Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.031509
Article

Tech Science Press

Trusted Cluster-Based Communication for Wireless Sensor Network Using Meta-Heuristic Algorithms

Pankaj Kumar Sharma[1,*] and Uma Shankar Modani[2]

[1]Department of Computer Engineeing, Mahila Engineering College, Ajmer, India
[2]Department of E&C Engineering, Engineering College, Ajmer, India
*Corresponding Author: Pankaj Kumar Sharma. Email: pankaj.gmeca@gmail.com
Received: 19 April 2022; Accepted: 16 June 2022

Abstract: The mobile transient and sensor network's routing algorithm detects available multi-hop paths between source and destination nodes. However, some methods are not as reliable or trustworthy as expected. Therefore, finding a reliable method is an important factor in improving communication security. For further enhancement of protected communication, we suggest a trust cluster based secure routing (TCSR) framework for wireless sensor network (WSN) using optimization algorithms. First, we introduce an efficient cluster formation using a modified tug of war optimization (MTWO) algorithm, which provides load-balanced clusters for energy-efficient data transmission. Second, we illustrate the optimal head selection using multiple design constraints received signal strength, congestion rate, data loss rate, and throughput of the node. Those parameters are optimized by a butterfly optimal deep neural network (BO-DNN), which provides first-level security towards the selection of the best head node. Third, we utilize the lightweight signcryption to encrypt the data between two nodes during data transmission, which provides second-level security. The model provides an estimation of the trust level of each route to help a source node to select the most secure one. The nodes of the network improve reliability and security by maintaining the reliability component. Simulation results showed that the proposed scheme achieved 45.6% of delivery ratio.

Keywords: Trust model; WSN; secure routing; cluster formation; load-balanced clusters

1 Introduction

Routing is a basic feature of the Wireless Sensor Network (WSN). However, although many routing protocols have been suggested, most are tailored to the node's limited functionality and network usability, and security issues remain unresolved [1]. WSN plays an important role in a spacious variety of applications, from critical military observation to forest fire monitoring and security monitoring [2]. Advances in hardware technology micro-electro-mechanical systems (MEMS) knowledge and wireless statements have led to the increase of fresh types of computing devices famous as sensor nodes [3]. Along with the rapid development of electronic and wireless communications, there are also extensive

applications for the WSN [4]. The basic part of this network configuration is how the sensors transmit data. Special routing protocols are required to control the transport phase [5]. WSN contains a large number of sensor nodes, and the nodes are clustered throughout the forest. Nodes commonly use wireless communication and are easily attacked by enemies, especially if heard. Therefore, all sent messages must be encrypted [6].

Advances in the microwave and digital electronics have created low-cost power sensors that can connect wireless networks and build wireless sensor networks [7]. To achieve its potential, WSN requires new technologies and methods that take into account the size and extreme mobility of these networks, the limited resources of sensor devices, and the inaccessible open communication configuration. These restrictions represent unique design issues [8]. Recently, the Integrated WSN of sensor technology, wireless communication technology, and built-in computing technology has developed into the latest study area in the field of in sequence knowledge [9]. Most recently proposed sensor network routing protocols are subject to various attacks. To address this issue, some researchers have begun developing secure routing protocols for WSN [10]. Previously, several routing protocols were suggested for WSN. Security and energy effectiveness are two major concerns associated with WSN routing [11]. Wireless sensor networks are considered to be one of the most important technologies in the 21st century. Sensitivity Electronic sensors measure the atmospheric conditions associated with the surroundings and convert them into electrical signals. In many WSN applications [12], WSN has several small sensor nodes that enable detection, computation, and wireless communication. Random or static layouts are used to create a network of sensor nodes depending on the application [13–15].

Nodes can connect manually and all nodes are involved in finding and maintaining paths to other nodes in the network. Security is the most important factor when building or designing a sensor network. WSN is helpful for a range of applications, but this white document focuses happening applications that operate in a great environment, such as battlefields, which prevent damage from manual engineering work [16]. Recently, a WSN has appeared in a range of applications, with home safety, forces systems, and fitness-minded. The antennas nodes deployed in this network are the topic of multiple WSN attacks, such as sinkholes, selective forward, spoofing, and wormholes [17,18]. With the rapid development of the Internet of Things (IoT), cloud computing, and social networking; smart cities are gaining more and more attention in modern society. With a variety of decentralized smart devices, Smart City can offer city dwellers a variety of applications such as environmental monitoring, traffic management, and social entertainment [19]. WSN consists of a small figure of antenna nodes that are squat power and source-sensitive sensor drive. This antenna node communicates wirelessly primarily with broadcasting [20–25]. The major donations of proposed TCSR frameworks are, MTWO and BO-DNN used to choose the trusted node for the secure routing protocol. Modified tug of war optimization is used to balance the load for efficient data transmission. Then, we illustrate the optimal head selection using multiple design constraints received signal strength, congestion rate, data loss rate, and throughput of the node. Finally, we utilize the lightweight signcryption to encrypt the data between two nodes during data transmission, which provides second-level security.

The rest of this paper is organized. In Section 2 related works are explained in the area of trust-based routing protocols in WSNs. The problem statement and main objective are explained in Section 3. In Section 4, the proposed algorithm is presented. The results, comparative analysis, and effectiveness of the framework are deliberated in Section 5. The final section describes the conclusion of the paper.

2 Related Works

Basha et al. [26] used WSNs in military applications, and sometimes electronic devices to process the most important personal data, such as physical electronic sensors, medical devices that report medical needs, and all kinds of drugs. Many methods and techniques have been developed for this purpose, of which

faith-based methods are the best. The trust system provides integrity, reliability, and data access to all nodes and provides excellent security. Data overhead is a reliable approach that creates problems such as system congestion. This has a direct impact on the data collection process, which greatly shortens the overall life of the network. This study suggests the rewarding smart Ad hoc routing (RSAR) protocol: the RSAR method for solving specific problems. RSAR starts by measuring the reliability factor of individual sensor nodes. Values are calculated using the optimal confidence deduction copy with the uncertain traction of the combat optimization algorithm. Information integration reduces the instantaneous data flow of individual nodes, filters only the required data, and sends the collected in sequence to the getting page. The efficient power competence of this particular function can be achieved by duplicating and removing invalid data from the stored data, which increases WSN life by saving the battery. The reliability factor calculations provided in this way help to assess the reliability and identify the attack and reduce the attack.

Saeed et al. [27] suggested a locked force resourceful and collaborative steering procedure for underwater WSN (UWSN). Secure Energy Efficient and Cooperative Routing (SEECR) contains an energy-efficient function and strapping protection against attack in the aquatic surroundings. SEECR uses supportive steering to improve network presentation. SEECR is environmentally friendly as it uses the least amount of calculations to implement resource-limited UWSN environment protection. To estimate the presentation of SEECR, this study compares the presentation of SEECR with that of Adaptive Mobility of Courier Nodes in Threshold-optimized DBR (AMCTD). This is a known routing protocol for adaptive movement of courier nodes in a threshold-optimal DPR-UWSN environment. The results indicate to the presentation of SEECR is healthier than that of AMCTD. 9% improvement on SEECR live terminals, 50% or more reduction in transmission loss, 9% performance improvement, 23% power line reduction, 25% non-latency reduction. In addition, the attack significantly reduces the effectiveness of the AMCTD, while the impact of the attack is minimal due to the security features included in the SECR.

Babaeer et al. [28] explained that in a wireless sensor network, a sensor sometimes transmits detected data to a central station in a particular environment via wireless communication. Leaving it open could lead to a security attack. Single-hole attacks are destructive attacks that target a network layer, where single-hole nodes attract other nodes and advertise the best route to the base station. This frees up other sensor node pockets and compromises network safety. Therefore, to ensure data integrity when transmitting this task, Threshold recommends a lightweight and locked method founded on the Beginning Sensitive Energy Efficient Sensor Network protocol and watermarking technology. The uniform encryption used in this project is wild and effective and uses less energy when detecting sensor nodes for single detection and defense purposes. This method certifies the honesty and reliability of the data detected when data is transferred from the sensor terminal to the base station and can detect data corruption.

Ahutu et al. [29] suggested that the nodes in the WSN are rich and energy-efficient because the computational capabilities are limited and the nodes run on a standard battery. suitable to the low safety surroundings of the WSN, a few spiteful nodes can dig the guys to another location, drop the guys and damage the network due to hearing impairment, which is called a wormhole attack. Current protocols address the issue of wormhole attacks isolated from multi-node power consumption. However, other specific solutions are considered to reduce consumption to detect these attacks, but better performance needs to be explored. This study introduces a frivolous multi-hop steering procedure for 802.15.4 WSN, which aims to reduce force expenditure and notice wormhole attacks. Research has shown to MAC Centralized Routing Protocol (MCRP) is better than added related protocol currently in use.

Pavani et al. [30] focused on the power spending of antenna networks. Cluster-based steering protocols are frequently recommended to decrease force expenditure. However, bricks are weak because of malicious margins. The malicious node sends the wrong message to the cluster header and increases statement slide and force expenditure. Secure cluster-based steering is the most important solution that uses more power during

data broadcast. In this learning, the author of the Secure Cluster-Based Routing Protocol (SCPRP) uses Adaptive Particle Mass Optimization (PMO) using the Optimal Firefly Algorithm when transferring data over a wireless sensor network. This study aims to improve the overall network life by reducing the expenditure of nodes and energy consumption. The planned SCPRP is based on a hexagonal antenna network configuration designed using three processes, including force proficient cluster, locked steering, and safety testing. The presentation of the future SCPRP is appraised using NS-3, as well as various other factors such as encryption time, encryption time, power expenditure, pocket drip rate, and system life. SCPRP has been shown to violate previous approaches.

Kojima et al. [31] In this study, the secure routing protocol is a technique for validating routing using cryptographic authentication on ad hoc networks where devices can switch networks over wireless communication. Secure DSR, a secure routing protocol used by identity-based ISDSR is a recently introduced cryptographic compact network, somewhere each tool receives the steering in sequence and the signature size created by the previous device. Signed. ID information transmitted through the packet can be used as a community key. though ISDSR has to communicate with a centralized generation center (KGC), so it is difficult to participate in the new instrument protocol. In addition, the results of ISDSSR implementation are not presented. ISDSR +, a safe steering procedure lacking central KGC, which uses dispersed, key age group and general functions of ISDSR. ISDSR + uses a new autograph method that allows nodes to attain a covert key as long as the digit of existing KGCs exceeds a confident limit. This means that many KGCs are not available, but the lingering KGCs can unmovingly enter a covert key. We are implementing a prototype of raspberry pie to show the best results for ISDSR +. 0.1 V Calculation time for secret key generation and travel time (RTD) shows results in reasonable adjustment. Better than the pure secure routing protocol with RDT RSA signature on ISDSR.

Albakri et al. [32] discussed the new design of secure end-to-end routing protocol in wireless sensor networks. They are based on the collection Key Pre-Distribution System (GKPS) with multi-layer polynomials. Group keys, also known as routing keys, are second-hand to keep information transmitted over the complete steering route. In particular, it is the first and foremost protected statement that uses single-path keys to keep information across the route, rather than using secure communication between links with multiple pairs of shared keys. The difficulty among all multi-model base core sharing programs is to the safety of these programs is called fixed K-security, which depends on the size of the selected multivariate. In added terms, if the size of the selected polynomial is k, capturing a k + 1 sensor (or added) may undermine the security of your scheme. Mounting the size of the polynomial may get better safety, but it also increases the storeroom and computing supplies of the sensor. In this study, the primary polymorphic GKPS base on polymorphism was developed. The security probability of this program is likely to compromise KK's security, i.e., GKPS after the K + 1 sensor is captured. The sensor was found to greatly reduce the risk of capture attack.

Sun et al. [33] presented a protected steering procedure based on multi-object ant colony-optimization (SRPMA) for wireless antenna network. And Colony developed the algorithm as a multi-oriented steering algorithm that considers the remaining force of a node and the reliability of a trail as two optimized targets. A single path is created hereby information containing multiple pheromones and two purpose functions. The reliability rating copy was reputable with the enhanced D-S source theory with collision pre-processing to estimate the reliability level of the tip node. A variety of routing results of complex distance scales can be obtained using an external archiving method using the Pareto Optimal Solution mechanism. Simulation results using NS2 show that the specific algorithm for black crack assault in WSN steering will realize the desired performance.

Kavidha et al. [34] concern was energy consumption and quality of service (QoS) in WSN. Similar sensor nodes in a versatile network are efficient network strategies. Features include advanced processing

capabilities, additional memory performance, and remote transfer capabilities. Effective clustering and path generation between pairs of nodes, as well as effective innovative cryptographic algorithms and adaptive DTMA scheduling (ECADS) methods, have been proposed as protocols to facilitate network communication. This allows data packets to be delivered to the mobile pool promptly. Here we present a protocol called Neural Elliptic Collies (NEG) Encryption for competent data protection. Additionally, position solitude (entry join failure discovery) is in use in reports for best safety. The cluster head (CH) is selected based on its ability to control data collection across multiple nodes in the network. It presents a hybrid of DTMA-based and Lion optimization preparation for optimum CH collection used for optimal dynamism efficiency. Lastly, Icats can be enhanced using WSN presentation metrics such as package deliverance rate, performance, low power consumption, communication slide, and back-to-back stoppage.

Karthick [35] points out that the use of autonomous networks (SONs) is increasingly used as it is increasing day by day. Unlike a normal network, SON can be reconfigured in the event of a network failure. However, when routing on this network, data is lost due to a lack of security. Therefore, several researchers have conducted research to provide secure routing across different SONs. However, security is still an issue, especially when guiding SONs over a wireless sensor network (WSN). In this study, WSN developed a new protocol for safe detection. The specific protocol is called the Trust-Distrust Protocol (TDP). Routing is done in 4 steps, according to the specific protocol. The initial step is k-, which is the space organization via the algorithm. The next step is Link Quality Appraisal (LQA), wherever the excellence of each system node is evaluated. The third step is to rank based on the LQA worth and assign quality points to each join in the network. In the final step, the safest routing trail is resolutely based on the quality point. Evaluate performance against existing LEACH protocols. This protocol eventually overrides the current routing protocol and recommends blood circulation in the SON.

3 Problem Statements and Network Model

3.1 Problem Statement

Hue et al. [36] have proposed the OR in WSNs by the A hybrid optimization algorithm known as Monarch-Cat Swamp Optimization (M-CSO) is a combination of Monarch Butterfly Optimization. The system works on two main points: the selection of security nodes and the selection of opportunistic nodes in select security nodes. The variety of security nodes with tolerance steady is based on faith, communication, and QoS parameters. Those parameters are clear, and QoS determines what describes the length and delay of the connection. M-CSO selects opportunistic nodes based on the reliability, distance, wait, and connectivity of the exercise parameters. Several solutions have been proposed to protect WSN, including secure routing. This is the main protocol of the WSN because it directs the data distribution to the routing base station. It is therefore important to consciously lead a flexible and safe path from packet drop, makeover, and engagement processes. It offers several solutions to protect the root, especially from uncompromising edges. In general, this will easily eliminate common attacks and significantly reduce WSN performance. Traditional security systems, such as encryption and authentication, cannot withstand attacks in any way because they are often from uncompromising nodes. A trust system was recently established to improve security and strengthen node cooperation. For further enhancement of protected communication, in this document, we suggest a TCSR) framework for WSN using optimization algorithms. The major contributions of proposed TCSR frameworks are summarized as follows:

1. First, we introduce an efficient cluster formation using the MTWO algorithm, which provides load-balanced clusters for energy-efficient data transmission.
2. Second, we illustrate the optimal head selection using multiple design constraints received signal strength, congestion rate, data loss rate, and throughput of the node. Those parameters are

optimized by a BO-DNN, which provides first-level security towards the selection of the best head node.

3. Third, we utilize the lightweight signcryption to encrypt the data between two nodes during data transmission, which provides second-level security.

3.2 Network Model

The main objective of the proposed TCSR procedure is summarized as follows:

1. To propose a new secure routing framework for WSN.
2. To study and develop a novel clustering technique for node grouping.
3. To study and collect multiple design constraints for head node selection.
4. To ensure first-level security towards the selection of the best optimal head node.
5. To illustrate a new secure crypto algorithm for encryption purposes should be a lightweight.
6. To ensure second-level security towards a new secure crypto algorithm.

The proposed TCSR framework can implement in Network Simulator (Ns2) tool and the effectiveness of the TCSR framework is evaluated using different simulation setups. The performance of the proposed framework can compare with the existing state-of-art routing techniques in terms of different performance metrics. Fig. 1 shows the proposed TCSR framework for WSN using optimization algorithms.

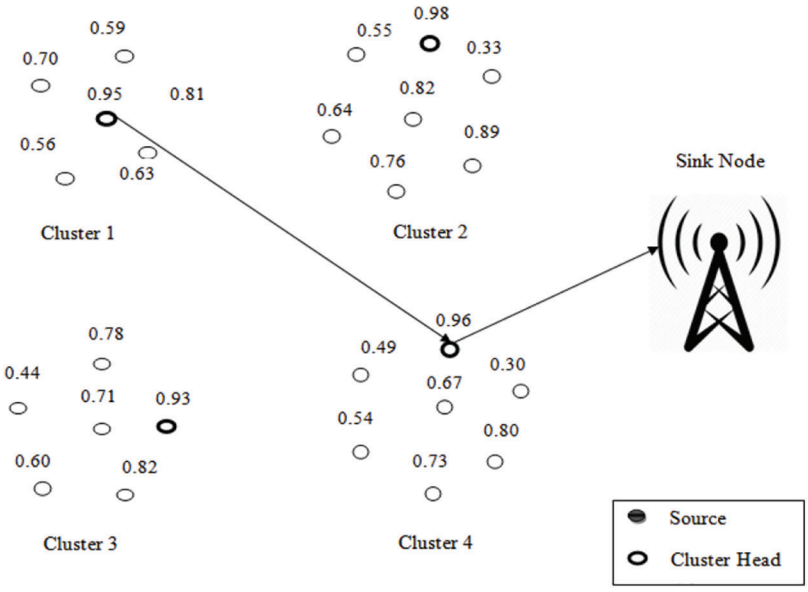


Figure 1: Proposed TCSR protocol

4 Proposed TCSR Framework for WSN Using Optimization Algorithms

4.1 Energy-Efficient Data Transmission Using MTWO Algorithm

The MTWO is a demographic meta-heuristic algorithm that assumes that each candidate solution is Xi = {Xi, j a. The weight of the band is resolute by the class of its solution and its proportion to the amount of traction that the group can exert on the rope. Logically, the opposite team must preserve at least a similar strength to hold on to the ropes. The brighter team hastens to the lighter squad, which creates MTWO's accumulator operator. This algorithm improves the quality of the solution with the

described accumulator operator to balance proper testing/use. The stages of MTWO can be summarized as follows: Step 1: Start N An approximate population of initial solutions is generated:

Step 1: Initialize a population of N primary solutions is generated at random

$$z_{ab}^{0} = z_{b,\min} + rand(z_{b,\max} - z_{b,\min}) \forall b = 1,\ 2,\ 3,\ \ldots,\ n \tag{1}$$

Here z_{ab}^{0}. presents the initial value of *bth* variable of the *ath* element solution; $z_{b,min}$ and $z_{b,max}$ are the minimum and maximum allowable ideals for the *bth* flexible, respectively; *rand* represents a random number that is identical sharing in the period [0,1]; n is the number of optimization elements.

Step 2: Determination of element designs and weight assignment

For the applicant solutions, the aim function values are estimated. All of the original results are arranged and noted in a memory. Every solution is considered as a team that has the following weight:

$$W_a = \frac{fit(a) - fit_{worst}}{fit_{best} - fit_{worst}} + 1 \quad \forall a = 1,\ 2,\ 3,\ \ldots..,\ n \tag{2}$$

where $fit(a)$ the kinetic value of it particle; The exercise value in Group 5 is calculated as the objective operational value for which the controlled complications are penalized; fit_{best} and fit_{worst} represents the fitness ideals for the greatest and worst contestant solutions for the present repetition. Team weight ranges from 1 to 2.

Step 3: Competition and displacement

The resultant force influence the team *a* due to its contact with heftier team b in the *cth* repetition can then be considered as follows:

$$F_{\tau,ab}^{c} = F_{v,ab}^{k} - W_{\tau}^{c},\ \ \mu_b \tag{3}$$

where, $F_{p,ab}^{\mathrm{k}}$ is the lugging energy among teams *a* and *b* in the *cth* iteration, and μ_b is coefficient considered for kinematic friction. Therefore, team *a* quickens towards team *j*:

$$A_{ab}^{c} = \frac{F_{\tau,ab}^{c}}{W_{\tau}^{c},\ \ \mu_b} * g_{ab}^{c} \tag{4}$$

where A_{ab}^{c} is the hastening of the team *a* towards team *b* in the *cth* repetition; g_{ab}^{c} is the gravitational hastening constant clear as:

$$g_{ab}^{c} = x_{b}^{c} - x_{a}^{c} \tag{5}$$

The second term in the above equation is randomized by the algorithm. This term can describe any part of the search area that I moved after removing the used power and before stopping. KK's role is to regularly reduce the irregular part of the team measure. In most requests [0.9, 0.99] intervals can be calculated as default. The higher the value, the more the algorithm collects and the candidate solution helps to navigate the search space further. The interval is the selectable factor [0,1] and this parameter panels the phase as the applicant moves through the search space. When searching the search space more accurately in smaller steps, you must select a smaller value of this parameter between 0.01 and 0.05. Design variables that exceed the allowable limit per minute, respectively.

$$\Delta x_{a}^{c} = \sum_{b=1}^{N} \Delta x_{ab}^{c} \tag{6}$$

The new situation of the team a at the finish of the cth repetition is then considered as:

$$x_a^{c+1} = x_a^c - \Delta x_a^c \tag{7}$$

$$x_a^c = GB_b + \frac{rand\, n}{k} GB_b - x_{ab}^{c-1} \tag{8}$$

GB_b (i.e., the best solution ever) is the *bth* adjustable of the greatest solution in the world. Randn is the most common distribution drawn by random numbers. The newly created variable is still unlikely to be out of the search area. In these cases, fly pack technology is used. The above plan is used with a confident probability (0.5 in this file). The limit for the remaining events is calculated as the fresh rate of the *bth* optimization flexible.

4.2 Optimal Head Selection Using BO-DNN

In the particular utilitarian type how idle factors and perceptions interface was somewhat subjective. With a solitary layer, be that as it may, this can be very testing on account of the recognition we secure this issue by including extra layers. Within BO-DNN this is extra dubious since we first want to opt how and anywhere to include additional non-linearity. Our exchange underneath centers basically around long short-term memory (LSTM) yet it smears to other arrangement models, as well. We can add additional nonlinearity to the gating components. We could stack different layers of LSTMs over one another. This outcome in a system is progressively adaptable due to the blend of a few straightforward layers. In particular, data may be significant at various degrees of the stack. We should maintain prominent rank information about money-related financial situations (bear or positively trending business sector) easy to get to at a significant equal, while at a lesser equal we just record shorter-term fleeting elements.

4.3 Encrypt Data Using Lightweight Signcryption

The signature scheme generalizes the parameters to all users, which is summarized below. The structure of the proposed signature scheme is shown in Fig. 2. The circumstances under consideration include Key transaction: Create a public/private pair of keys for both parties (sender-Alice, receiver-pop) according to the algorithm. 1. Signature Creation, Encryption: Alice wants to send a message to Bob safely. Alice accepts the Pope's public key and signs the message and gives the text. Seed Signature verification and encryption: Receive unsigned text (r; s; c) from Bob Alice and retrieve the message (M) [36].

Algorithm: Key Generation Algorithm

1 Procedure GENERATE THE KEYS

2. Generates two large integers α_a, α_b

3. Alice has chosen a secret key α_a. Similarly, Bob's secret key is α_b

4. Selects a random number x and computes both the public key of Alice $T_{g,\alpha_a}(x)$ mod p and Bob $T_{g,\alpha_b}(x)$ mod p.

5. Send the tuples $(\alpha_a;\ x,\ (T_{g,\alpha_a}(x))$ mod p, and $(\alpha_b;\ x,\ (T_{g,\alpha_b}(x))$ mod p to Alice and Bob respectively.

6. Publish the public keys of Alice $(x,\ (T_{g,\alpha_a}(x))$ and Bob $(x,\ (T_{g,\alpha_b}(x))$.

7. End procedure.

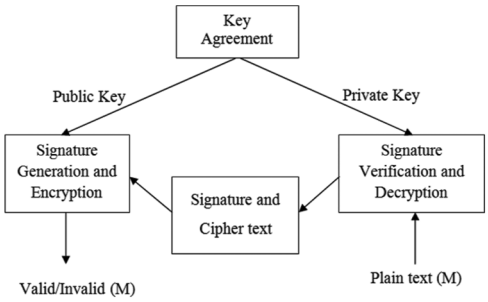


Figure 2: Signcryption process for data encryption

5 Results and Discussion

The comparative analysis of proposed and existing routing protocols is discussed in this section with different simulation setups. Here, the proposed TCSR protocol is compared with the existing routing protocol i.e., M-CSO [37].

5.1 Simulation Parameters

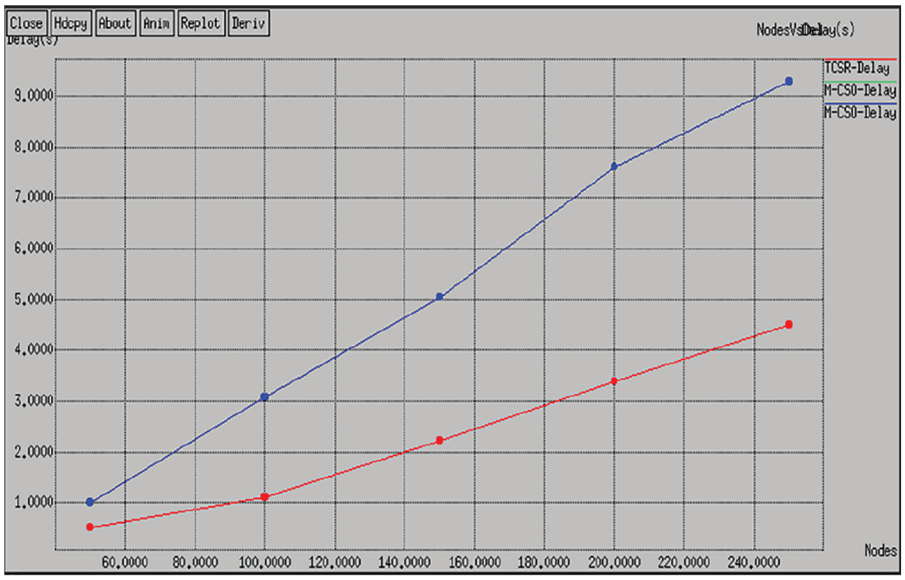
The proposed approach is implemented in the platform of NS2. In a sensor network of the size 1500 m × 1500 m area with randomly deployed sensor nodes, the simulation has been performed. The bandwidth is set at a low rate of 256 Kbps. Set the maximum data packet cache to 50, which increases the signal conflicting probability. We use IEEE 802_11 MAC protocol incorporates with wireless channel and wireless phy type network interface. The maximum number of packet transfers between source-destination is 1000 bits. The initial energy per node is 1 J and the total energy is 150 J. Transmission energy is 50 nJ/bit and the receiving energy is fixed at 50 nJ/bit. The performance of the proposed TCSR protocol is investigated by three dissimilar simulation situations impact of node density, attack nodes, and rounds. The performance of the proposed TCSR protocol is compared with the existing M-CSO routing protocol in terms of different metrics delay, throughput, energy consumption, delivery ratio, and detection rate.

5.2 Scenario-1 Node Density

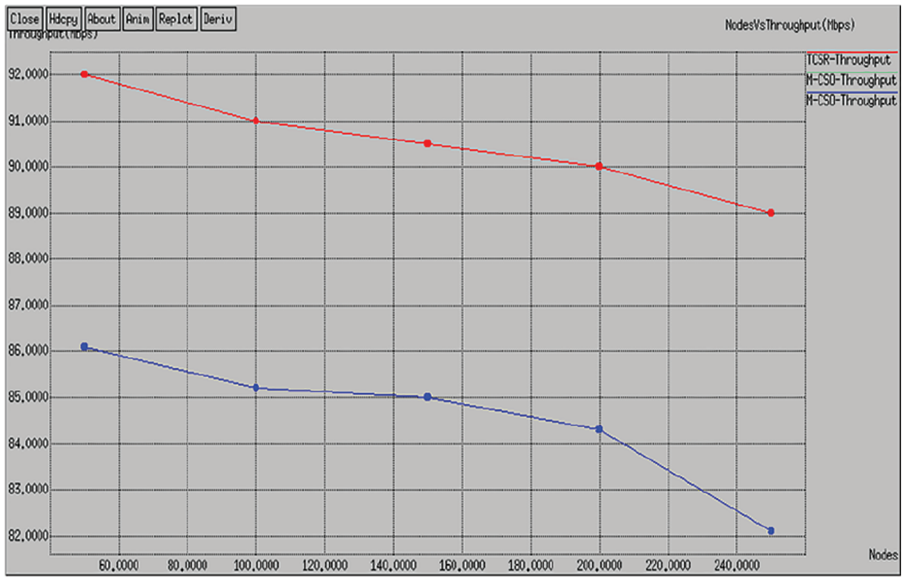
In this situation, we vary the number of nodes as 50, 100, 150, 200, and 250 with a fixed network size of $1500 \times 1500\ m^2$. The comparative study of the proposed and existing routing protocol is given in Tab. 1. As shown in Fig. 3a, the delay of the intended plot shows that TCSR is very effective evaluated to existing M-CSO routing protocol. Numerically, the projected TCSR protocol achieves a 60% improvement of delay over the existing protocol. The comparative analysis of the proposed and existing routing protocol is given in Fig. 3b. The plot shows the throughput of the proposed TCSR is very effective compared to the existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 34% improvement in throughput over the existing protocol. The comparative analysis of the proposed and existing routing protocol is given in Fig. 3c. The plot clearly shows the energy consumption of the proposed TCSR is extremely effective compared to the existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 25.6% enhancement of energy utilization more than the existing protocol. The comparative analysis of the proposed and existing routing protocol is given in Fig. 3d. The plot shows the delivery ratio of the proposed TCSR is very effective compared to the existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 45.6% improvement in packet delivery ratio over the existing protocol. The comparative analysis of the proposed and existing routing protocol is given in Fig. 3e. The plot shows the attack detection rate of the proposed TCSR is very effective compared to the existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 39.34% improvement in detection rate over the existing protocol.

Table 1: Performance comparison with the impact of nodes

1-Delay, 2-Throughput, 3-Energy consumption, 4-Deliver ratio, 5-Detection rate										
	TCSR					M-CSO				
	1	2	3	4	5	1	2	3	4	5
50	0.5	92	0.5	90	95	1	86	0.9	80	91
100	1	91	0.6	89	82	3	85	1.2	79	89
150	2	90	0.7	87	90	5	85	1.3	76	89
200	3	90	0.8	86	89	8	84	1.5	75	86
250	4	89	0.9	85	87	9	82	1.9	74	85

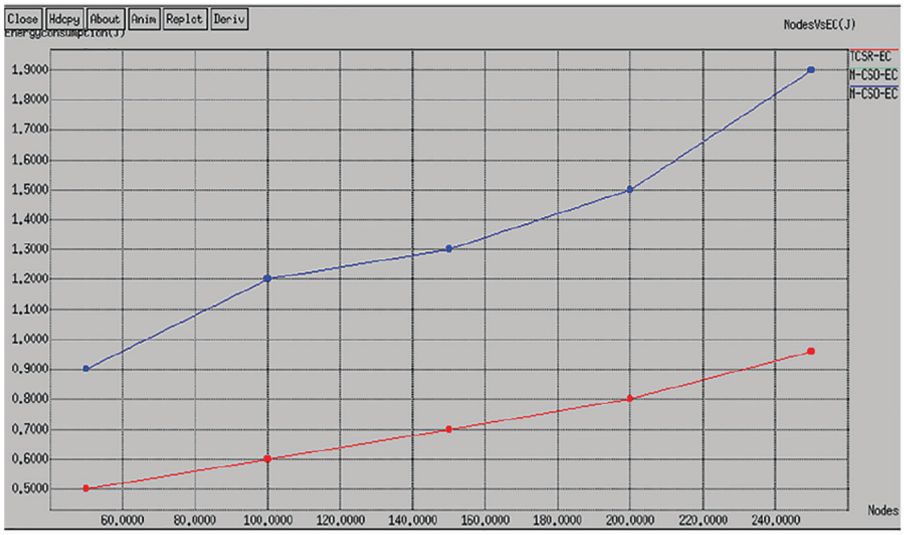


(a)

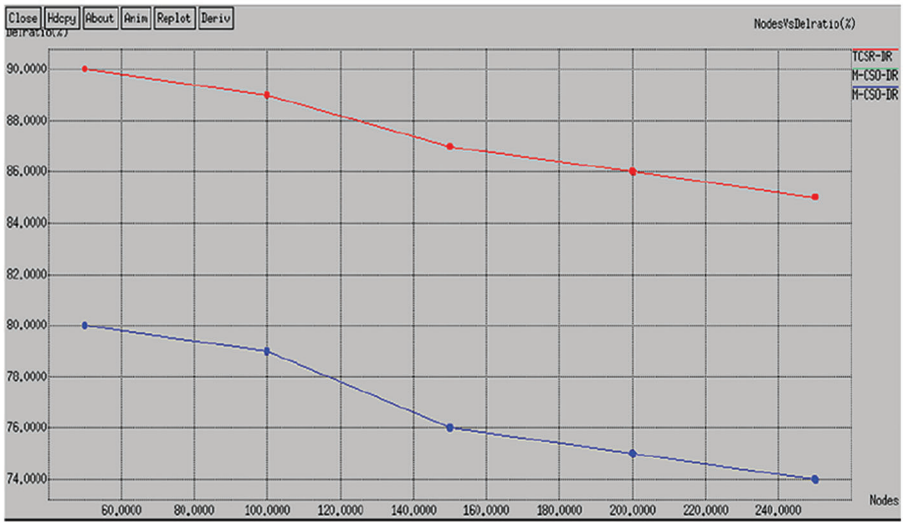


(b)

Figure 3: Continued

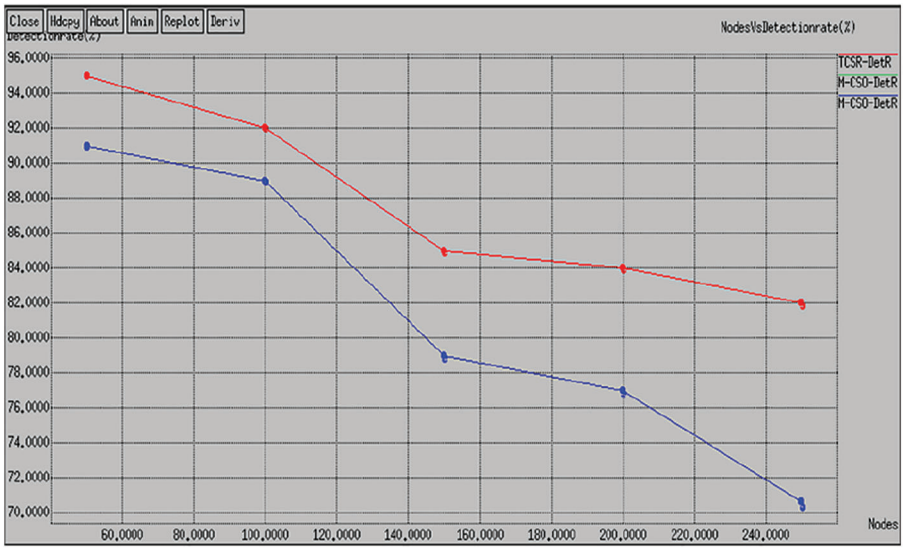


(c)



(d)

Figure 3: (Continued)

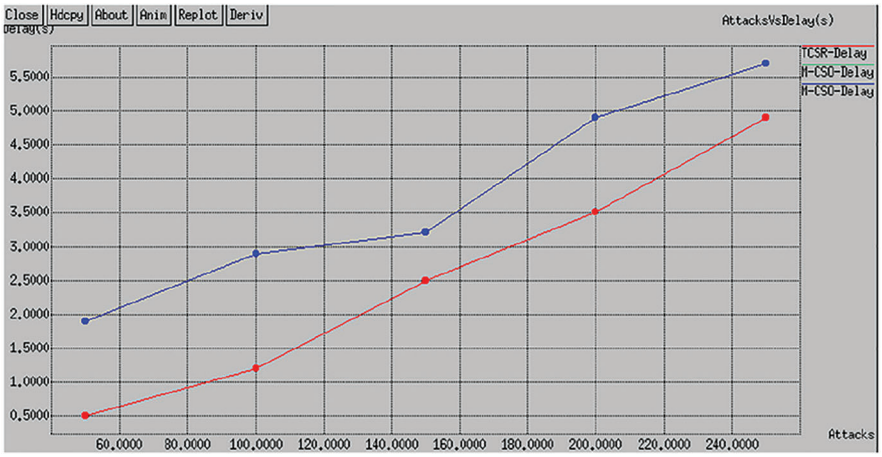


(e)

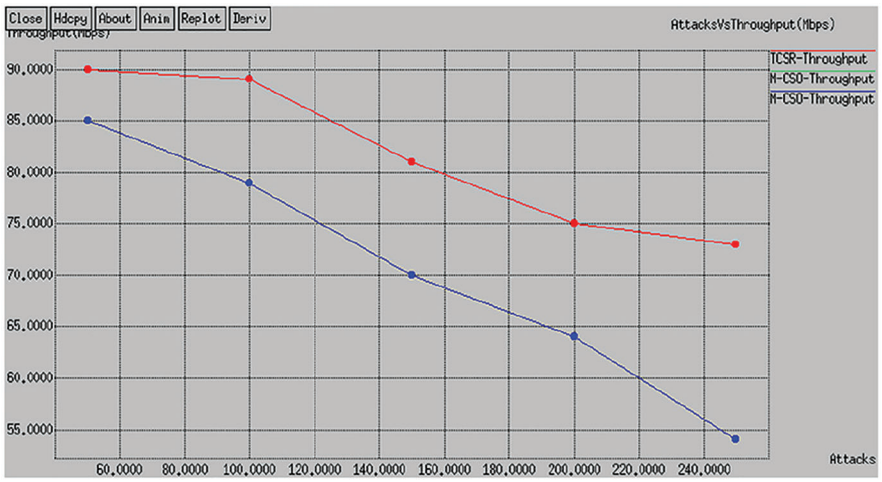
Figure 3: Performance analysis with node densities (a) Delay (b) Throughput (c) Energy consumption (d) Delivery rate (e) Detection rate

5.3 Scenario-2 Attack Densities

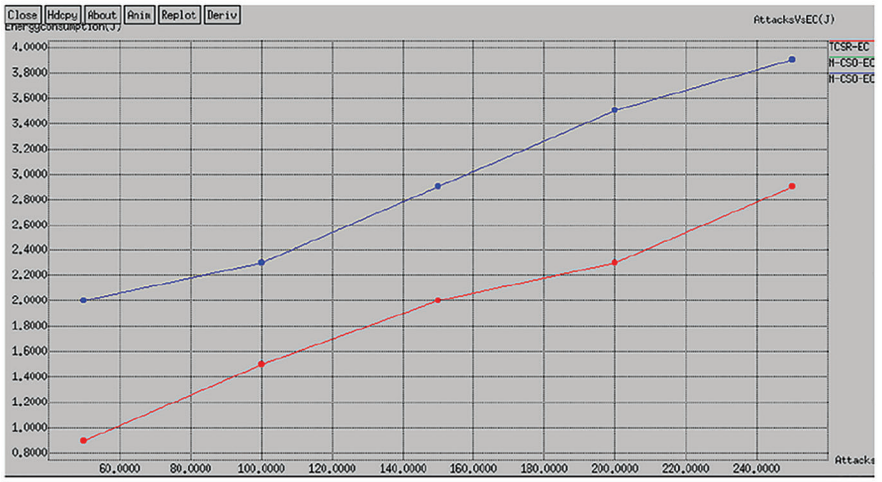
In this circumstance, we vary the number of attacks as 5, 10, 15, 20, and 25 with a fixed node as 250 and network size as 1500×1500 m^2. Here, we introduce three different attacks Blackhole, wormhole, and Dos attacks. The comparative study of proposed and existing routing protocols with different attacks is given in Tab. 2. The plan shows the interruption of the proposed TCSR is very effective evaluated to the existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 25% improvement of delay over the existing protocol as shown in Fig. 4a. The comparative study of proposed and existing routing protocols with different attacks is given in Fig. 4b. The plan shows the throughput of the proposed TCSR is very effective evaluated to existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 24.6% enhancement of throughput over the existing protocol. The comparative study of proposed and existing routing protocols with different attacks is given in Fig. 4c. The scheme shows the energy utilization of the proposed TCSR is very effective evaluated to existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 35% improvement in energy consumption over the existing protocol. The comparative study of proposed and existing routing protocols with different attacks is given in Fig. 4d. The plan shows the deliverance ratio of the proposed TCSR is extremely effective compared to the existing M-CSO routing protocol. Numerically, the proposed TCSR protocol achieves a 32.1% improvement in packet delivery ratio over the existing protocol. The comparative analysis of proposed and existing routing protocols with different attacks is given in Fig. 4e. The plot clearly shows the attack detection rate of the proposed TCSR is very effective compared to the existing M-CSO(31) routing protocol. Numerically, the proposed TCSR protocol achieves a 29.12% improvement in detection rate over the existing protocol.



(a)

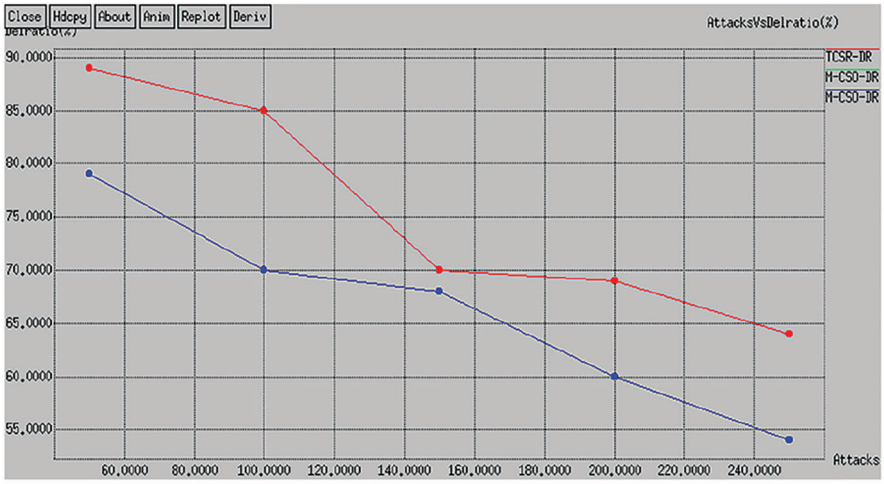


(b)

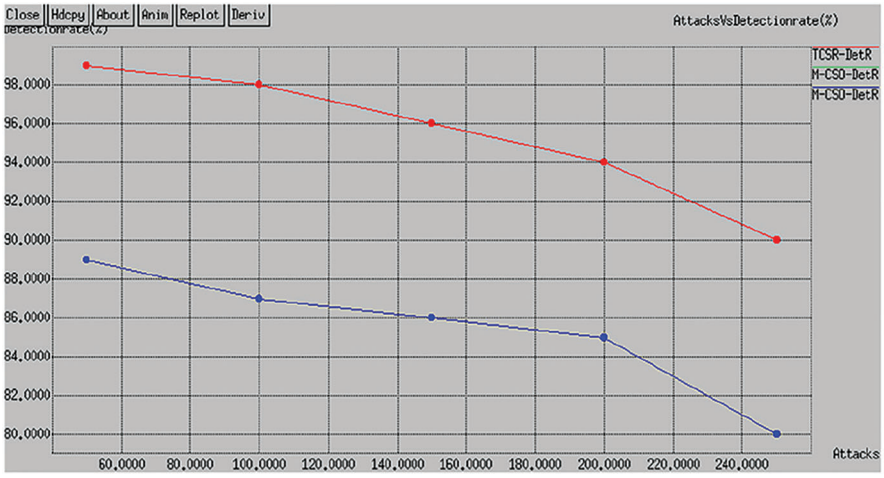


(c)

Figure 4: Continued



(d)



(e)

Figure 4: Performance analysis with attack densities (a) Delay (b) Throughput (c) Energy consumption (d) Delivery rate (e) Detection rate

Table 2: Performance comparison with the impact of attacks

1-Delay, 2-Throughput, 3-Energy consumption, 4-Deliver ratio, 5-Detection rate										
	TCSR					M-CSO				
	1	2	3	4	5	1	2	3	4	5
5	0.5	90	0.9	89	99	1.9	85	2	79	89
10	1.2	89	1.5	85	98	2.9	79	2.3	70	87
15	2.5	81	2	70	96	3.2	70	2.9	68	86
20	3.5	75	2.3	69	94	4.9	64	3.5	60	85
25	4.9	73	2.9	64	90	5.7	64	3.9	54	80

6 Conclusion

We have proposed a TCSR framework for WSN utilizing optimization algorithms. An efficient cluster formation is based on the MTWO algorithm, which provides load-balanced clusters for energy-efficient data transmission. The optimal head selection is performed using multiple design constraints received signal strength, congestion rate, data loss rate, and throughput of the node. A BO-DNN is used to optimize the constraints. The lightweight signcryption was utilized to encrypt the data between two nodes during data transmission, which provides second-level security. Finally, the results prove the effectiveness of the proposed TCSR protocol over existing state-of-art routing protocols in terms of different performance metrics.

Acknowledgement: The author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Prabhu and M. A. EA, "Trust based secure routing mechanisms for wireless sensor networks: A survey," in *2020 6th Int. Conf. on Advanced Computing and Communication Systems (ICACCS)*, pp. 1003–1009. IEEE, 2020.

[2] M. Biradar and B. Mathapathi, "Secure, reliable and energy efficient routing in WSN: A systematic literature survey," in *2021 Int. Conf. on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, pp. 1–13, IEEE, 2021.

[3] K. Hamouid, A. Barkat and S. Othmen, "Secure and lightweight hierarchical cluster-based data routing for wireless sensor networks," in *2019 Int. Conf. on Networking and Advanced Systems (ICNAS)*, pp. 1–6. IEEE, 2019.

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

[5] I. Almomani and E. Almashakbeh, "A power-efficient secure routing protocol for wireless sensor networks," *WSEAS Transaction on Computers*, vol. 9, no. 9, pp. 1042–1052, 2010.

[6] H. Lazrag, A. Chehri, R. Saadane and M. D. Rahmani, "A blockchain-based approach for optimal and secure routing in wireless sensor networks and IoT," in *2019 15th Int. Conf. on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp. 411–415. IEEE, 2019.

[7] O. Singh, V. Rishiwal, L. Kumar and P. Yadav, "Secure energy aware routingin wireless sensor networks," in *2019 4th Int. Conf. on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–6. IEEE, 2019.

[8] A. R. Kumar and A. Sivagami, "Balanced load clustering with trusted multipath relay routing protocol for wireless sensor network," in *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, vol. 1, pp. 1–6. IEEE, 2019.

[9] Y. Lan, Z. Zhibin, G. Fuxiang and Y. Ge, "The research on certainty-based secure routing protocol in wireless sensor networks," in *2006 Int. Conf. on Wireless Communications, Networking and Mobile Computing*, pp. 1–5. IEEE, 2006.

[10] G. Acs, L. Buttyán and I. Vajda, "The security proof of a link-state routing protocol for wireless sensor networks," in *In 2007 IEEE Int. Conf. on Mobile Adhoc and Sensor Systems*, pp. 1–6. IEEE, 2007.

[11] H. W. Ferng and D. Rachmarini, "A secure routing protocol for wireless sensor networks with consideration of energy efficiency," in *In 2012 IEEE Network Operations and Management Symp.*, pp. 105–112. IEEE, 2012.

[12] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through optimal power control and optimal handoff-based recovery mechanism," *Journal of Computer Networks and Communications*, vol. 2012, pp. 1–8, 2012.

[13] C. Deepa and B. Latha, "HHCS: Hybrid hierarchical cluster based secure routing protocol for wireless sensor networks," in *In Int. Conf. on Information Communication and Embedded Systems (ICICES2014)*, pp. 1–6. IEEE, 2014.

[14] J. Zhou, "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks," *International Journal of Distributed Sensor Networks 9*, no. vol. 4, pp. 1–17, 2013.

[15] N. A. Alrajeh, M. S. Alabed and M. S. Elwahiby, "Secure ant-based routing protocol for wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 9, no. 6, pp. 1–9, 2013.

[16] P. Gong, T. Chen and Q. Xu, "ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2015, pp. 1–10, 2015.

[17] A. M. El-Semary, "Energy-efficient secure routing protocol based on roulette-wheel and μtesla forwireless sensor networks," *International Journal of Sensor Networks and Data Communications*, vol. 1, pp. 1–13, 2012.

[18] W. Xin-sheng, Z. Yong-zhao and W. Liang-min, "Load-balanced secure routing protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 6, pp. 1–13, 2013.

[19] J. Duan, D. Yang, H. Zhu, S. Zhang and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, pp. 209436, 2014.

[20] H. Sarma, A. Kar and R. Mall, "A hierarchical and role based secure routing protocol for mobile wireless sensor networks," *Wireless Personal Communications*, vol. 90, no. 3, pp. 1067–1103, 2016.

[21] B. Yin, S. W. Zhou, S. W. Zhang, K. Gu and F. Yu, "On efficient processing of continuous reverse skyline queries in wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 4, pp. 1931–1953, 2017.

[22] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah and G. J. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Computers Materials & Continua*, vol. 56, no. 3, pp. 433–446, 2018.

[23] J. Wang, X. J. Gu, W. Liu, A. K. Sangaiah and H. J. Kim, "An empower hamilton loop based data collection algorithm with mobile agent for WSNs," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, pp. 1–14, 2019.

[24] J. Wang, Y. Gao, C. Zhou, S. Sherratt and L. Wang, "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for WSNs," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 695–711, 2020.

[25] J. Wang, Y. Gao, W. Liu, W. Wu and S. J. Lim, "An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks," *Computers Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.

[26] A. R. Basha, "Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network," *IET Wireless Sensor Systems*, vol. 10, no. 4, pp. 166–174, 2020.

[27] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad and M. Khattak, "SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 107419–107433, 2020.

[28] H. Babaeer and S. AL-ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking," *IEEE Access*, vol. 8, pp. 92098–92109, 2020.

[29] O. Ahutu and H. El-Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020.

[30] M. Pavani and P. Trinatha Rao, "Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks," *IET Wireless Sensor Systems*, vol. 9, no. 5, pp. 274–283, 2019.

[31] H. Kojima, N. Yanai and J. Cruz, "ISDSR+: Improving the security and availability of secure routing protocol," *IEEE Access*, vol. 7, pp. 74849–74868, 2019.

[32] A. Albakri and L. Harn, "Non-interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks," *IEEE Access*, vol. 7, pp. 31615–31623, 2019.

[33] Z. Sun, M. Wei, Z. Zhang and G. Qu, "Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks," *Applied Soft Computing*, vol. 77, pp. 366–375, 2019.

[34] V. Kavidha and S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with mobile sink," *Peer-to-Peer Networking and Applications*, vol. 12, no. 4, pp. 881–892, 2018.

[35] S. Karthick, "TDP: A novel secure and energy aware routing protocol for wireless sensor networks," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 2, pp. 76–84, 2018.

[36] T. T. K. Hue, T. M. Hoang and A. Braeken, "Lightweight signcryption scheme based on discrete chebyshev maps," in *2017 12th Int. Conf. for Internet Technology and Secured Transactions (ICITST)*, pp. 43–47. IEEE, 2017.

[37] P. Patil, R. Deshpande and P. 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.