cross-pollination. In self-pollination, the pollen from one flower pollinates the same flower. Besides, the pollen grains exchange from different plants to other flowers is defined as cross-pollination. Additionally, this FPA also has some other pollination such as abiotic and biotic pollination. In abiotic pollination, the pollen is transferred through wind whereas the pollination that happened via birds, insects and other animals is depicted as biotic pollination. Here, the flower constancy is observed in the insect pollinators specifically honeybees. Further, the insect pollinators are moved to the specific flowers and ignore the other types. Therefore, the redevelopment of similar flowers is increased in the FPA.

Four rules exist during the FPA development that are given as follows:

- The cross and biotic pollination are monitored as global pollination. The Lévy flights are followed by the pollinators carrying the pollens who fly for a large distance (Rule 1).
- The local pollination denotes the self and biotic pollination (Rule 2).
- The constancy of flowers is monitored as same as the probability of redevelopment that is proportional to the similarity of 2 different flowers processed in the FPA (Rule3).
- The switching between the local and global

pollination is handled by the value of switch probability $p \in [0\ 1]$.

Eq. (1) expresses the flower constancy of global pollination.

$$x_i^{t+1} = x_i^t + \gamma L(\lambda)(g_* - x_i^t) \quad (1)$$

Where, the i^{th} pollen for iteration t is denoted as x_i^t; an optimal solution is g_*; the scaling factor utilized for controlling the step size is denoted as γ; the step size according to the Lévy flights is denoted as $L(\lambda)$ which is related to the pollination strength. The insects fly through a huge distance with discrete distance steps which is derived from the Lévy distribution as expressed in Eq. (2).

$$L \sim \frac{\lambda \Gamma(\lambda) \sin\left(\frac{\pi\lambda}{2}\right)}{\pi} \frac{1}{s^{1+\lambda}} \quad (s \gg s_0 > 0) \quad (2)$$

Where, the gamma function is denoted as $\Gamma(\lambda)$ which is valid for larger steps i.e., $s > 0$. Eq. (3) shows the local pollination done by the flower constancy (Rule 2 and Rule 3).

$$x_i^{t+1} = x_i^t + \varepsilon(x_j^t - x_k^t) \quad (3)$$

Where the pollen from discrete flowers of similar plant categories are x_j^t and x_k^t, and the random number in the range of $[0\ 1]$ is denoted as ε. The location update is specified as a local random walk when the x_j^t and x_k^t originated from the same population/ species. Moreover, pollination happens at both the local and global levels (Rule 4). To switch among the scales, the switch or proximity probability is used in FPA. The objective function is used to update the location of a population which is formulated in the following section.

3.2.3. Formulation of objective function

The TFPA considers four unique objective functions such as trust value (f_1), communication cost (f_2), residual energy (f_3), number of hops (f_4) to improve the CPS performance. Eq. (4) expresses the objective function (i.e., fitness) used in the overall MO-THOA method.

$$f = \delta_1 f_1 + \delta_2 f_2 + \delta_3 f_3 + \delta_4 f_4 \quad (4)$$

Where the weighted parameters assigned to each objective function are denoted as $\delta_1, \delta_2, \delta_3$ & δ_4.

The definition of the objective functions is mentioned as follows:

- In general, trust is the metric where one sensor has trust in another sensor based on the previous information of node behavior and implication achieved from the authenticated nodes. Since the trust is computed based on the forwarding ratio expressed in Eq. (5). The forwarding ratio is the proportion of the number of packets received and the number of packets forwarded between the nodes.

$$f_1 = \frac{Number\ of\ packets\ successively\ received_{p,q}}{Number\ of\ packets\ broadcasted_{p,q}} \quad (5)$$

Where, p and q represent the example nodes.

- Eq. (6) expresses the communication cost required to communicate with the neighbor node.

$$f_2 = \frac{d_{avg}^2}{d_0^2} \quad (6)$$

Where, d_{avg}^2 defines the average distance between the sensor and adjacent sensor and d_0^2 denotes the radius of the sensor.

- The residual energy expressed in Eq. (7) is generally considered an important parameter for the CPS. A large amount of energy is required by CH because it has to accomplish the data collection and transmission.

$$f_3 = \sum_{i=1}^{NC} E_{ACH_i} \quad (7)$$

Where, E_{ACH_i} defines the i^{th} ACH residual energy.

- Some hops define the number of nodes connected to the specific ACH in the CPS.

$$f_4 = \sum_{i=1}^{NC} CM_i \quad (8)$$

Where, CM_i denotes the number of cluster members for the i^{th} CH.

The derived objective function is utilized for selecting the secure ACH from each cluster. The calculation of node's trustworthiness is used to eliminate the malicious nodes for minimizing packet loss. The communication cost is used to identify the shortest path which lessens the energy consumption of the sensors. Further, the node failure is avoided by considering the residual energy of the sensors which avoids the packet loss. Moreover, the number of hops is used to perform the load balancing while broadcasting the data packets.

3.3 Adaptive secure routing using TACO

After identifying the ACHs from the clusters, the route from the source ACH and destination is identified using the TACO. The control messages of AODV such as route request (RREQ), route reply (RREP), route error (RERR), and hello (HELLO) messages are used by this TACO. The pheromone value from the TACO is included in the conventional RREQ and RREP message to identify the optimal secure route. The source ACH broadcasts the RREQ to all the neighbor ACHs while initializing the route discovery.

The calculation of the pheromone value is detailed as follows:

In this initialization phase, each node has artificial ants and each link corresponds with a weight. Eq. (9) shows the node transition rule which is the probability of selecting m as the next relay ACH from l by n^{th} ant.

$$P_{lm}^{n} = \begin{cases} \frac{[\tau_{lm}(t)]^{\alpha}[\eta_{lm}(t)]^{\beta}}{\sum_{o\epsilon\mathcal{N}_n}[\tau_{lo}(t)]^{\alpha}[\eta_{lo}(t)]^{\beta}} & if\ m\epsilon\mathcal{N}_n \\ 0 & otherwise \end{cases} \quad (9)$$

Where, the heuristic value and pheromone intensity are denoted as η_{lm} and τ_{lm} respectively; the relative importance of η_{lm} and τ_{lm} are controlled by the parameters β and α; The set of ACHs n isn't visited yet is denoted as $\mathcal{N}_n$.

The real ant's food search process is replicated by the artificial ants. In this phase, the node transition rule is used to select the next ACH, when a source ACH wants to transmit the data to the destination. Since, the visited ACHs information is stored in the memory. If the ant (i.e., relay ACH) reaches the destination, the same route is retraced to the source ACH. Accordingly, the pheromone update rule is used to update the pheromone value of the route. This rule comprises the pheromone reinforcement and pheromone evaporation that maximize or minimize the route's pheromone respectively. Hence, the ACO finds the adaptive secure path from the source ACH to the destination. The rule of pheromone update is expressed in Eq. (10).

$$\tau_{lm}^{new} = (1-\rho)\tau_{lm}^{old} + \sum_{n=1}^{NA}\Delta\tau_{lm}^{n} \quad (10)$$

Where the number of ants is denoted as NA and the pheromone decay coefficient is denoted as $\rho\ \epsilon\ (0,1)$. The amount of pheromone of the route l and m by ant n is computed as shown in Eq. (3).

$$\Delta\tau_{lm}^{n} = \begin{cases} \frac{Q}{f_n} & if\ the\ ant\ n\ travelled\ route\ (l,m) \\ 0 & otherwise \end{cases} \quad (11)$$

Where the constant value is Q and the objective function of the route is denoted as f_n. Here, the objective function is equal to the objective function calculated in section 3.2.3.

The ACH with a better pheromone rate transmits the RREP through the reverse route followed by the route generated once the source ACH receives the RREP from the destination. Hence, the secure adaptive route is obtained by avoiding the malicious nodes that exist in the CPS. Further, route maintenance is accomplished using the HELLO and RERR messages.

4. Results and discussion

This section explains in detail the results and discussion of the MO-THOA method which is used to accomplish secure and reliable data transmission over the CPS. The execution of the MO-THOA method is done in the network simulator – 2.34 (NS-2.34) whereas the system is operated with the 6-GB RAM and Intel i5 Core processor. In a surface area of $500\text{m} \times 500\text{m}$, the varying mobile nodes of 20, 50, 100 and 150 are deployed to analyze the performances of MO-THOA. The simulation parameters of the MO-THOA are shown in Table 1.

The performance of the MO-THOA is analyzed using PDR, AEED and NRO. Here, existing methods namely GU-WOA [18], MOACO [19] and MCRP [20] are used to analyze the efficiency of the MO-THOA method. These existing methods are simulated by using the same specifications mentioned in Table 1.

4.1 Packet delivery ratio

The PDR is defined in Eq. (12) which also defines how much packet drop rate is reduced by the MO-THOA.

Table 1. Simulation parameters of MO-THOA

Parameter	Value
Area	$500\text{m} \times 500\text{m}$
Number of nodes	20, 50, 100 and 150
Initial energy	2 J
Traffic source	CBR
Mac	IEEE 802.11 DCP
Propagation model	Two-ray ground reflection
Node speed	0~5m/s
Antenna pattern	OmniAntenna
Network interface type	WirlessPhy
Simulation time	7000 seconds

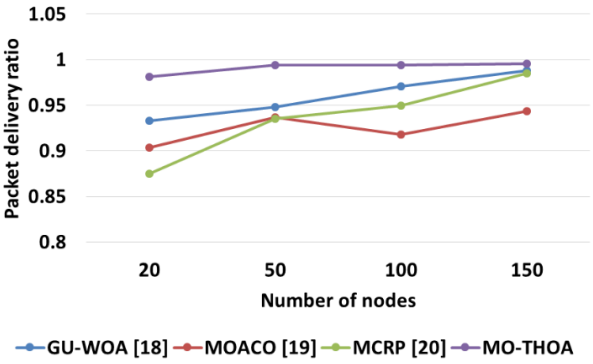

Figure. 2 PDR analysis for MO-THOA

$$PDR = \frac{Amount\ of\ received\ packets}{Amount\ of\ generated\ packets} \quad (12)$$

The PDR analysis of MO-THOA, GU-WOA [18], MOACO [19] and MCRP [20] for varying nodes is shown in Fig. 2. Fig. 2 indicates that the MO-THOA achieves better PDR than the GU-WOA [18], MOACO [19] and MCRP [20]. For example, the PDR of the MO-THOA ranges from 0.981 to 0.996 whereas the PDR of the MCRP [20] is obtained between 0.875 to 0.985. The data delivery is increased by mitigating the malicious nodes using the trust based adaptive routing of MO-THOA. Additionally, the node failure or link failure or monitored using residual energy which further enhances the PDR. However, the inappropriate objective function of MOACO [19] causes less PDR while broadcasting the packets whereas MCRP [20] failed to mitigate the malicious nodes during the data broadcasting process.

4.2 Average end-to-end delay

An AEED is expressed in Eq. (13) which defines the amount of time taken to transmit the data from the source to the destination.

$$AEED = \frac{Sum\ of\ time\ taken\ to\ transmit\ packet\ to\ receiver}{Number\ of\ packet\ received\ by\ receiver} \quad (13)$$

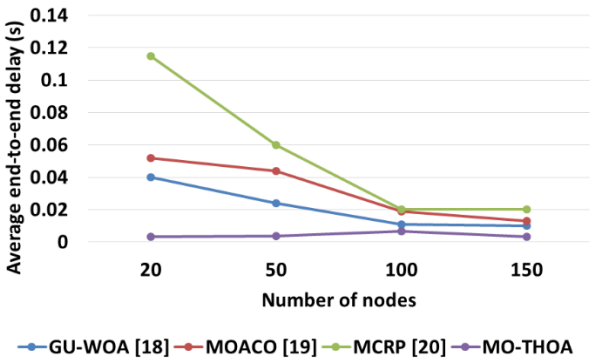

Figure. 3 AEED analysis for MO-THOA

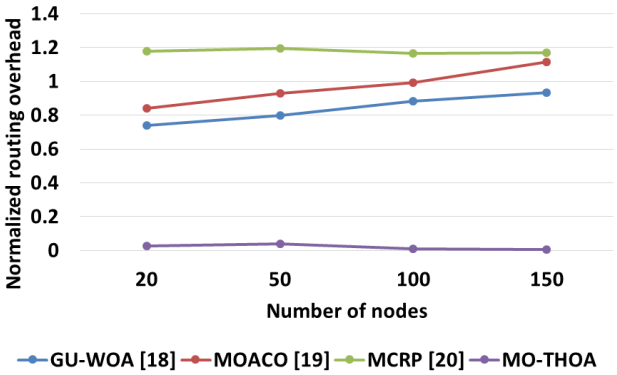

Figure. 4 NRO analysis for MO-THOA

The analysis of AEED is presented in Fig. 3 for MO-THOA, GU-WOA [18], MOACO [19] and MCRP [20]. From Fig. 3, it is confirmed that the MO-THOA has a lesser delay than the GU-WOA [18], MOACO [19] and MCRP [20]. For example, the AEED of MO-THOA is ranged from 0.0033 s to 0.0066s whereas the MCRP [20] ranges from 0.02s to 0.115s. Therefore, an AEED of MO-THOA is greatly reduced while transmitting the information because of the lesser control packet utilization in the adaptive route discovery and shortest path identification.

4.3 Normalized routing overhead

Eq. (14) expresses the NRO which represents the number of resources consumed by the MO-THOA for accomplishing the communication.

$$NRO = \frac{Amount\ of\ routing\ packet\ transmission}{Amount\ of\ data\ packet\ transmission} \quad (14)$$

The NRO analysis of MO-THOA, GU-WOA [18], MOACO [19] and MCRP [20] for varying nodes is shown in Fig. 4. Fig. 4 indicates that the MO-THOA achieves less NRO than the GU-WOA [18], MOACO [19] and MCRP [20]. For example, the NRO of the MO-THOA ranges from 0.007 to 0.04 whereas the NRO of the MCRP [20] is obtained between 1.165 to 1.195. The MO-THOA utilizes only less amount of control packets because it uses distinct objective functions for generating the routing path.

4.4 Node energy consumption

The energy consumption of the node defines that the amount of energy consumed by the node while transmitting and receiving the data packets.

The analysis of node's energy consumption is presented in Fig. 5 for MO-THOA, GU-WOA [18], MOACO [19] and MCRP [20]. From Fig. 5, it is confirmed that the MO-THOA has a lesser energy

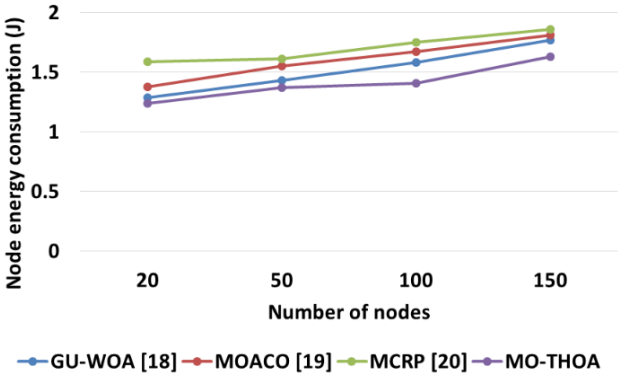

Figure. 5 Energy consumption analysis for MO-THOA

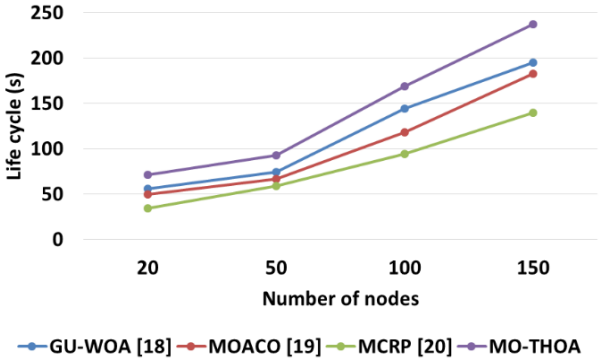

Figure. 6 Life cycle analysis for MO-THOA

consumption than the GU-WOA [18], MOACO [19] and MCRP [20]. For example, the energy consumption of MO-THOA is ranged from 1.24J to 1.63J whereas the MCRP [20] ranges from 1.59J to 1.86J. The adaptive secure routing of MO-THOA is used to achieve lesser energy consumption based on the shortest path discovery.

4.5 Life cycle and total node survival time

Life cycle is defined as the first node which exhausts their full energy while performing the communication. Moreover, the total node survival time defines the time at which all nodes in the network exhausts their full energy in the network.

The life cycle and total node survival time analysis of MO-THOA, GU-WOA [18], MOACO [19] and MCRP [20] for varying nodes is shown in Fig. 6 and Fig. 7 respectively. Fig. 6 indicates that the MO-THOA achieves higher life cycle than the GU-WOA [18], MOACO [19] and MCRP [20]. Similarly, Fig. 7 also shows that the MO-THOA achieves higher total node survival time than the other existing methods. For example, the life cycle of the MO-THOA ranges from 71s to 237s whereas the life cycle of the MCRP [20] is obtained between 34s to 140s. The MO-THOA based secure routing avoids the

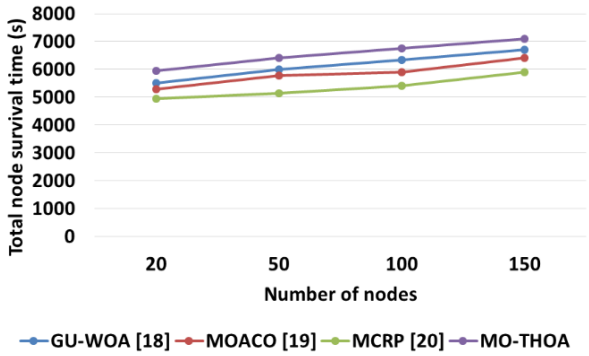

Figure 7. Total node survival time analysis for MO-THOA

malicious nodes which helps to minimize the energy consumption. Simultaneously, the shortest path generation also used to minimize the energy consumption of the nodes. Hence, the lesser energy consumption of MO-THOA helps to increase the life cycle and total node survival time in the CPS.

Table 2 shows the comparative analysis of the MO-THOA with GU-WOA [18], MOACO [19] and MCRP [20]. From Table 2, it is known that the MO-THOA provides better performance than the GU-WOA [18], MOACO [19] and MCRP [20]. In that, the MO-THOA outperforms well for the network with both the less and high node density, when compared to the GU-WOA [18], MOACO [19] and MCRP [20]. The total node survival time of MO-THOA is 7108 for 150 nodes whereas the GU-WOA [18] obtains 6711s, MOACO [19] obtains 6407s and MCRP [20] obtains 5905s. This total node survival time states that the MO-THOA achieves higher stability than the GU-WOA [18], MOACO [19] and MCRP [20]. The PDR of the MO-THOA is enhanced because of the malicious node mitigation using trust based adaptive clustering and routing of MO-THOA. However, the GU-WOA [18] uses the LEACH as basic routing algorithm which performs the direct data transmission from the cluster head to destination. Subsequently, the direct data transmission increases the energy consumption over the network. Next, the MOACO [19] considers only residual energy and trust as a fitness function to accomplish the communication which leads to affect the network performance. On the other hand, the MCRP [20] doesn't provide any security against malicious nodes. So, the data transmission using MCRP [20] may be susceptible to malicious attacks. Moreover, the lesser control packet utilization of MO-THOA helps to minimize the AEED and NRO. Therefore, the developed adaptive secure clustering and routing offers higher PDR while broadcasting the information over the CPS.

Table 2. Comparative analysis of MO-THOA

Performances	Methods	Number of nodes			
		20	50	100	150
PDR	GU-WOA [18]	0.933	0.948	0.971	0.988
	MOACO [19]	0.904	0.937	0.918	0.944
	MCRP [20]	0.875	0.935	0.95	0.985
	MO-THOA	0.981	0.994	0.994	0.996
AEED (s)	GU-WOA [18]	0.04	0.024	0.011	0.01
	MOACO [19]	0.052	0.044	0.019	0.013
	MCRP [20]	0.115	0.06	0.02	0.02
	MO-THOA	0.0035	0.0038	0.0066	0.0033
NRO	GU-WOA [18]	0.74	0.797	0.883	0.934
	MOACO [19]	0.841	0.93	0.993	1.113
	MCRP [20]	1.18	1.195	1.165	1.17
	MO-THOA	0.027	0.04	0.008	0.007
Node energy consumption (J)	GU-WOA [18]	1.29	1.43	1.58	1.77
	MOACO [19]	1.38	1.55	1.67	1.81
	MCRP [20]	1.59	1.61	1.75	1.86
	MO-THOA	1.24	1.37	1.41	1.63
Life cycle (s)	GU-WOA [18]	56	74	144	195
	MOACO [19]	50	67	118	183
	MCRP [20]	34	59	94	140
	MO-THOA	71	93	169	237
Total node survival time (s)	GU-WOA [18]	5506	6005	6329	6711
	MOACO [19]	5300	5786	5911	6407
	MCRP [20]	4938	5140	5418	5905
	MO-THOA	5938	6410	6752	7108

5. Conclusion

In this paper, the MO-THOA-based secure ACH and route selection is accomplished to improve the CPS performances. The K-means clustering and TFPA based secure ACH selection are used to improve the data exchange between the sensors. Specifically, the TFPA avoids the malicious nodes during the ACH selection which minimizes the packet loss. Moreover, the TACO discovers the secure optimal route via ACHs with less transmission distance that helps to minimize the AEED. Therefore, the developed trust based optimizations are used to improve the security against malicious nodes which resulted in high data delivery. From the results, it is identified that the MO-THOA outperforms well than the GU-WOA, MOACO and MCRP. The PDR of the MO-THOA for 20 nodes is 0.981, it is high when compared to the GU-WOA, MOACO and MCRP. In the future, a novel optimization algorithm can be used for improving the performance of CPS.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

As there are two authors involved in this work, Rajeshwari M Hegde have contributed "Conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation and Myself Saritha I G contributed writing—original draft preparation, writing—review and editing, visualization, supervision, project administration, funding acquisition, etc.

References

[1] M. Z. A. Bhuiyan, J. Wu, G. M. Weiss, T. Hayajneh, T. Wang, and G. Wang, "Event detection through differential pattern mining in cyber-physical systems", *IEEE Transactions on Big Data*, Vol. 6, No. 4, pp. 652-665. 2017.

[2] H. Xia, F. Xiao, S. S. Zhang, X. G. Cheng, and Z. K. Pan, "A reputation-based model for trust evaluation in social cyber-physical systems", *IEEE Transactions on Network Science and Engineering*, Vol. 7, No. 2, pp. 792-804, 2018.

[3] S. Redhu and R. M. Hegde, "Network lifetime improvement using landmark-assisted mobile sink scheduling for cyber-physical system applications", *Ad Hoc Networks*, Vol. 87, pp. 37-48, 2019.

[4] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, T. Wang, J. Wu, S. Q. Salih, Y. Li, and T. Hayajneh, "TrustData: Trustworthy and secured data collection for event detection in industrial cyber-

physical system", *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 5, pp. 3311-3321, 2019.

[5] N. Yi, J. Xu, L. Yan, and L. Huang, "Task optimization and scheduling of distributed cyber–physical system based on improved ant colony algorithm", *Future Generation Computer Systems*, Vol. 109, pp. 134-148, 2020.

[6] Y. Huo, W. Dong, J. Qian, and T. Jing, "Coalition game-based secure and effective clustering communication in vehicular cyber-physical system (VCPS)", *Sensors*, Vol. 17, No. 3, p. 475, 2017.

[7] Y. Yin, F. Yu, Y. Xu, L. Yu, and J. Mu, "Network location-aware service recommendation with random walk in cyber-physical systems", *Sensors*, Vol. 17, No. 9, p. 2059, 2017.

[8] X. Luo, D. Zhang, D. Yang, J. Liu, X. Chang, and H. Ning, "A kernel machine-based secure data sensing and fusion scheme in wireless sensor networks for the cyber-physical systems", *Future Generation Computer Systems*, Vol. 61, pp. 85-96, 2016.

[9] X. Liu, N. Xiong, N. Zhang, A. Liu, H. Shen, H. and C. Huang, "A trust with abstract information verified routing scheme for cyber-physical network", *IEEE Access*, Vol. 6, pp. 3882-3898, 2018.

[10] M. Alaeiyan, A. Dehghantanha, T. Dargahi, M. Conti, and S. Parsa, "A multilabel fuzzy relevance clustering system for malware attack attribution in the edge layer of cyber-physical networks", *ACM Transactions on Cyber-Physical Systems*, Vol. 4, No. 3, pp. 1-22, 2020.

[11] J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie, W. Gui, and J. P. Niyoyita, "Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection", *Expert Systems with Applications*, Vol. 158, p. 113578, 2020.

[12] P. A. Patil, R. S. Deshpande, and P. B. Mane, "Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm", *Wireless Personal Communications*, Vol. 115, No. 1, pp. 415-437, 2020.

[13] Z. Min, G. Yang, A. K. Sangaiah, S. Bai, and G. Liu, "A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1, pp. 1-14, 2019.

[14] M. Revanesh, V. Sridhar, and J. M. Acken, "Secure coronas based zone clustering and routing model for distributed wireless sensor networks", *Wireless Personal Communications*, Vol. 112, No. 3, pp. 1829-1857, 2020.

[15] K. Thangaramya, K. Kulothungan, S. Indira Gandhi, M. Selvi, S. V. N. S. Kumar, and K. Arputharaj, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN", *Soft Computing*, Vol. 24, No. 21, pp. 16483-16497, 2020.

[16] S. Kanchan, G. Singh, and N. S. Chaudhari, "SPSR-VCP: secure and privacy preserving SignRecryption in vehicular cyber physical systems", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 13, No. 1, pp. 1-20, 2022.

[17] M. Adil, M. A. Jan, S. Mastorakis, H. Song, M. M. Jadoon, S. Abbas, and A. Farouk, "Hash-mac-dsdv: Mutual authentication for intelligent iot-based cyber-physical systems", *IEEE Internet of Things Journal*, 2021.

[18] D. L. Reddy, C. G. Puttamadappa, and H. N. G. Suresh, "Hybrid optimization algorithm for security aware cluster head selection process to aid hierarchical routing in wireless sensor network", *IET Communications*, Vol. 15, No. 12, pp. 1561-1575, 2021.

[19] X. Wang, "Low-Energy Secure Routing Protocol for WSNs Based on Multiobjective Ant Colony Optimization Algorithm", *Journal of Sensors*, 2021.

[20] J. Shen, C. Wang, A. Wang, Q. Liu, and Y. Xiang, "Moving centroid based routing protocol for incompletely predictable cyber devices in cyber-physical-social distributed systems", *Future Generation Computer Systems*, Vol. 108, pp. 1129-1139, 2020.