

AN OPTIMIZED CLUSTER HEAD SELECTION AND SECURED WIRELESS SENSOR NETWORK USING MRSA

Yesu Arumaidhas Adline Jancy, Balasubramanian Gomathy*

Received on July 8, 2023

Presented by Ch. Roumenin, Member of BAS, on September 26, 2023

Abstract

Currently, Wireless Sensor Networks (WSNs) play a vital role in remote monitoring and sharing of information in an infrastructure. Even though WSNs have numerous advantages, their usage is reduced by node's lifetime and data loss. The aforementioned problems in WSNs were overcome by using energy efficient protocols by various researchers. But most of the authors focused on either trust model or energy efficient model, or analyzed both models using separate algorithms. However, this leads to repeated process and to high energy consumption. Here, the cluster head is selected by using the swarm intelligence algorithm and LEACH protocol. The hybrid ant colony and modified Particle swarm algorithm are used to select the cluster heads. The CH selection depends on the two parameters, namely residual energy and number of successful transmissions of node. The node's trust is assessed using these two parameters (transmission nodes and residual energy), which also assist in ensuring the safety of the data and energy. The proposed system uses a digital signature algorithm known as the modified RSA algorithm to achieve network security when performing cryptography on data. The performance obtained by the proposed method was compared to other existing techniques in terms of throughput, energy consumption, packet delivery ratio, and network lifetime.

Key words: wireless sensor networks, security, modified RSA, energy, trust, packet transmission, swarm intelligence, CH selection

Introduction. Due to the fact that just the head node, also known as the cluster head (CH), is permitted to connect with the sink or BS, cluster-based

DOI:10.7546/CRABS.2023.12.10

networking has shown to be the most effective method for preserving energy in power-starved sensor network. The CHs must be well chosen because they are in charge of data collecting and aggregation, which would be necessary to maintain the network's energy budget. A probabilistic approach called low-energy adaptive clustering hierarchy (LEACH) regularly adjusts the head position to optimize power usage. Nevertheless, because the CH is chosen based on chance, the network is prematurely ended as a cluster and with much less remaining energy wins the election. A LEACH protocol has been altered throughout time in accordance with the needs of the user application, and many CH election techniques have been proposed for lowering energy usage and extending its range. Determined by remaining energy, the CH for the subsequent round must be established through LEACH protocol using fuzzy logic.

Related work. The researchers in [1] propose a methodical modelling of the resource needed to secure communications in a cluster formation WSN. The concept is used to create a multi-hop cluster method that employs the blockchain's Proof of Authentication (POAh) mechanism and is built on spectrum classifications. The overall number of nodes, the network's energy, and each node's first and last dead nodes were the variables that were examined. In [2] unfortunately, these advanced devices have several drawbacks, such as their great energy, storage, processing, and computational resource requirements. In addition to these limitations, a major issue for WSNs is balancing dependability with safe data transfer. This study proposes an energy-efficient secure routing protocol and a key distribution confirmation as remedies for these issues. Node clustering, cluster head (CH) identification, key authorization, and safe routing make up the suggested methodology. In [3] a WSN has sensor nodes (SNs) dispersed at random. After the CH is chosen using the Rider Bald Eagle Search (RBES) method, an energy-efficient seagull K-medoid cluster (SKC) approach is developed to build these SNs depending on the intrinsic features of nodes. Since security is a crucial problem, the Key Agreement technique is then implemented utilizing a key generation authentication mechanism, which provides safer data transfer over the network. In the end, the Decisions Trust Routing Protocol was developed to offer reliable and secure routing for IoT-based WSN. In [4] the software utilized to carry out the experiment is MATLAB. According to testing results, the recommended approach is superior to the ones already in use for dependable and energy-efficient routes. In order to select the most suitable cluster heads, a self-organizing map neural network is used to conduct a preliminary clustering algorithm on the network's node. The firefly algorithm (FA) is then employed to optimize networks grouping by taking into account the cluster's relative reasonableness, the cluster head resources, the distance inside the cluster, and other variables. In [5] the decision domain concept is introduced to the FA in order to distribute cluster heads even more and produce sensible clusters. In this stage, inter-cluster routing is constructed using an improved ant colony optimization. The node's angle, distance, as well

as energy are taken into consideration to improve the heuristic function's ability to pick the very next hop with more accuracy. The statistical variance coefficient is taken into account while updating pheromones, and the path is optimized by combining resource and distance. In [6] a polling control technique predicated on busy/idle node is introduced to even further increase the network throughput, just as it did during the interconnectivity phase. The simulated investigation's findings show that EECRAIFA can effectively balance network energy consumption in a range of application scenarios, extend network lifetime, and boost throughput. In this research, a hybrid approach for elephant herding optimization (EHO) and migrating bird optimization (MBO) is proposed for WSN secured data assurance routing (SDAR) and dynamic data security. The MBO algorithm's path discovery method is used to advance the BIOSARP by raising the trust level, and the Clan Updating Operators in the EHO algorithm is raised to update the SDAR and locate the best path. In [7] the recommended technique is implemented using the network simulator 2 (NS2) application. The experimental findings are investigated using assessment metrics such as packet delivery (DR), energy use (EC), packet excess (PO), and accuracy. Finally, the experimental results demonstrate that the proposed strategy outperforms other conventional methods like LEACH and others by providing improved packet DR, EC, PO, and accuracy.

In [8] the NS3 tool is used to position nodes in the network area, and a unique F-CSO is performed with respect to three variables: distance, degree, and transmitting energy. Throughout the optimization process, the best nodes are taken into account and must satisfy the three criteria of reduced transmitting data lengths between nodes, higher transmission degree, as well as maximum transmission energy. These nodes are gathered into a group using the fuzzy rule method and then optimized using the crow search strategy to get the exact nodes needed for trust-based transmissions. Routing may also be done using the OLSR protocol. In [9] the proposed system's performance is compared with that of earlier research in terms of execution time, throughput, and packet delivery ratio for the system for recognising malicious nodes with and without using the recommended F-CSO. The evaluation's results show that F-CSO efficiently finds malicious nodes and achieves better outcomes with various parameters. A hybrid approach is known as FAGWO-H that fuses grey-wolf optimization and firefly optimization to offer a fault-tolerant cluster-based routing protocol for WSNs (GWO). In [10] the optimum path between the cluster's head (CH) and the base stations is selected utilizing GWO and FA. For FA and GWO, the suggested approach makes use of two novel fitness functions. To improve network performance while maintaining QoS standards, the technique takes into account the fault endurance and energy consumption of the node sensors and CHs. We assessed the technique's effectiveness and contrasted them to the most current cutting-edge techniques using a range of WSN scenarios. In [11] the best cluster head (CH) is selected using a Self-adaptive dingo optimizer with Brownian motion (SDO-BM) technique while

taking into account a number of restrictions, including energy, bandwidth, delay, complexity, trustworthiness, service quality (quality-of-service), and privacy (higher risk, lower risk, and medium risk). If the selected optimal CH is flawed, the network is stabilized using fault tolerance and power hole prevention techniques. In order to ensure that the SADO-BM model continues evolving, analysis is finally finished. The recommended model produces the greatest outcomes when compared to other models. Numerous approaches are used to remedy many WSN flaws. This research provides an error-tolerant multi-path routing approach for WSNs. The `wsnsimpy0.2.5` tool is used to simulate WSNs initially. In [12] the clustering is carried out using the low-energy adaptive clustering hierarchy method to select the optimum CH. Furthermore, multipath routing is accomplished utilizing conditionally improving invasive elephant herding optimization (CIIEHO), a proposed technique for selecting many routes to improve routing. Recently, the fitness was built while taking many factors into account, such as resource, inaccuracy, connection quality, intra-cluster length, and delay. In [13] the Enhanced Invasive Weed Optimizer, Elephants Herding Optimization, and Conditionally Autoregressive Value at Risk make up the created CIIEHO (CAViaR). With an adequate power of 0.9992 J, short distances of 15.815, reduced latency of 0.1022 s, and highest throughputs of 0.999, the suggested CIIEHO delivered better results.

Proposed work. The proposed work is thoroughly explained in this section. Figure 1 illustrates the architecture of the proposed model.

The free-space model is utilised if the distance d between receiving and transmitting nodes is below the threshold distance d_0 ; otherwise, the multi-path fading paradigm is used. Forwarding 1 bit per packet to a node d metres distant requires

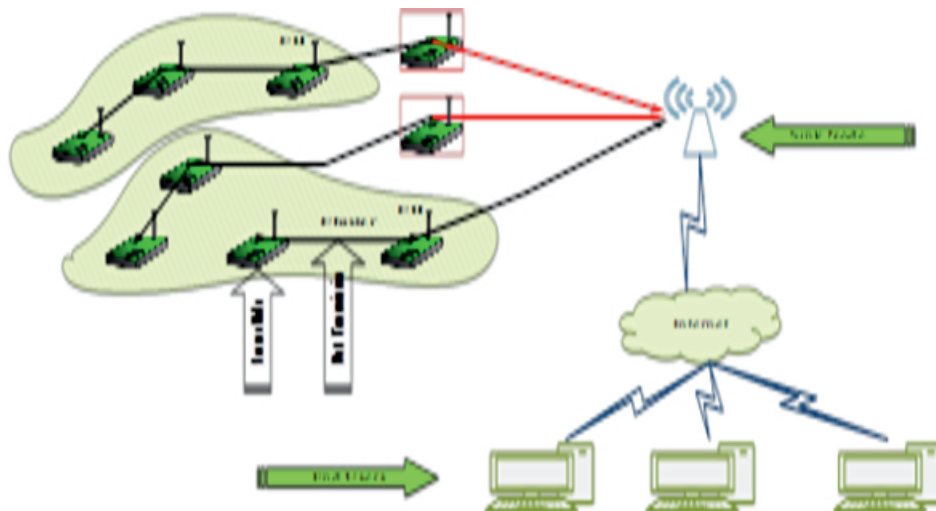


Fig. 1. Proposed system model

using the amount of energy stated as follows:

$$(1) \quad \begin{aligned} E_{Tx} &= E_{Tx_elec}(l) + E_{Tx_amp}(l, d), \\ E_{Tx}(l, d) &= \begin{cases} E_{elec} \times l + E_{fs} \times l \times d^2, & d \leq d_0 \\ E_{elec} \times l + E_{amp} \times l \times d^4, & d > d_0. \end{cases} \end{aligned}$$

The threshold separation d_0 is

$$(2) \quad d_0 = \sqrt{E_{fs}/E_{amp}}.$$

The following formula illustrates the energy needed to receive a packet of l bits:

$$(3) \quad E_{Rx}(l) = E_{elec} \times l.$$

Considering flawless data aggregation, the absorbed energy by the CH is expressed as follows:

$$(4) \quad E_{CH} = (n/k - 1)lE_{elec} + (n/k)lE_{DA} + lE_{elec} + lE_{fs}d_{toBS}^4,$$

where k is how many cluster there are in the network, and d_{toBS} is how far CH is from the access point.

$$(5) \quad E[d_{toCH}^2] = \int_0^{X_{max}} \int_0^{Y_{max}} ((x^2 + y^2) \times \rho(x + y)) \, dx \, dy.$$

The amount of power needed for a typical sensing node to send information to CH is expressed as:

$$(6) \quad E_{node} = lE_{elec} + lE_{fs}d_{toCH}^2.$$

The network's entire energy dissipation was computed as follows:

$$(7) \quad E_{total} = l \times \left(2nE_{elec} + nE_{DA} + kE_{mp}d_{toBS}^4 + E_{fs}\frac{M}{2\pi k}n \right),$$

$$(8) \quad \begin{aligned} V_{i+1} &= w^*V_i + \text{rand}^*c_1^*(\text{GBEST} - X_i) + \text{rand}^*c_2^*(\text{PBEST}_i - X_i), \\ X_{i+1} &= X_i + V_{i+1}, \quad i = 1, \dots, N, \end{aligned}$$

$$(9) \quad w = (t - s)/t,$$

where t is the maximum number of iterations and s is a measure of iteration.

The following formula is changed to reflect the ants' new locations:

$$(10) \quad x_t^k = x_{global}^{best} \pm \partial x, \quad t = 1, \dots, I,$$

where t represents the index for iteration, I represents the total number of iterations,

$$(11) \quad \alpha_t = 0.1 \times \alpha_{t-1}, \quad \sqrt{I} \text{ iterations},$$

where $x_{\text{global}}^{\text{best}}$ the dimensions of the optimal solutions determined by ants are equal to ∂x . $\pm$ sign is a movement's direction operator. The following equation determines whether anything is (+) or (-):

$$(12) \quad \bar{x}_t^{\text{best}} = x_{\text{global}}^{\text{best}} + \left(x_{\text{global}}^{\text{best}} \times 0.01 \right).$$

If $f(\bar{x}_t^{\text{best}}) \leq f(x_{\text{global}}^{\text{best}})$, (+) sign is used, otherwise (-) is used in the above equations. The pheromones' trail was refreshed utilising strengthening and vanishing, and it just increased the best result.

$$(13) \quad \begin{aligned} \tau_t &= 0.1 \times \tau_{t-1}, \\ \tau_t &= \tau_{t-1} + \left(0.01 \times f(x_{\text{global}}^{\text{best}}) \right). \end{aligned}$$

Below is an illustration of how PSO and ACO interact.

$$(14) \quad \text{IF } f(p_{\text{global}}^{\text{best}}) \leq f(x_{\text{global}}^{\text{best}}) \text{ THEN } x_{\text{global}}^{\text{best}} = p_{\text{global}}^{\text{best}}$$

update the direction of ants using the above equations.

$$(15) \quad \text{ELSE } p_{\text{global}}^{\text{best}} = x_{\text{global}}^{\text{best}}.$$

Then, the sender signs the hash value using the private key. Thus, the digital signature cannot be generated by any other user without the original private key. Then, the generated digital signature is appended with the data (or) document for further verification.

In Fig. 2, the procedure of the digital signature generation process is illustrated. First, the signer initiates the process by generating a hash value for a piece of data from the document. Then, the signature is appended to the data. Last, the digitally signed data is sent to the receiver.

Data encryption and decryption is performed by using these generated keys. The pipeline architecture of the RSA algorithm is depicted in Fig. 3. The first stage includes prime number generation. In the second stage, key generation process is performed. The third stage involves encryption and decryption processes.

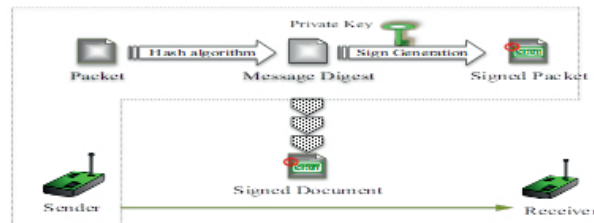


Fig. 2. Digital signature generation

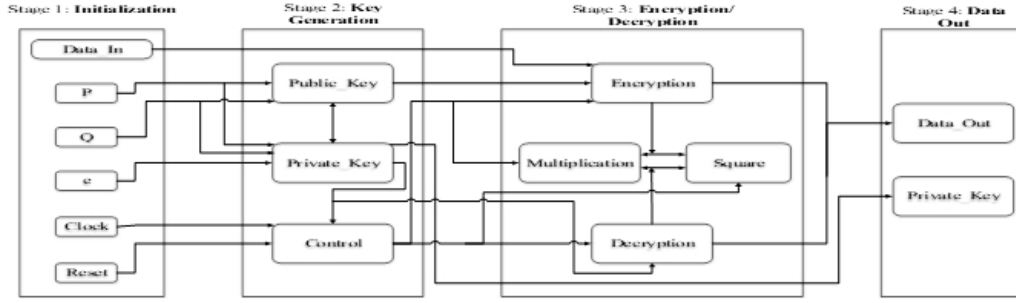


Fig. 3. RSA algorithm process

In this manner, data is encrypted in the RSA algorithm.

$$(16) \quad x_i^{t+1} = x_i^t + v_i^{t+1},$$

$$(17) \quad v_{kj}^{t+1} = g * v_{kj}^t + a_1 * e^{-\beta r_p^2} * (pbest_{kj} - x_{kj}^t) + a_2 * e^{-\beta r_g^2} * (gbest_j - x_{kj}^t).$$

Given that this is an issue of minimizing, $pbest_k$ the following updates:

$$(18) \quad pbest_k = x_k^{t+1} \text{ if } \text{fitness}(x_k^{t+1}) < \text{fitness}(pbest_k),$$

$$(19) \quad |x_k - X_k| = \sqrt{\sum_{j=1}^n (x_{kj} - X_{kj})^2},$$

where x_{kj} signifies the position of the j -th element of k -th mayfly and X_k either signifies $pbest_k$ or $gbest$.

$$(20) \quad v_{kj}^{t+1} = g * v_{kj}^t + d * r,$$

$$(21) \quad y_i^{t+1} = y_i^t + v_i^{t+1},$$

where y_i^t is maintained by applying the female mayfly's velocity to the location of the fly at time t as v_i^{t+1} .

$$(22) \quad v_{kj}^{t+1} = \begin{cases} g * v_{kj}^t + a_2 * e^{-\beta r_{mf}^2} * (x_{kj}^t - y_{kj}^t) & \text{if } \text{fitness}(y_k) > \text{fitness}(x_k) \\ g * v_{kj}^t + fl * r & \text{if } \text{fitness}(y_k) \leq \text{fitness}(x_k). \end{cases}$$

Mayfly crossover: To do the crossover procedure, first select the male mayfly, after that select the females. Since it depends on how fit they are, the best male breeds with the best female in this scenario. After a crossing, as shown, there are two offspring born.

$$(23) \quad \begin{aligned} O(S) \ 1 &= r_{of} * \text{male} + (1 - r_{of}) * \text{female}, \\ O(S) \ 2 &= r_{of} * \text{female} + (1 - r_{of}) * \text{male} \end{aligned}$$

Here, male is the parent of the male mayfly, female is certainly the parent of the female mayfly, and r_{of} is a predefined integer between 0 and 1. The beginning speeds of the progeny are fixed at 0.

Mayfly mutated gene: To increase the algorithm's ability to explore, the newly created offspring are modified. An additional randomly dispersed value is added to the offspring's variables as described in

$$(24) \quad \text{offspring } g'_n = \text{offspring } g_n + \kappa,$$

where κ is the number generator with a normal distribution.

Conclusion. An energy-efficient and trust-based WSN concept is put forward in this study. Thus, the LEACH method and the swarm intelligence method are used to choose the cluster leader. The cluster head is chosen using a customized form of the particle swarm method and a hybridized ant colony. The two characteristics of remaining energy and the amount of nodes communications that were successful are used to choose the cluster head. This two-parameter analysis of the node's trust aids in the data and energy preservation. This employs the enhanced RSA approach for digital signatures to apply encryption to data and safeguard networking. The efficiency of the suggested methodology was contrasted to other current strategies in terms of packet delivery ratio, throughput, network life, and node energy use. In the future, another trust-based management system will be proposed for sensor node verification.

REFERENCES

- [1] SINDHUJA M., K. SELVAMANI (2019) Cluster head selection framework for risk awareness enabled IoT networks using ant lion optimisation approach, *Wirel. Pers. Commun.*, **107**(4), 1–21, <https://doi.org/10.1007/s11277-019-06237-w>.
- [2] CHAUHAN S., M. SINGH, A. KUMAR (2021) Cluster head selection in heterogeneous wireless sensor network using a new evolutionary algorithm, *Wirel. Pers. Commun.*, **119**(4), 1–32, <https://doi.org/10.1007/s11277-021-08225-5>.
- [3] KHOT P., U. NAIK (2021) Particle-water wave optimization for secure routing in wireless sensor network using cluster head selection, *Wirel. Pers. Commun.*, **119**(2), 2405–2429, <https://doi.org/10.1007/s11277-021-08335-0>.
- [4] DANIEL J., S. F. V. FRANCIS, V. SARVESHWARAN (2021) Cluster head selection in wireless sensor network using tunicate swarm butterfly optimization algorithm, *Wirel. Netw.*, **27**(8), 1–18, <https://doi.org/10.1007/s11276-021-02812-x>.
- [5] SARKAR A., T. S. MURUGAN (2019) Cluster head selection for energy efficient and delay-less routing in wireless sensor network, *Wirel. Netw.*, **25**(1), 303–320, <https://doi.org/10.1007/s11276-017-1558-2>.
- [6] DONGYAO J., H. ZHU, S. ZOU, P. HU (2015) Dynamic cluster head selection method for wireless sensor network, *IEEE Sensors J.*, **16**(8), 1–1, <https://doi.org/10.1109/JSEN.2015.2512322>.

- [7] SUBRAMANIAN P., M. S. JOSEPH, S. SENTHILKUMAR, D. S. ALEX (2020) A hybrid grey wolf and crow search optimization algorithm-based optimal cluster head selection scheme for wireless sensor networks, *Wirel. Pers. Commun.*, **113**(4), 1–21, <https://doi.org/10.1007/s11277-020-07259-5>.
- [8] AUGUSTINE S., J. P. ANANTH (2020) Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks, *Wirel. Netw.*, **26**(1), 5113–5132, <https://doi.org/10.1007/s11276-020-02352-w>.
- [9] KARDI A., R. ZAGROUBA (2020) RaCH: A new radial cluster head selection algorithm for wireless sensor networks, *Wirel. Pers. Comm.*, **113**(4), 2127–2140, <https://doi.org/10.1007/s11277-020-07315-0>.
- [10] RAJESH D., T. JAYA (2020) A mathematical model for energy efficient secured CH clustering protocol for mobile wireless sensor network, *Wirel. Pers. Commun.*, **112**(2), 421–438, <https://doi.org/10.1007/s11277-020-07036-4>.
- [11] DING X. X., T. T. WANG, H. CHU, X. LIU, Y. FENG (2019) An enhanced cluster head selection of LEACH based on power consumption and density of sensor nodes in wireless sensor networks, *Wirel. Pers. Commun.*, **109**(4), 2277–2287, <https://doi.org/10.1007/s11277-019-06681-8>.
- [12] MEENA U., P. SHARMA (2022) Secret dynamic key authentication and decision trust secure routing framework for Internet of Things based WSN, *Wirel. Pers. Commun.*, **125**(2), 1753–1781, <https://doi.org/10.1007/s11277-022-09632-y>.
- [13] ALJUBAYRI M., Z. YANG, M. SHIKH-BAHAEI (2021) Cross-layer multipath congestion control, routing and scheduling design in ad hoc wireless networks, *IET Commun.*, **15**(8), 1096–1108, <https://doi.org/10.1049/cmu2.12145>.
- [14] EBRAHIM N. S., M. T. QUASIM (2021) EMCSS efficient multi-channel and time-slot scheduling, *Wirel. Netw.*, **27**(4), 2879–2890, <https://doi.org/10.1007/s11276-021-02620-3>.
- [15] LEE S.-B., S. NGUYEN-XUAN, J.-H. KWON, E. J. KIM (2022) Multiple concurrent slotframe scheduling for wireless power transfer enabled wireless sensor networks, *Sensors*, **22**(12), 4520, <https://doi.org/10.3390/s22124520>.

*Department of Electronics
and Communication Engineering
Sri Ramakrishna Engineering College
Coimbatore, Tamil Nadu 641022, India
e-mail: adlinejancy667@gmail.com*

**Department of Computer Science
and Engineering
Dr. N. G. P. Institute of Technology
Coimbatore, Tamil Nadu 641041, India
e-mail: bgomramesh@gmail.com*