Wireless Networks
https://doi.org/10.1007/s11276-020-02299-y

CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications

Dipali K. Shende[1,3] · S. S. Sonavane[2]

Abstract
WSN serves as a medium for linking the physical and information network of IoT. Energy and trust are the two major factors that facilitate reliable communication in the network. During multicast routing, the BS engages in forwarding the data securely to the multiple destinations through the intermediate nodes, which is the major challenge in IoT. The paper addresses the challenges through proposing an energy-aware multicast routing protocol based on the optimization, CrowWhale-ETR, which is the integration of CSA and WOA based on the objective function designed with the energy and trust factors of the nodes. Initially, the trust and energy of the nodes are evaluated for establishing the routes that is chosen optimally using CWOA. This optimally chosen path is used for the data transmission, in which energy and trusts of the individual nodes are updated at the end of the individual transmission, in such a way the secure nodes can be selected, and which improves the secure communication in the network. The simulation is analyzed using 50 and 100 nodes in terms of the performance measures. The proposed method acquired the minimal delay of 0.2729 and 0.3491, maximal detection rate of 0.6726, maximal energy of 66.4275 and 71.0567, and maximal throughput of 0.4625 and 0.8649 in the presence and absence of attacks with 50 nodes for analysis.

Keywords IoT · Multicast routing · Optimization · WSN · Trust · CrowWhale-ETR · CSA · WOA

Abbreviations

WSN	Wireless sensor network
IoT	Internet of things
BS	Base station
CrowWhale-ETR	Crow Whale-energy trust routing
CSA	Crow search algorithm
WOA	Whale optimization algorithm
QoS	Quality of service
CWOA	CrowWhale optimization algorithm
GPS	Global positioning system
ESMR	Efficient self-organizing multicast routing protocol
CA	Certification authorities
GMR	Geographic multicast routing
QMRPRNS	QoS multicast routing protocol using reliable node selection scheme
FAST + FAMOUS	Faster algorithm + fast multiconstrained multicast routing algorithm
DDoS	Distributed denial of service
RFID	Radio-frequency identification
MITM	Man in the middle
MANET	Mobile ad hoc network

1 Introduction

Internet of things (IoT), a significant network interlinks the physical world with the cyber environment, which consisted of a large number of the objects, like sensors, RFID tags, actuators, and mobile devices that are connected to the internet through a wired/wireless connection [1]. Former IoT applications engage in sensing and actuating the surroundings with the limited computing and battery-operated devices communicating through a wireless channel [2]. On the other hand, the goal of IoT communication concentrated on the utilization of minimal network resources and power with

✉ Dipali K. Shende
shendedipalik@gmail.com

[1] Sinhgad Institute of Technology Lonavala, Kusgaon, Lonavla, Maharashtra 410401, India

[2] Indira College of Engineering and Management, Parandwadi, Pune, Maharashtra 410506, India

[3] JSPM, RSCOE, Tathwade, Pune, Maharashtra, India

Published online: 25 March 2020

effective QoS. The growth of IoT finds its valuable application in IoT mainly, in the medical and multimedia applications [3, 4]. The network optimization led to the energy conservation and the power conservation is assisted through the routing efficiency [5, 6]. WSN establish the effective means of communication in IoT through its powerful nodes [7]. IoT elaborates the idea of Internet from a homogeneous network of devices including the computers, home appliances, consumer electronics, or sensors nodes of WSNs. The merits of linking the WSN with other IoT members goes beyond the remote access, since the heterogeneous information models are capable of collaborating among each other to ensure a common service [8–10].

WSNs provide highly flexible monitoring and control in effective cost as they are autonomous and infrastructure-less [11]. The cost of the individual nodes is effective as the nodes in WSN are limited with respect to energy, memory, processing, and/or communication resources. Since energy is the major constraint, IoT serves as a compromising area that links billions of wireless sensors [7]. In MANET the network nodes are free to move to anywhere in the network [12]. The functioning and importance of the existing systems in industry are sometimes transformed with the reliable solutions rendered using IoT. Though IoT ensures opportunities for establishing the effective system, power consumption seems to be a major challenge in IoT [13]. Generally, the dynamic nature of the WSN environment is due to the unstable weather situations, exhaustion of sensor battery, presence or absence of the hurdle among the nodes in the network, mobility of the sensor and sink nodes. Due to the above fact, there is a frequent change in the routes between the nodes, which requires tracing and reacting through an effective routing protocol [11, 14–16]. Therefore, performing the network routing is a challenge because of the non-static nodes, which randomly move in the pre-defined search space [17, 18]. Secure node multicasting routing algorithm enhances the security by selecting the routes based on the fewer number of transmissions and also create a bandwidth minimal multicast tree. This will resist all the threats including wormhole attack [19].

For IoT applications, the messages are disseminated to few nodes through multicast transmissions. The multicast routing protocol establishes multicast paths for sending data packets between source and destination [20]. As an instance, an application in IoT using multicast transmission updates the prices in market on a electronic shelf labels. Literature subdivides the routing protocols as: non-geographic and geographic-based. In case of the non-geographic-based solutions, the request packets are flooded from the multicast source to all the destination nodes [6, 8, 21], whereas, in geographic-based multicast routing, the nodes know the location using GPS devices [5]. Multichannel routing minimizes the interference and congestion for improving the data rates and reducing the power consumption [22] that guarantees multiple QoS constraints. On the other hand, the network topology from adaptive to dynamic assists better performance in multimedia communications of IoT [23–25]. There is a need for highly efficient multicast routing to address the needs of multimedia communications in highly dynamic IoT environments. The main aim of algorithms for multicast routing increases the resource utilization and reduces the network energy consumption of the network than attaining the multiple QoS of multimedia communications [3].

1.1 Problem statement

The physical objects are monitored and controlled over the internet is called IoT. WSN is a medium to link the information and physical network of IoT. In multicast routing, the data is transmitted to the set of destination node from a base station in which the major challenge is secure transmission of data. The challenges for the efficient routing in the WSN are mentioned below,

- The nodes in the heterogeneous IoT differ from each other based on the memory, which are mostly memory less tags with effective sensors/actuators. On the other hand, the eligibilities of the nodes are different for assisting the reliable transport that is considered while establishing routes. Moreover, lower power transmission affects the reliability of the link with higher end-to-end errors [26].
- The burden of the nodes and the communication channels along with the greater mobility capabilities impose huge security threads to the IoT network. Additionally, the self-organizing nature of IoT nodes and the application of the solution based on the CA through the servers linked, pose a challenge for secure routing [27].
- The demerits associated with the WSN includes: random positioning of nodes, dynamic environment, restricted power, and limited processing ability. These issues pose unreliable communication and are subjected to the range issues [28].
- The multicast routing algorithm depending on priority assignment rule to detect the routes is computationally intensive and did not take into account, the trust level and energy even though these constraints are significant in IoT applications [5].

The proposed method the energy and trust of the nodes are evaluated and choose an optimal path for the data transmission using CWOA. This optimally chosen path is used for the data transmission, in which energy and trusts of the individual nodes are updated at the end of the individual transmission, in such a way the secure nodes can be selected, and which improves the secure communication in the network.

The primary intention of this research is to design and develop CWOA for energy aware multicast routing in WSN for IoT applications. This work aims to propose an enhanced version of the well-known multicast routing algorithm based on the CWOA. The proposed work aims to consider the two parameters including energy consumption and node's trust value. By considering these two parameters, a routing framework, called CrowWhale-ETR is proposed based on the four important steps, (1) measuring the trust level of a route, (2) measuring the energy level of a route, (3) route discovery, (4) route choosing. At first, the trust level and energy level of the nodes is measured based on the mathematical model. Once these parameters are computed, the route discovery and choosing is performed based on CWOA which is a new algorithm to be proposed by integrating COA with WOA.

The major contributions of the research are:

- To design and develop an effective algorithm for energy and trust aware multicast routing in WSN for IoT applications.
- Propose an enhanced version of the well-known multicast routing algorithm based on the CWOA.
- Aims to consider the parameters, energy and trust of the nodes that is employed to formulate the objective function for the proposed routing framework, called CrowWhale-ETR.

The rest of the paper is organized as: The review of the existing routing protocols is demonstrated in Sect. 2 along with the demerits of the methods. The proposed method of routing with the proposed protocol is discussed brief in Sects. 3 and 4 highlights the results of the proposed method. The summary of the paper is given in Sect. 5.

2 Literature survey

The section demonstrates the review of the eight literature works and the demerits of the methods are discussed to reveal the motivation behind the new model. Huang et al. [3] developed multicast algorithms to enable the multimedia routing based on the entropy, which employed the spanning tree and shortest tree paths. The method outperformed in terms of accuracy and speed, and minimized the complexity, but the method suffered with the limited resources. Pan and Yang [5] developed a routing protocol that chosen the intermediate nodes, eradicates the loops, and verified if the multicast links could be further merged. The transmission links were minimized and the path lengths were shortened. Moreover, the latency of multicast was reduced, but node mobility was supported. Porambage et al. [26] developed a group key establishment that was more effective for the centralized applications, but suffered from the MITM attack. Li et al. [29] developed the heuristic algorithms that yielded a better solution for the traditional NP complex issue and the delay bound was met while consuming much transmit power. Nisha and Balakannan [30] introduced energy ESMR that utilized the energy balance and rendered effective network lifespan. The method was efficient in enhancing the success packet rate, but the future energy of the node was required. Zhu et al. [31] developed a two-stage framework to optimize the path of the transmissions. There was found to be no interference, where there was a need for large time leading to the time complexity. Wang et al. [32] was developed using the distributed algorithm that solved the inter-layer optimization issue, which rendered higher flexibility and stability, which possessed slow convergence.

3 Proposed protocol for multi-cast routing in WSN for the IoT application

The main aim of multi-cast routing is to distribute the data to the multiple destinations and in this paper, the multicast routing is performed optimally using the proposed Crow–Whale optimization. The mobile nodes in the IoT network are subjected to the evaluation of the fit factor, which is based on trust and energy. Upon the selection of the secure nodes, the routes are discovered for the optimal selection of the optimal routes. The routes are chosen based on the proposed CrowWhale optimization, which is the modification of the WOA [33, 34]. The optimally chosen path is used for the data transmission that is followed with the trust and energy update. The energy and trust of the individual nodes are updated at the end of the individual transmission in such a way that the secure node selection using the fit factor is continued for the next round. Figure 1 shows the block diagram of the multi-cast routing using the developed optimization. The environment consists of nIoT mobile nodes that are engaged in collecting and forwarding the data to the destination.

Mobility model of WSN The nodes mobility [35] describes the position, velocity, and acceleration of nodes in the environment. The performance of the routing protocol is analyzed with the mobility model that depends on the distance. Let us assume two nodes N_i and N_j placed at (u_i, v_i) and (u_j, v_j) such that $\Omega^i \in (u_i, v_i)$ and $\Omega^j \in (u_j, v_j)$. N_i and N_k traverse in a particular direction through variable velocity with an angle θ_1 and θ_2. The nodes N_i and N_k travel a distance ∂_1 and ∂_2, and after moving a particular distance, the nodes attain a new position (u_i^{new}, v_i^{new}) and (u_j^{new}, v_j^{new}), respectively. Initially, the Euclidean distance

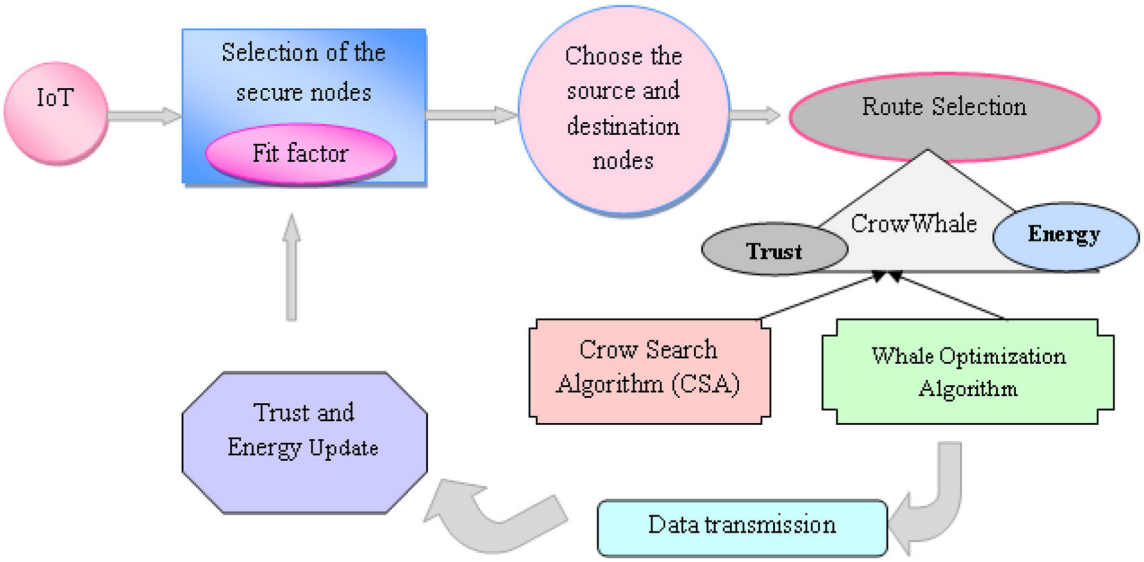

Fig. 1 Multicast routing using CrowWhale optimization

of the nodes at positions $N_i\,(u_i, v_i)$ and $N_j\,(u_j,\ v_j)$ is given as,

$$\partial_{(uv,0)} = \sqrt{\left|u_i - u_j\right|^2 + \left|v_i - v_j\right|^2} \tag{1}$$

The velocity of the nodes N_i and N_k is v_{N_i} and v_{N_j} making an angle θ_1 and θ_2 to travel the distances ∂_1 and ∂_2 that is represented as,

$$\partial_1 = v_{N_i} \times t \tag{2}$$

$$\partial_2 = v_{N_j} \times t \tag{3}$$

At t, the node acquire a new position, which is given by,

$$u_i^{t+1} = u_i^t + v_{N_i} \times t \times \cos\,\theta \tag{4}$$

$$v_i^{new} = v_i^{old} + \vartheta_{N_i} \times t \times \cos\,\varphi \tag{5}$$

When the node $N_k\,(u_k,\ v_k)$ travel a distance ∂_2 making an angle θ_2, the node N_j acquire a new position as given as,

$$u_j^{t+1} = u_j^t + v_{N_j} \times t \times \cos\,\theta \tag{6}$$

$$u_j^{t+1} = u_j^t + v_{N_j} \times t \times \cos\,\theta \tag{7}$$

After the nodes attain a new position, the distance between the nodes is computed as given by,

$$\partial_{(u^{t+1}\,v^{t+1},\,t)} = \sqrt{\left|u_i^{t+1} - u_j^{t+1}\right|^2 + \left|v_i^{t+1} - v_j^{t+1}\right|^2} \tag{8}$$

3.1 Computation of the fit factor to select the secure nodes

The fit factor is the significant factor to choose the secure nodes in order to progress the secure communication in the network, which improves the data confidentiality and integrity. The fit factor is formulated based on the trust and the energy of the individual nodes in the network and the node with the maximal trust and energy is chosen to be the secure node. The fit factor is computed as,

$$Fit_{ij} = D = \frac{1}{2} \times \left[\varepsilon_i + \frac{1}{N} \times \sum_{\substack{j=1 \\ i \in j}}^{N} T_{ij}\right] \tag{9}$$

where N refers to the total number of the neighbors, ε_i is the energy of the ith node in the IoT network, and T_{ij} specifies the trust factor of the jth neighbor of the ith node. The genuine nodes from the IoT network are chosen based on the trust and energy of the nodes, which are then subjected to the route selection phase using the proposed optimization.

3.1.1 Calculation of trust

The trust [36] and energy model [37] of the IoT nodes are computed as follows:

$$T_{ij} = T_{i,j}^{direct} + T_{i,j}^{indirect} + T_{i,j}^{recent} + T_{i,j}^{bytes} \tag{10}$$

The trust used for the evaluation of the node trust is direct trust $T_{i,j}^{direct}$, indirect trust $T_{i,j}^{indirect}$, recent trust $T_{i,j}^{recent}$, and trust-based on the number of bytes transmitted $T_{i,j}^{bytes}$. Initially, whenever the transmission initializes in the nodes, the trust is set to a maximum of one and the trust factors include:

3.1.2 Direct trust

The direct trust [36] depends on the deviation in the actual and estimated time and this computation is based on the witness factor, which contributes much for the enhancement of the nodal trust. The witness factor is based on the ith node, which accepts the public key and the sth sink node in IoT, which authenticates with the node rendering the public key. Therefore, the trust value is based on the approximate time of the nodes and the direct trust is formulated as,

$$T_{i,j}^{direct}(t) = \frac{1}{3}\left[T_{i,j}^{direct}(t-1) - \left[\frac{T^{key} - E^{key}}{T^{key}}\right] + \omega\right] \tag{11}$$

where T^{key} specifies the appropriate time required to send the key, E^{key} signifies the expected time for receiving the key, and ω refers to the witness factor of jth destination.

3.1.3 Indirect trust

The indirect trust [36] is significant whenever a node receives the public key for authentication with any other node that does not hold a witness value. Thus, the indirect trust specifies the trust worthiness of the nodes and the formula for calculating the indirect trust of the nodes is given as,

$$T_{i,j}^{indirect}(t) = \frac{1}{N}\sum_{i=1}^{N} T_{i,x}^{indirect}(x) \tag{12}$$

where N indicates the total neighbor nodes in the ith node.

3.1.4 Recent trust

The recent trust [21] is computed as the node regression of indirect and direct trust of the nodes in the network, the key authenticity, and the acknowledgment belonging to the sink node, which is the function of the time. The recent trust is formulated as,

$$T_{i,j}^{recent}(t) = \alpha * T_{i,j}^{direct}(t) + (1-\alpha) \times T_{i,j}^{indirect}(t) \tag{13}$$

where $\alpha = 0.3$.

3.1.5 Trust based on the data bytes

The robustness of the routing is enhanced through the inclusion of the trust factor that is based on the data bytes, which is based on the total number of the data bytes send from the source node to the total number of the data bytes received through the destination node. The trust factor based on the data bytes is given as,

$$T_{i,j}^{\partial} = \frac{1}{2} \times \left[\frac{\partial_{i,j}^{i}}{d} + \frac{\partial_{i,j}^{j}}{d}\right] \tag{12}$$

where $\partial_{i,j}^{i}$ specifies the data bytes forwarded using the source node and $\partial_{i,j}^{j}$ denotes the bytes received in the destination node. The data packet limit for sending and receiving the data is represented as, d.

3.1.6 Energy model of the network

The sensors in IoT are fully battery-operated and hence, energy of the nodes is the major constraint, which needs to be controlled as it is essential for extending the life-time of the IoT network. Let us assume that the energy [38] in the node at the beginning of the communication is, ε_0. During communication, when the receiver receives the transmitted data there is energy-loss, which duly depends on the distance of transmission and the nature of the node, which can be any of the cluster head or the nodes present in the particular cluster. The transmission depends on the routing protocol and the dissipation in the energy is as a result of the usage of the radio electronics and power amplifier in the transmitter. While transmitting the data packet, the energy dissipation occurs in the node that is based on the following equation,

$$\begin{aligned}\varepsilon_{dis}(K_i) = {} & \varepsilon_{elec} \times \ell_i + \varepsilon_{pa} \times \ell_i \\ & \times \left\|K_i - H_j\right\|^4; if \ \left\|K_i - H_j\right\| \geq \beta_0\end{aligned} \tag{14}$$

where ε_{elec} is the electronic energy, $\varepsilon_{dis}(N_i)$ specifies the energy dissipation of ith node. The number of bytes send by ith node is denoted as, ℓ_i and ε_{pa} is the energy of power amplifier available in the transmitter. The energy dissipation is based on a parameter β_0 such that the distance between the ith sensor node and jth head is computed and compared with β_0. Whenever the distance between node K_i and its corresponding H_j lies below β_0, the energy dissipation in the normal sensor node is based on Eq. (14) or otherwise, the energy dissipation of K_i is computed based on Eq. (15).

$$\begin{aligned}\varepsilon_{dis}(K_i) = {} & \varepsilon_{elec} \times \ell_i + \varepsilon_{fs} \times \ell_i \times \left\|K_i - H_j\right\|^2; \\ & if \ \left\|K_i - H_j\right\| < \beta_0\end{aligned} \tag{15}$$

$$L_{D_0} = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{pa}}} \tag{16}$$

where ε_{fs} is the free space energy. The electrical energy is based on the modulation, filtering, coding, and so on, associated with the transmitter and data aggregation that is given as,

$$\varepsilon_{elec} = \varepsilon_{tx} + \varepsilon_{agg} \tag{17}$$

where ε_{tx} specifies the transmitter energy and ε_{agg} signifies

the energy of data aggregation. $\|K_i - H_j\|$ is the distance between the ith node and jth cluster head. When the normal node K_i tries to communicate with H_j, there is a loss in the energy at the cluster head based on the electrical energy at the receiver side and the data bytes received by the cluster head. The energy dissipation at the jth cluster head is given as,

$$\varepsilon_{dis}(H_j) = \varepsilon_{elec} \times \ell_i \tag{18}$$

Once the data transmission and reception ends, all the sensor nodes and the cluster heads are updated based on the energy of the nodes and dissipated energy of the nodes, given as,

$$\varepsilon_{t+1}(K_i) = \varepsilon_t(K_i) - \varepsilon_{dis}(K_i) \tag{19}$$

$$\varepsilon_{t+1}(H_i) = \varepsilon_t(H_i) - \varepsilon_{dis}(H_i) \tag{20}$$

where (H_j) is the energy dissipation of the cluster head or the receiver during the transfer of the data packets by the normal node. The energy update of the nodes continues until the node becomes dead or in other words, when the energy of the nodes becomes zero.

3.2 Generation and selection of the optimal routes based on the proposed CrowWhale-ETR protocol

Once the genuine nodes are chosen from the IoT network, the source and the destination nodes are fixed for the random generation of the routing paths for which the proposed CrowWhale ETR is employed. The randomly generated routes are selected optimally using the optimization algorithm, CrowWhale optimization, which follows the optimization steps of CSA. The optimization follows the objective function that is based on the fit factor of the IoT nodes in the network. The section discusses the optimal route selection steps of the proposed algorithm.

3.2.1 Solution encoding

The solution encoding is the representation of the solution signifying the nodes involved in the routing. Since it is the multicast routing, the source is the same and there are multiple destinations, which refers to data forwarding from a source to the multiple destinations through the intermediate nodes. The dimension of the solution vector is given as, $(m \times k)$, where, m specifies the multicast destinations and k indicates the maximal number of the intermediate nodes. Figure 2 shows the solution vector. Let us suppose that there are ten genuine nodes of IoT network engaged in communication and from Fig. 2, it is evident that the node '5' acts as the source node and there are three destinations, '4', '8', and '9'.

The solution vector is demonstrated clearly as in Fig. 3, which is the clear picture of the multi-cast routing among the genuine nodes, determined using the fit factor.

3.2.2 Objective function

The objective is evaluated based on the fit factor of the nodes, which utilizes the trust and the energy of the nodes. The objective function is given as,

$$O = \sum_{i=1}^{b} \sum_{j=1}^{|b_i|} Fit_{ij} \tag{21}$$

where b refers to the total destinations and $|b_i|$ signifies the number of the intermediate nodes in the destination paths. The randomly generated paths that contribute to the maximal value of the fitness are chosen as the optimal path based on the proposed optimization algorithm.

3.2.3 Optimization steps to select the optimal routes for progressing the multicast routing in IoT

The optimal routes to progress the multicast routing are determined using the proposed optimization, CrowWhale, which is the modification of the CSA [2] with the WOA [33]. The proposed CrowWhale optimization follows the optimization steps of CSA with the modified equation. The advantages of CSA are that there is a proper balance between the intensification and diversification that is controlled using the parameter, awareness probability A. The decrease in A often leads to the local search to determine the current solution, which often results in intensification and increasing values of A causes the global search for the solution resulting in exploration. The higher values of A causes the diversification phase of the Whales. Moreover, the convergence of CSA is found to be better and is reported to be around 1 s. However, fine tuning of the optimal parameter is essential in order to switch between the intensification and diversification phases, and it is noted that CSA is effective for both the unimodal and multimodal functions, but based on the control parameter, A. In case of the ineffective parameter tuning, it results in the local optimal convergence. Therefore, WOA is integrated with the CSA that exhibited adaptive nature and finally, results in the global optimal convergence. There is a simultaneous balance in the local optimal avoidance and convergence speed is high during the course of the iterations. The benefit of CSA is that the algorithm is simple and requires less computational cost.

CSA is based on the social behaviour of the Crows, which is meant for the intelligent behaviour and the tool-making ability. Crows hide their food and observe the other neighbors to find their hiding place, and steal the food of

others. Generally speaking, Crows live in flocks, memorize the hiding position of the Crows, and pilfer the caches based on a specific probability. Let us assume that there are q number of Crows in the search space and their positions are denoted as, Z^l; $(1 \le l \le q)$. The q Crows are positions randomly in the a dimensional space and the individual position of the Crow specifies the feasible solution. The solution matrix is denoted as,

$$Z = \begin{bmatrix} Z_1^1 & Z_2^1 & \dots & Z_a^1 \\ Z_1^2 & Z_2^2 & \dots & Z_a^2 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ Z_1^q & Z_2^q & \dots & Z_a^q \end{bmatrix} \tag{22}$$

The Crow update their position based on the memory or hiding place of the Crow, which is represented as,

$$M = \begin{bmatrix} M_1^1 & M_2^1 & \dots & M_a^1 \\ M_1^2 & M_2^2 & \dots & M_a^2 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ M_1^q & M_2^q & \dots & M_a^q \end{bmatrix} \tag{23}$$

The position update follows two rules given as,

(1) Crow κ is unaware that Crow l is following while in search of the hidden place of Crow κ and hence, the update equation is given as,

$$Z^{l,\tau+1} = Z^{l,\tau} + R_1 \times L^{l,\tau} \times \left(M^{\kappa,\tau} - Z^{l,\tau}\right) \tag{24}$$

Rearranging the above equation, we get,

$$Z^{l,\tau+1} = Z^{l,\tau} + R_1 \times L^{l,\tau} \times M^{\kappa,\tau} - R_1 \times L^{l,\tau} \times Z^{l,\tau} \tag{25}$$

$$Z^{l,\tau+1} = Z^{l,\tau} \times \left(1 - R_1 \times L^{l,\tau}\right) + R_1 \times L^{l,\tau} \times M^{\kappa,\tau} \tag{26}$$

where $Z^{l,\tau+1}$ refers to the position of the lth Crow in time $(\tau+1)$. R_1 refers to the random number that varies between 0 and 1, $M^{\kappa,\tau}$ signifies the position of the hiding place of kth Crow, $L^{l,\tau}$ indicates the flight length of the lth Crow, and $Z^{l,\tau}$ denotes the position of the lth Crow at time τ. The significance of the flight length $L^{l,\tau}$ is that the lower values of $L^{l,\tau}$ causes local search and greater values of $L^{l,\tau}$ leads to the global search. The standard update Eq. (26) of CSA is modified with the update equation of the WOA and the standard equation of WOA is given as,

$$Z^{l,\tau+1} = M^{\kappa,\tau} - \vec{P} \cdot \vec{V}; \quad \text{if } \rho < 0.5 \tag{27}$$

where ρ is the random probability that decides the switching between the exploitation and exploration phases, and $M^{\kappa,\tau}$ specify the best position of the Whale. The distance vector is represented as, $\vec{V}$ that is given as,

$$\vec{V} = \left|\vec{G} \cdot M^{\kappa,\tau} - Z^{l,\tau}\right| \tag{28}$$

The vectors, $\vec{P}$ and $\vec{G}$ are the coefficient vectors that are calculated as,

$$\vec{P} = 2 \cdot \vec{p} \cdot \vec{r} - \vec{p} \tag{29}$$

$$\vec{G} = 2 \cdot \vec{r} \tag{30}$$

The values of $\vec{p}$ is decreased from 2 to 0 during the course of the iteration and $\vec{r}$ be the random number between 0 and 1. Substitute the Eq. (28) in the Eq. (27), we get,

$$Z^{l,\tau+1} = M^{\kappa,\tau} - \vec{P} \cdot \left(\vec{G} \cdot M^{\kappa,\tau} - Z^{l,\tau}\right) \tag{31}$$

$$Z^{l,\tau+1} = M^{\kappa,\tau} - \vec{P} \,.\, \vec{G} \,.M^{\kappa,\tau} + \vec{P} \,.Z^{l,\tau} \tag{32}$$

$$\vec{P} \cdot Z^{l,\tau} = Z^{l,\tau+1} + \vec{P} \cdot \vec{G} \cdot M^{\kappa,\tau} - M^{\kappa,\tau} \tag{33}$$

$$Z^{l,\tau} = \frac{1}{\vec{P}}\left[Z^{l,\tau+1} + \vec{P} \cdot \vec{G} \cdot M^{\kappa,\tau} - M^{\kappa,\tau}\right] \tag{34}$$

The above equation is used to modify the Eq. (26) of CSA, which becomes the update equation of CrowWhale optimization. The update equations of CrowWhale is given as,

$$\begin{aligned} Z^{l,\tau+1} = {} & \frac{1}{\vec{P}}\left[Z^{l,\tau+1} + \vec{P} \cdot \vec{G} \cdot M^{\kappa,\tau} - M^{\kappa,\tau}\right] \\ & \times \left(1 - R_1 \times L^{l,\tau}\right) + R_1 \times L^{l,\tau} \times M^{\kappa,\tau} \end{aligned} \tag{35}$$

$$\begin{aligned} & Z^{l,\tau+1} - \frac{\left(1 - R_1 \times L^{l,\tau}\right)}{\vec{P}} \times Z^{l,\tau+1} \\ & = \frac{1}{\vec{P}}\left[\vec{P} \cdot \vec{G} \cdot M^{\kappa,\tau} - M^{\kappa,\tau}\right] \times \left(1 - R_1 \times L^{l,\tau}\right) \\ & \quad + R_1 \times L^{l,\tau} \times M^{\kappa,\tau} \end{aligned} \tag{36}$$

$$\begin{aligned} & Z^{l,\tau+1} \times \left[1 - \frac{\left(1 - R_1 \times L^{l,\tau}\right)}{\vec{P}}\right] \\ & = R_1 \times L^{l,\tau} \times M^{\kappa,\tau} + \frac{1}{\vec{P}}\left[\vec{P} \cdot \vec{G} \cdot M^{\kappa,\tau} - M^{\kappa,\tau}\right] \\ & \quad \times \left(1 - R_1 \times L^{l,\tau}\right) \end{aligned} \tag{37}$$

$$\begin{aligned} Z^{l,\tau+1} = {} & \frac{\vec{P}}{\vec{P} - 1 - R_1 \times L^{l,\tau}}\left\{R_1 \times L^{l,\tau} \times M^{\kappa,\tau}\right. \\ & \left. + \frac{\left(1 - R_1 \times L^{l,\tau}\right)}{\vec{P}}\left[\vec{P} \cdot \vec{G} \cdot M^{\kappa,\tau} - M^{\kappa,\tau}\right]\right\} \end{aligned} \tag{38}$$

(2) The Crow κ knows that the other Crow l follows it and hence, κth Crow fools the other Crow l through moving to the other position. Thus, the position of the Crow is updated randomly.

Upon updating the position of the Crow, the feasibility of the Crow is verified that is based on the objective

function, which is shown as in Eq. (21). The feasibility of the Crow is verified as follows:

$$M^{\kappa,\tau+1} = \begin{cases} Z^{l,\tau+1}; & fit\left(Z^{l,\tau+1}\right) > fit\left(M^{\kappa,\tau}\right) \\ M^{\kappa,\tau}; & Otherwise \end{cases} \tag{39}$$

where $fit\left(Z^{l,\tau+1}\right)$ refers to the fitness of the solution at time $(\tau+1)$ and $fit\left(M^{\kappa,\tau}\right)$ indicates the fitness of the best position. Whenever the fitness of the new solution is better compared with the best solution, the new solution is accepted or otherwise, the Crow stays in the previous position. The solutions are repeated for the maximal number of the iterations and the best solution is derived. The best solution represents the multicast routes to enable routing in the IoT environment. The pseudo code of the proposed algorithm is deliberated in Algorithm 1.

Algorithm 1: CrowWhale Optimization

Input : Random solution Z^{l}; $\left(1 \le l \le q\right)$

Output : Optimal solution, $M^{\kappa,\tau+1}$ [Multicast routes]

Begin

Random Initialization

Position of crow $Z = \begin{bmatrix} Z_1^1 & Z_2^1 & \ldots\ldots\ldots & Z_a^1 \\ Z_1^2 & Z_2^2 & \ldots\ldots\ldots.. & Z_a^2 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ Z_1^q & Z_2^q & \ldots\ldots\ldots.. & Z_a^q \end{bmatrix}$

Memory of crow $M = \begin{bmatrix} M_1^1 & M_2^1 & \ldots\ldots\ldots & M_a^1 \\ M_1^2 & M_2^2 & \ldots\ldots\ldots.. & M_a^2 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ M_1^q & M_2^q & \ldots\ldots\ldots.. & M_a^q \end{bmatrix}$

While $\left(\tau < \tau_{max}\right)$

For $l = 1 to\ q$

Randomly choose crow l

Fix the awareness probability A

If $R_\kappa \ge A^{\kappa,\tau}$

Update the position using equation (38)

$$Z^{l,\tau+1} = \frac{\vec{P}}{\vec{P} - 1 - R_1 \times L^{l,\tau}} \left\{ R_1 \times L^{l,\tau} \times M^{\kappa,\tau} + \frac{\left(1 - R_1 \times L^{l,\tau}\right)}{\vec{P}} \left[\vec{P}.\vec{G}.M^{\kappa,\tau} - M^{\kappa,\tau} \right] \right\}$$

Else

$Z^{l,\tau+1}$, Random search

Endif

EndFor

Evaluate the feasibility of the solutions

Check the new position of crow

Update the crows' memory

End While

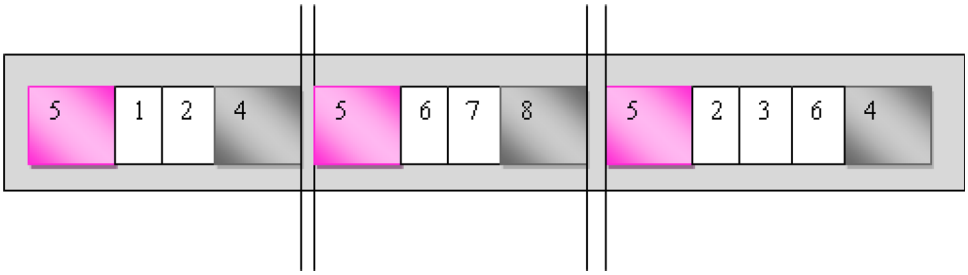

Fig. 2 Solution vector

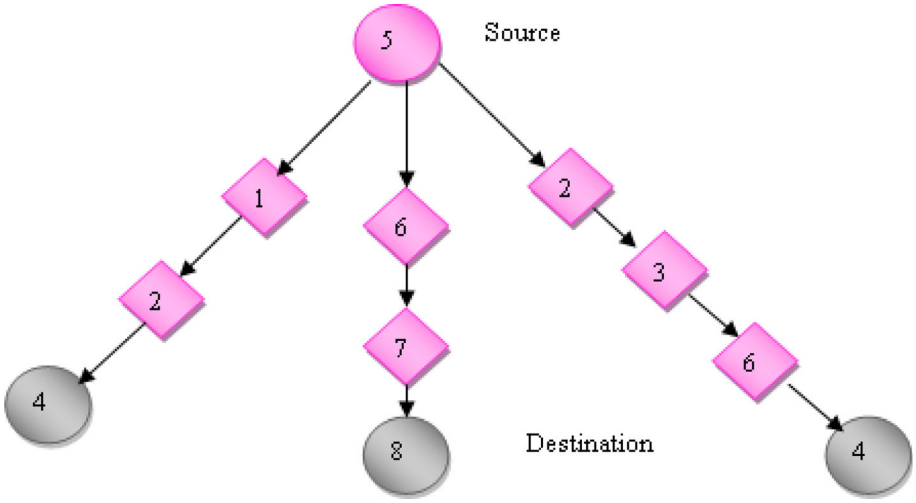

Fig. 3 Schematic diagram of the multicast routing

4 Results and discussion

The section deliberates the experimental analysis and discussion of the IoTs based on the proposed multicast routing algorithm. The evaluation of the results is deeply elaborated in this section.

4.1 Experimental setup

The experiment is analyzed in MATLAB and the simulation is developed with 50 and 100 nodes for analysis in the presence or absence of the node attacks. Two types of attacks are considered in the paper, which includes the black-hole attack and DDOS attack.

4.2 Simulation results

The analysis with 50 and 100 nodes are demonstrated in this section and Fig. 4 shows the simulation results. The analysis with the 50 nodes and 100 nodes are demonstrated in Fig. 4a, b, respectively. The attacker is detected effectively using the proposed protocol and the attacker is indicated with a red round in the simulation environment.

4.3 Performance metrics

The metrics employed for the analysis include: delay, detection rate, energy, and throughput of the network. The network energy refers to the energy remaining in the nodes after the end of the transmission and it should be a maximum value in order to extend the lifetime of the network. The throughput of the network is the total data rates transmitted over the network within a particular time and delay refers to the time taken for the transmission of the data. The detection rate refers to the accurate detection of the attacker and delay refers to the time taken for data transmission among the IoT nodes in the network. The effective method contributes with the maximal energy, throughput, and detection rate, but with minimal delay.

4.4 Comparative methods

The performance of the proposed protocol is compared with existing methods, like A FAST + FAMOUS [3], QMRPRNS [35], GMR [39], CSA [2], and WOA [33] in terms of throughput, delay, and energy.

4.5 Comparative analysis

The section enumerates the comparative analysis of the methods based on the performance metrics in the presence of two types of attacks, type-1 attack and type-2. The type-1 attack refers to the black hole attack and type-2 attack refers to the DDoS attack. The analysis is discussed with 50 nodes and 100 nodes in the simulation environment as shown below.

4.5.1 Using 50 nodes in the presence of type-1 attack

In the section, the analysis is progressed with 50 nodes in the presence of the type-1 attack. Figure 5 shows the analysis based on the performance metrics and Fig. 5a depicts the analysis based on delay. In the beginning of the rounds, there is no delay and with the increase in time, the delay increases. However, from the figure it is clear that the delay of the proposed method attained a minimal delay when compared with the existing methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR. The delay of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR is 0.473, 0.5815, 0.4706, 0.5583, 0.5273, and 0.3145, respectively when the time is 20 s. The analysis based on the detection rate is pictured in Fig. 5b. The effective method should afford with the maximal value of the detection rate, which ensures effective detection of the attacks. From the figure, on easily finalize that the detection rate decreases with time, still the detection rate of the proposed method is found to be high for the proposed method. At the beginning of routing, the detection rate is maximal for the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR, which reduces upon decreases with increasing time. The detection rate at 19 s is found to be 0.6988, 0.6988, 0.6988, 0.7275, 0.7273, and 0.7203, respectively for the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR, respectively. Figure 5c shows the energy of the methods with respect to time. The energy remained in the nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR are 61.5298, 60.5792, 59.6383, 59.2503, 55.2248, and 64.5024, respectively at time 20 s. Similarly, the analysis based on the throughput is enumerated in Fig. 5d. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR is 0.2368, 0.1823, 0.046, 0.2845, 0.364, and 0.0578 at 20 s. It is concluded from the analysis that the proposed method acquired the better delay, detection rate, energy, and throughput in the presence of 50 nodes.

4.5.2 Using 50 nodes in the presence of type-2 attack

In the section, the analysis is progressed with 50 nodes in the presence of the type-2 attack. Figure 6 shows the analysis based on the performance metrics and Fig. 6a depicts the analysis based on delay. In the beginning of the rounds, there is no delay and with the increase in time, the delay increases. However, from the figure it is clear that the delay of the proposed method attained a minimal delay when compared with the existing methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR. The delay of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR is 0.5213, 0.4181, 0.5761, 0.5613, 0.5085, and

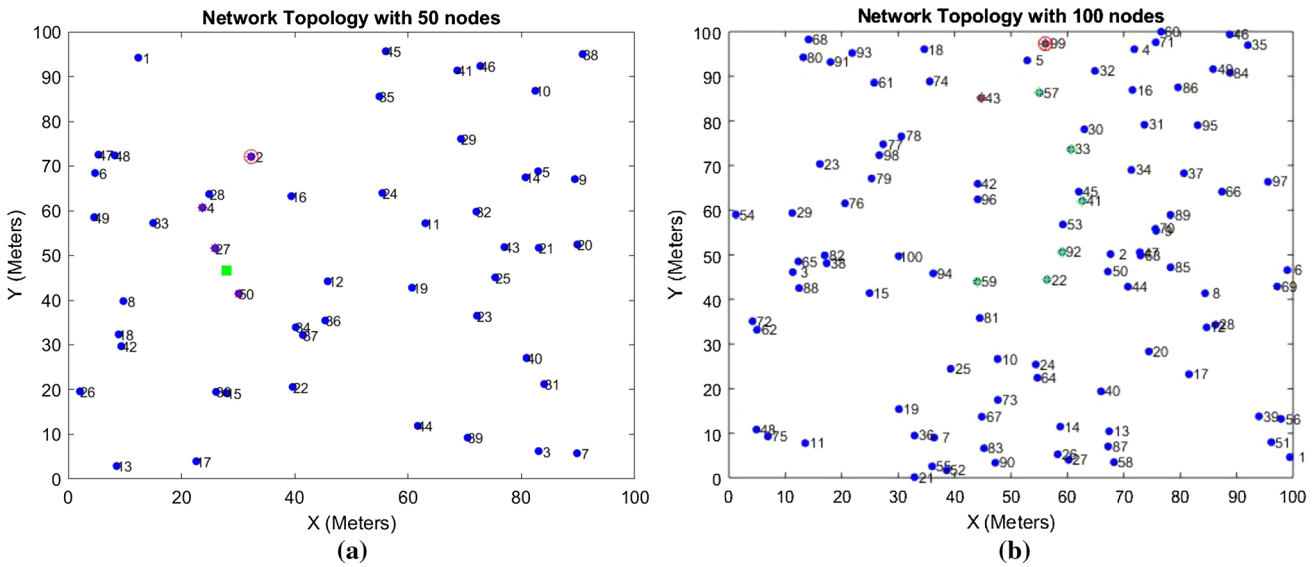

Fig. 4 Simulation results, **a** using 50 nodes and **b** using 100 nodes

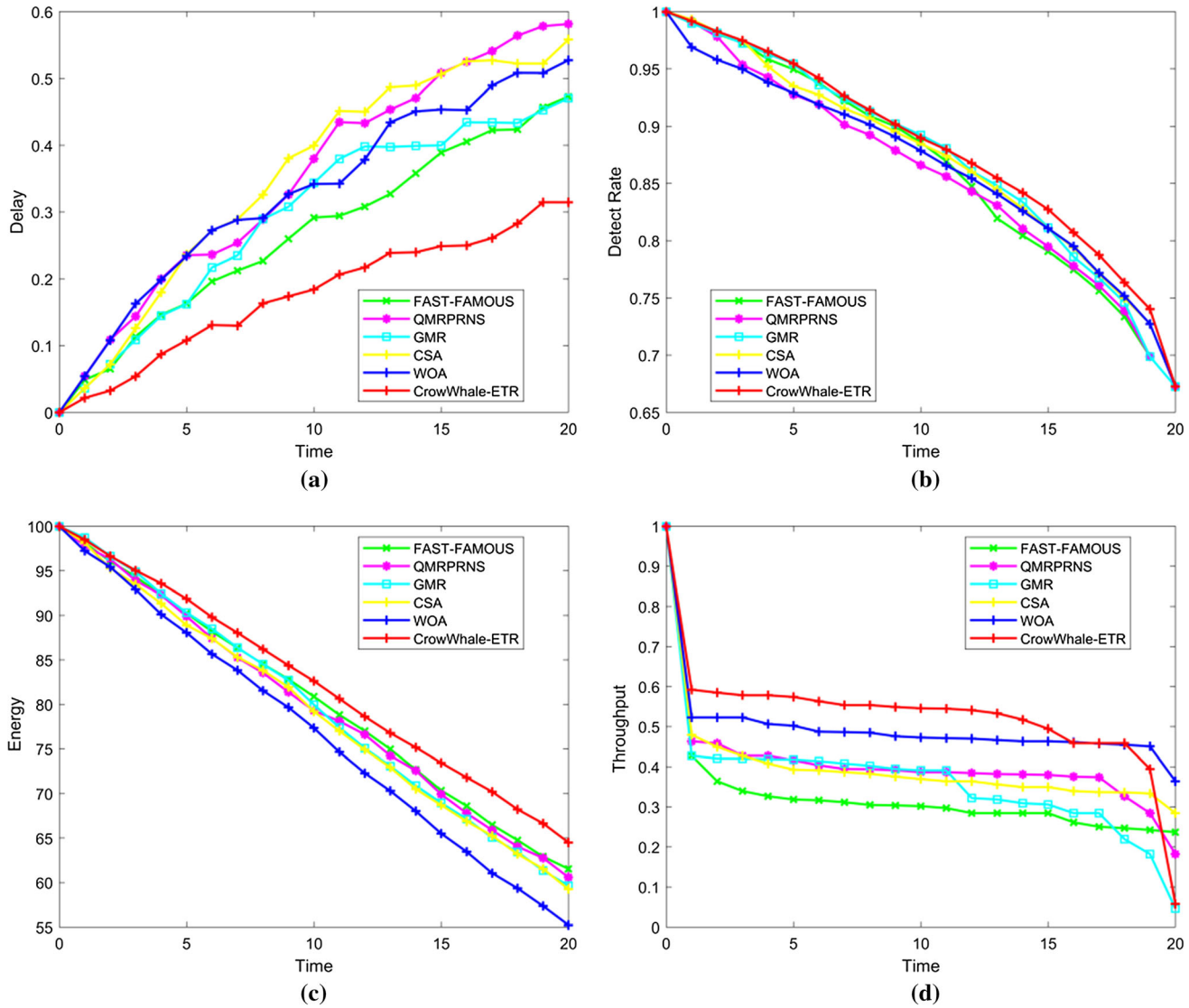

Fig. 5 Comparative analysis using 50 nodes in the presence of type-1 attack, **a** delay, **b** detection rate, **c** energy, and **d** throughput

0.2728, respectively when the time is 20 s. The analysis based on the detection rate is pictured in Fig. 6b. The effective method should afford with the maximal value of the detection rate, which ensures effective detection of the attacks. From the figure, on easily finalize that the detection rate decreases with time, still the detection rate of the proposed method is found to be high for the proposed method. At the beginning of routing, the detection rate is 0.9693, 0.9661, 0.9759, 0.9813, 0.9940, and 0.9765, respectively for the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR at 19 s. Figure 6c shows the energy of the methods with respect to time. The energy remained in the nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR are 64.34, 61.36, 56.75, 62, 61.39, and 66.42, respectively at time 20 s. Similarly, the analysis based on the throughput is enumerated in Fig. 6d. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.3621, 0.1981, 0.3763, 0.2983, 0.0644, and 0.4625 at 19 s. It is concluded from the analysis that the proposed method acquired the better delay, detection rate, energy, and throughput in the presence of 50 nodes.

4.5.3 Using 50 nodes in the absence of attacks

In the section, the analysis is progressed with 50 nodes in the absence of the attacks. Figure 7 shows the analysis based on the performance metrics and Fig. 7a depicts the analysis based on delay. In the beginning of the rounds, there is no delay and with the increase in time, the delay increases. However, from the figure it is clear that the delay

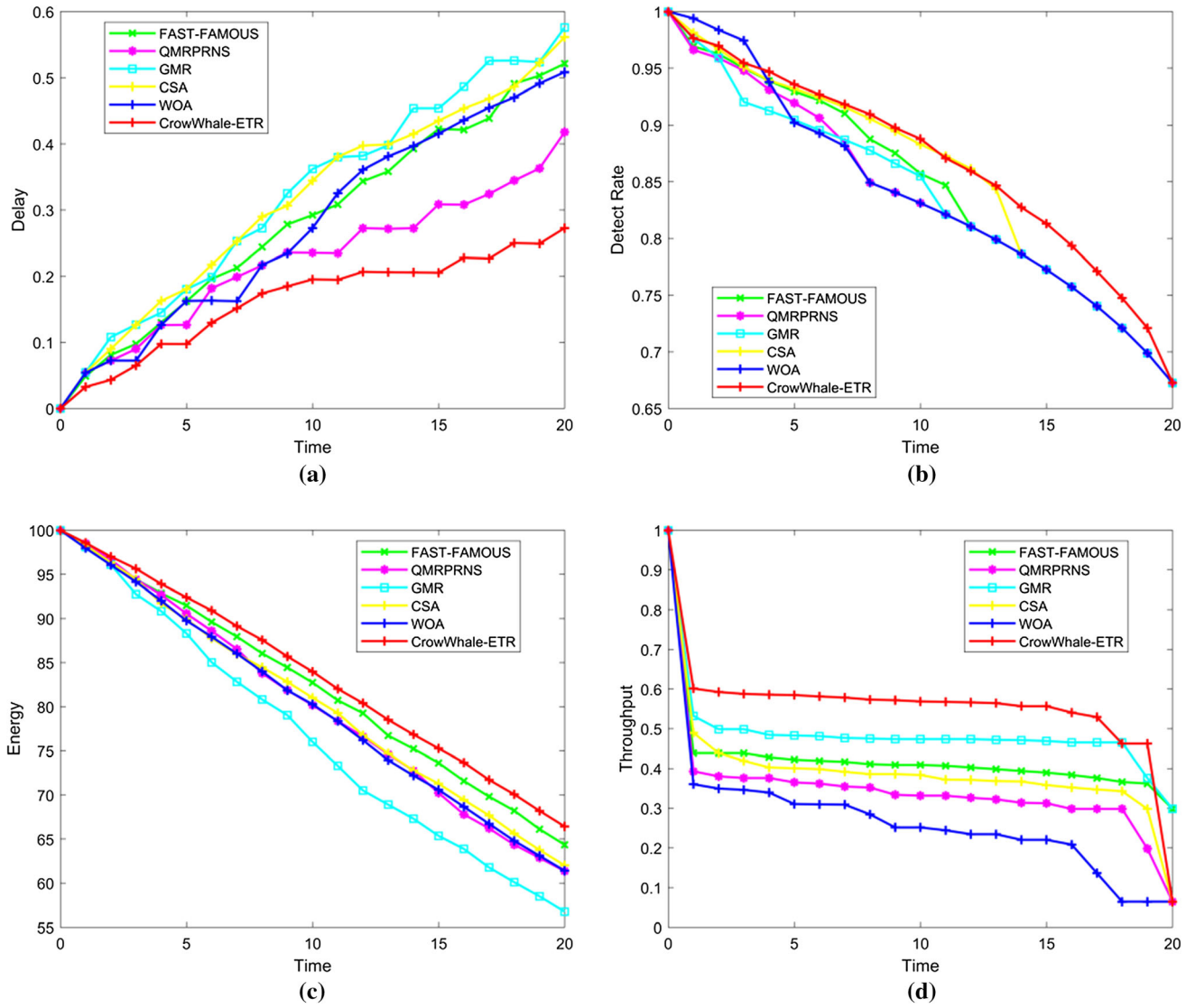

Fig. 6 Comparative analysis using 50 nodes in the presence of type-2 attack, **a** delay, **b** detection rate, **c** energy, and **d** throughput

of the proposed method attained a minimal delay when compared with the existing methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR. The delay of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.4377, 0.5976, 0.5255, 0.5418, 0.5622, and 0.3490, respectively when the time is 20 s. Figure 7b shows the energy of the methods with respect to time. The energy remained in the nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR are 64.11, 64.4689, 63.82, 63.27, 65.94, and 71.05, respectively at time 20 s. Similarly, the analysis based on the throughput is enumerated in Fig. 7c. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.856, 0.8571, 0.8522, 0.8522, 0.844, and 0.8649 at 20 s. It is concluded from the analysis that the proposed method acquired the better delay, detection rate, energy, and throughput in the presence of 50 nodes.

4.5.4 Using 100 nodes in the presence of type-1 attack

In the section, the analysis is progressed with 100 nodes in the presence of the type-1 attack. Figure 8 shows the analysis based on the performance metrics and Fig. 8a depicts the analysis based on delay. In the beginning of the rounds, there is no delay and with the increase in time, the delay increases. However, from the figure it is clear that the delay of the proposed method attained a minimal delay when compared with the existing methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR. The delay of the methods, FAST +

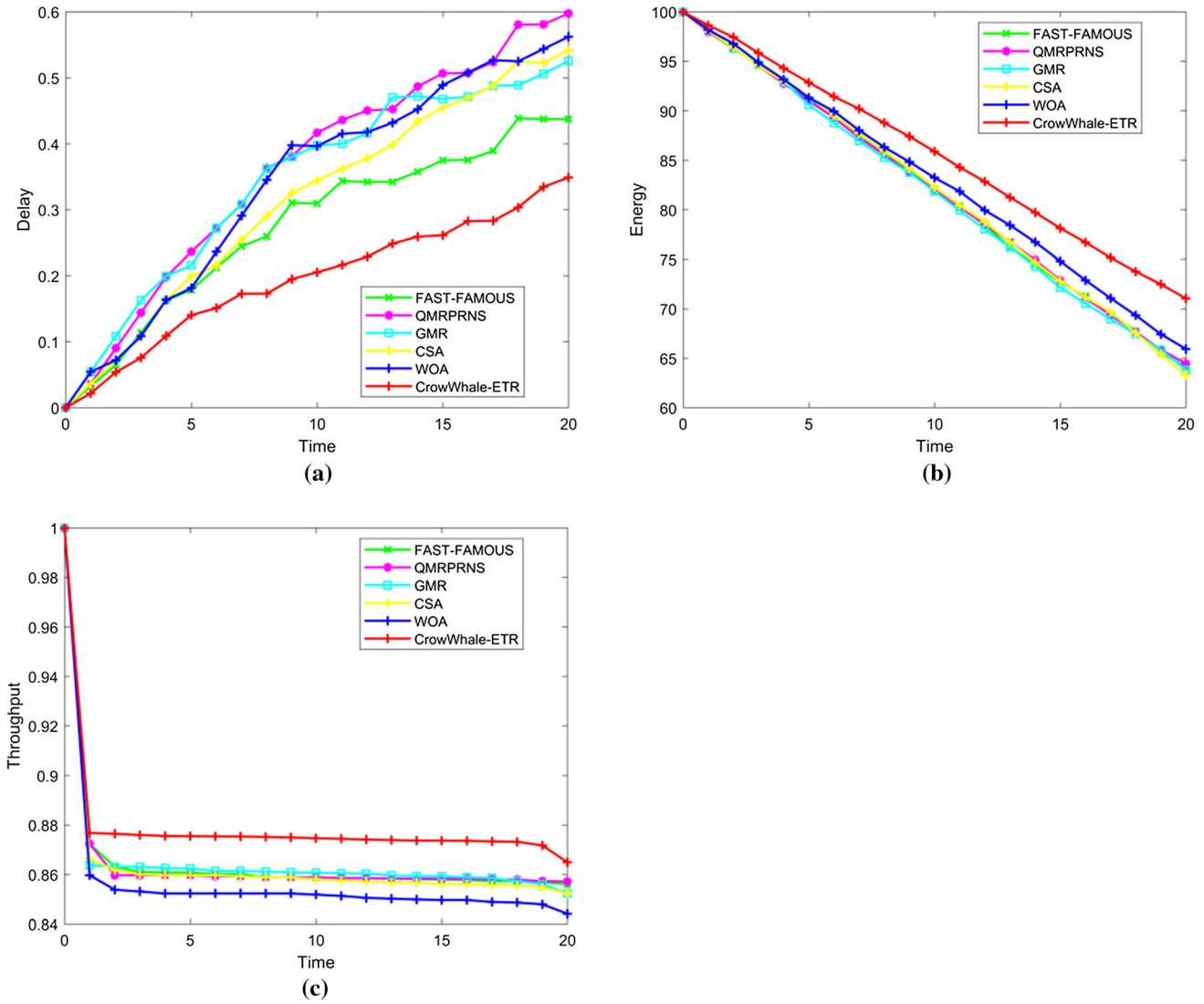

Fig. 7 Comparative analysis using 50 nodes in the absence of attacks, **a** delay, **b** energy, and **c** throughput

FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.2848, 0.3432, 0.3627, 0.3074, 0.3453, and 0.2233, respectively when the time is 20 s. The analysis based on the detection rate is pictured in Fig. 8b. The effective method should afford with the maximal value of the detection rate, which ensures effective detection of the attacks. From the figure, on easily finalize that the detection rate decreases with time, still the detection rate of the proposed method is found to be high for the proposed method. At the beginning of routing, the detection rate is 0.99, 0.9828, 0.9843, 0.9914, 0.9749, and 0.9914, respectively for the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR. The detection rate at 19 s is found to be 0.6988 for the methods, FAST + FAMOUS, QMRPRNS, GMR, and CSA, and 0.7234 and 0.718 for WOA and CrowWhale-ETR, respectively. Figure 8c shows the energy of the methods with respect to time. The energy remained in the nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR are 74.19, 77.25, 77.05, 77.60, 76.01, and 80.60, respectively at time 20 s. Similarly, the analysis based on the throughput is enumerated in Fig. 8d. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.0411, 0.0411, 0.137, 0.0411, 0.2078 and 0.0674 at 19 s. It is concluded from the analysis that the proposed method acquired the better delay, detection rate, energy, and throughput in the presence of 100 nodes.

4.5.5 Using 100 nodes in the presence of type-2 attack

In the section, the analysis is progressed with 100 nodes in the presence of the type-2 attack. Figure 9 shows the analysis based on the performance metrics and Fig. 9a

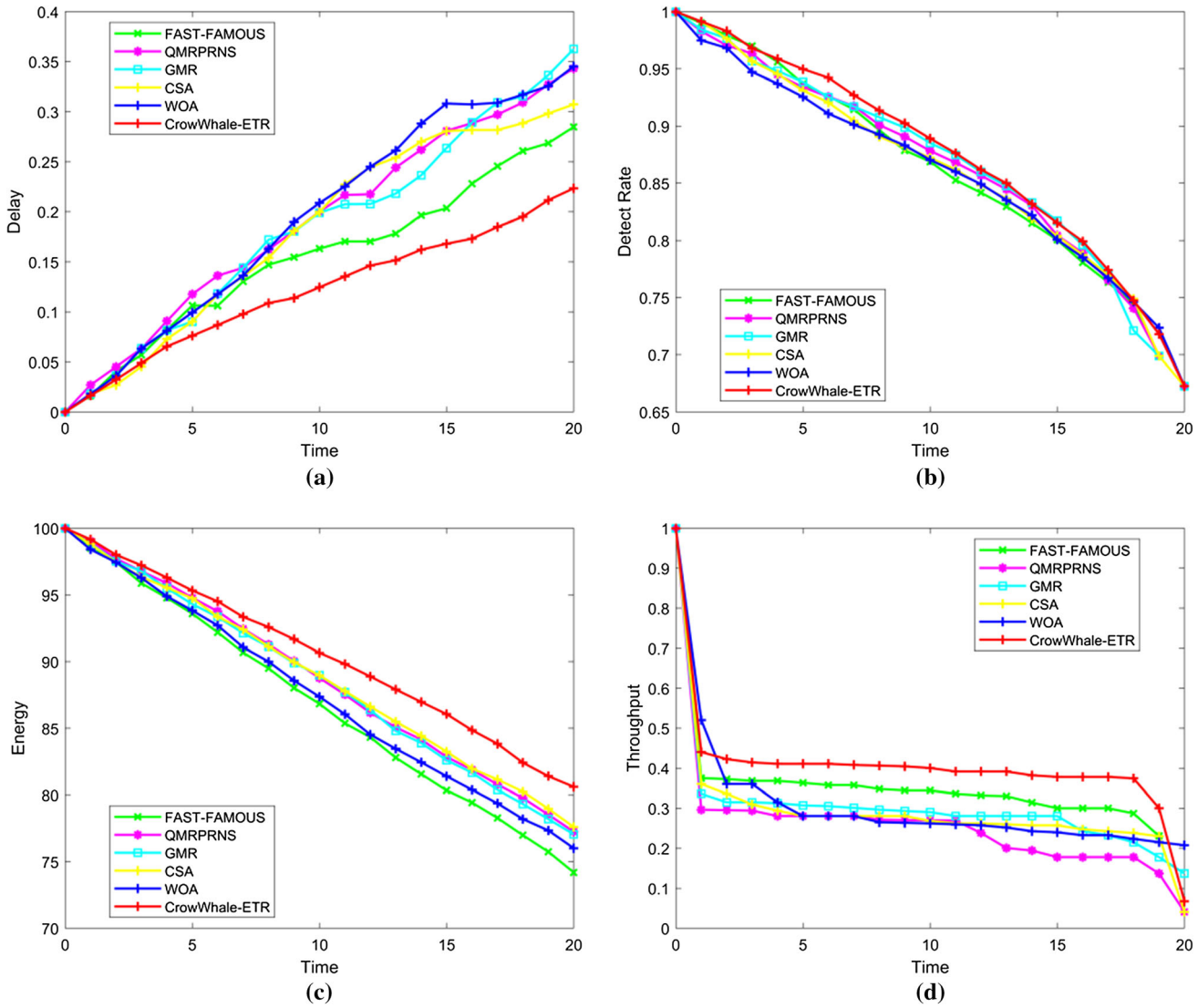

Fig. 8 Comparative analysis using 100 nodes in the presence of type-1 attack, **a** delay, **b** detection rate, **c** energy, and **d** throughput

depicts the analysis based on delay. In the beginning of the rounds, there is no delay and with the increase in time, the delay increases. However, from the figure it is clear that the delay of the proposed method attained a minimal delay when compared with the existing methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR. The delay of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR is 0.2604, 0.3818, 0.3354, 0.3438, 0.315, and 0.2161, respectively when the time is 20 s. The analysis based on the detection rate is pictured in Fig. 9b. The detection rate at 19 s is found to be 0.6988 for the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, and WOA, and 0.7227 for CrowWhale-ETR, respectively. Figure 9c shows the energy of the methods with respect to time. The energy remained in the nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR are 76.8121, 76.4678, 77.47, 77.38, 74.01, and 82.17, respectively at time 20 s. Similarly, the analysis based on the throughput is enumerated in Fig. 9d. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.0644, 0.3396, 0.2345, 0.1364, 0.3173, and 0.3558 at 19 s. It is concluded from the analysis that the proposed method acquired the better delay, detection rate, energy, and throughput in the presence of 100 nodes.

4.5.6 Using 100 nodes in the absence of attacks

In the section, the analysis is progressed with 100 nodes in the absence of the attacks. Figure 10 shows the analysis based on the performance metrics and Fig. 10a depicts the analysis based on delay. In the beginning of the rounds, there is no delay and with the increase in time, the delay

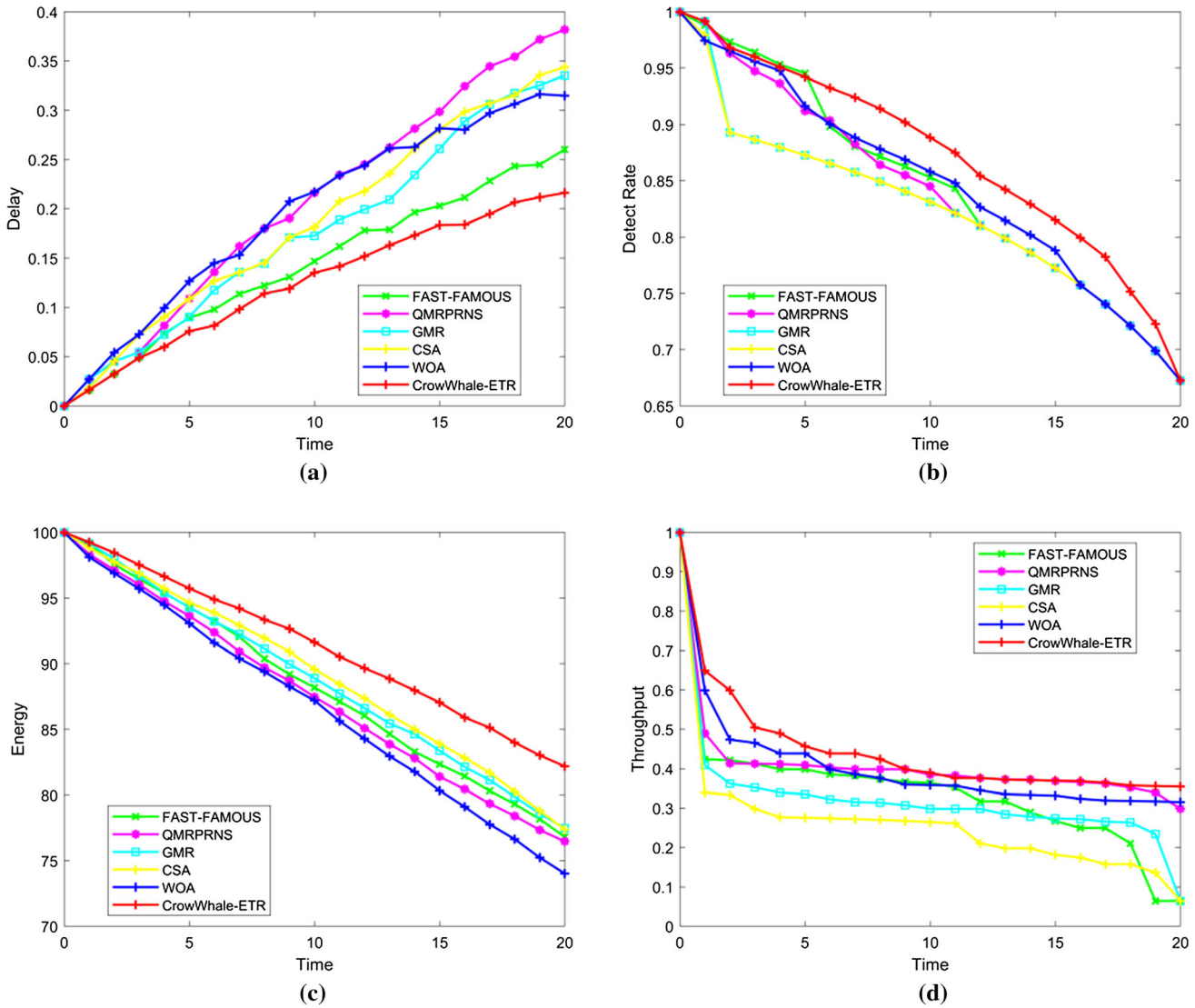

Fig. 9 Comparative analysis using 100 nodes in the presence of type-2 attack, **a** delay, **b** detection rate, **c** energy, and **d** throughput

increases. However, from the figure it is clear that the delay of the proposed method attained a minimal delay when compared with the existing methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR. The delay of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.3029, 0.3263, 0.3628, 0.3350, 0.3456, and 0.1855, respectively when the time is 20 s. Figure 10b shows the energy of the methods with respect to time. The energy remained in the nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and Crow-Whale-ETR are 78.54, 78.98, 78.44, 78.92, 80.47, and 82.53, respectively at time 20 s. Similarly, the analysis based on the throughput is enumerated in Fig. 10c. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.8349, 0.8663, 0.8724, 0.8761, 0.8596, and 0.8917 at 20 s. It is concluded from the analysis that the proposed method acquired the better delay, detection rate, energy, and throughput in the presence of 100 nodes.

4.6 Comparative discussion

The analysis with 50 nodes and 100 nodes are progressed based on the performance metrics as shown in Table 1. The proposed method acquired the minimal delay, maximal energy, maximal detection rate, and maximal throughput. The delay, detection rate, energy, and throughput of the proposed method are 0.2729, 0.6726, 66.4275, and 0.0645 respectively, whereas for the QMRPRNS method, the delay, detection rate, energy, and throughput of the proposed method is 0.4181, 0.6726, 61.361, and 0.0645, respectively using 50 nodes in the simulation environment. The delay, detection rate, energy, and throughput of the

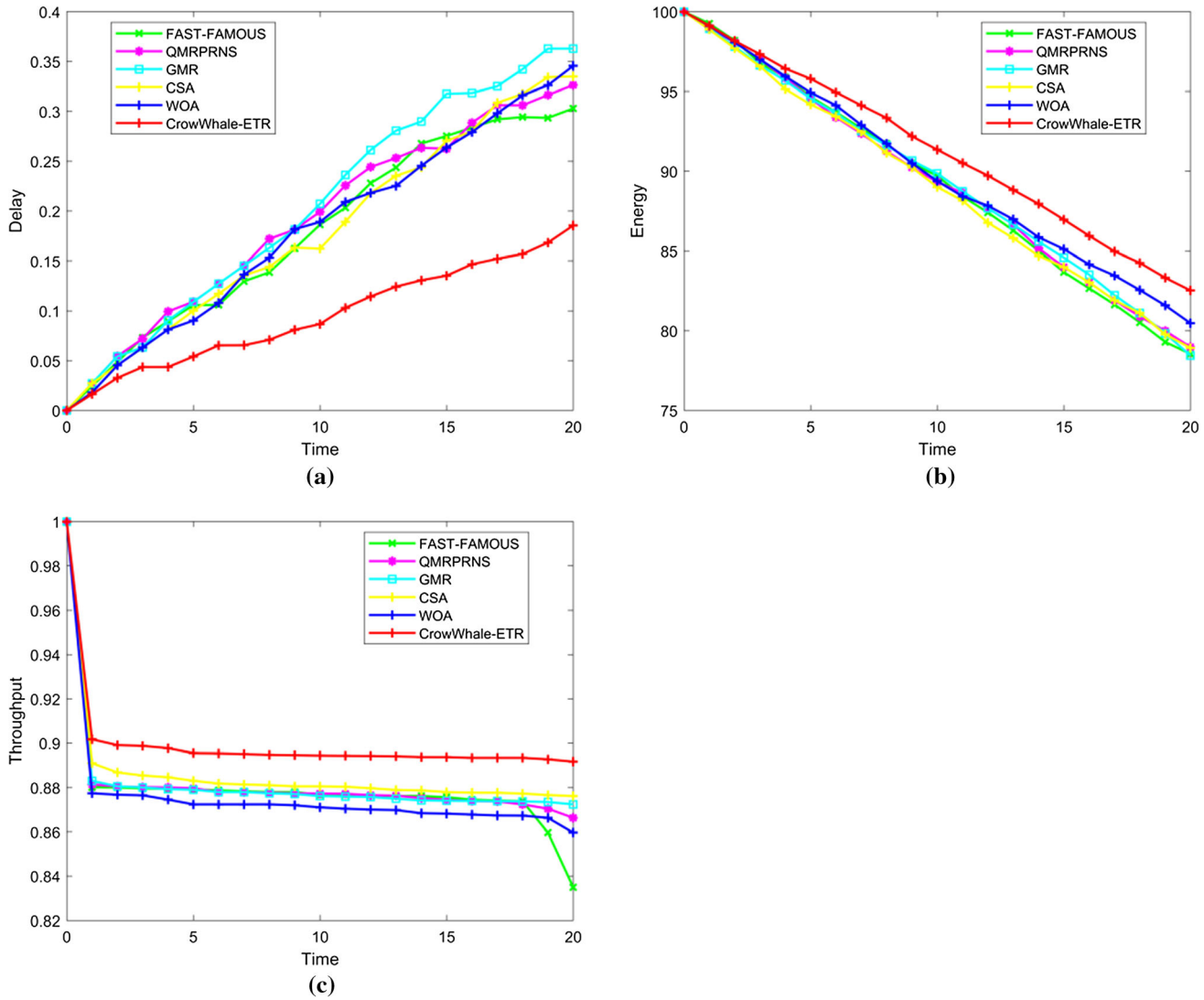

Fig. 10 Comparative analysis using 100 nodes in the absence of attacks, **a** delay, **b** energy, and **c** throughput

proposed method are 0.2162, 0.7228, 82.1774, and 0.3548, respectively using 100 nodes in the simulation environment. Finally, the analysis in the absence of attacks using 50 and 100 nodes is enumerated in Table 2.

The delay of the proposed method in the presence of 50 and 100 nodes are 0.3491and 0.1855, which is less when compared with the comparative methods. The energy of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR using 50 nodes is found to be 64.11, 64.4689, 63.8287, 63.2758, 65.9433, and 71.0567, whereas the energy with 100 nodes using the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 78.544, 78.980, 78.447, 78.927, 80.474, and 82.530. The throughput of the methods, FAST + FAMOUS, QMRPRNS, GMR, CSA, WOA, and CrowWhale-ETR is 0.8349, 0.8664, 0.8724, 0.8762, 0.8597, and 0.8917 in the presence of 100 nodes. The methods are analyzed based on the performance metrics and it is clear that the proposed method acquired the maximal throughput, minimal delay, and maximal energy, both with 50 and 100 nodes. Moreover, the detection capability of the proposed CrowWhale-ETR method was better in the presence of the attacks, DDoS and black hole attacks.

4.7 Analysis based on trade-off

The performance of the proposed system is analyzed using the metrics, such as energy, throughput, and delay, which are interrelated with each other. The trade-off between delay and throughput is that the proposed system has the maximum throughput when the delay is minimum. The trade-off between delay and the energy is that the proposed system has the maximum energy on the minimum delay.

Table 1 Comparative discussion in the presence of attack

Methods	Delay	Detection rate	Energy	Throughput
Analysis using 50 nodes				
FAST + FAMOUS	0.5213	0.6726	64.3481	0.4238
QMRPRNS	0.4181	0.6726	61.361	0.4897
GMR	0.5761	0.6726	56.7595	0.4091
CSA	0.5613	0.6726	62.0086	0.3396
WOA	0.5086	0.6726	61.3996	0.0645
CrowWhale-ETR	0.2729	0.6726	66.4275	0.4625
Analysis using 100 nodes				
FAST + FAMOUS	0.2605	0.6989	76.8122	0.4238
QMRPRNS	0.3819	0.6989	76.4678	0.4897
GMR	0.3354	0.6989	77.4766	0.4091
CSA	0.3438	0.6989	77.3893	0.3396
WOA	0.3150	0.6989	74.0186	0.599
CrowWhale-ETR	0.2162	0.7228	82.1774	0.6491

Table 2 Comparative discussion in the absence of attack

Methods	Delay	Energy	Throughput
Analysis using 50 nodes			
FAST + FAMOUS	0.4378	64.11	0.8561
QMRPRNS	0.5977	64.4689	0.8572
GMR	0.5256	63.8287	0.8523
CSA	0.5419	63.2758	0.8523
WOA	0.5622	65.9433	0.8441
CrowWhale-ETR	0.3491	71.05671	0.8649
Analysis using 100 nodes			
FAST + FAMOUS	0.3030	78.544	0.8349
QMRPRNS	0.3264	78.980	0.8664
GMR	0.3629	78.447	0.8724
CSA	0.3350	78.927	0.8762
WOA	0.3457	80.474	0.8597
CrowWhale-ETR	0.1855	82.530	0.8917

Similarly, when the energy increases the proposed system has the maximum throughput. Overall, the proposed system offers the better performance results with minimum delay, maximum energy and maximum throughput.

5 Conclusion

The energy-aware multicast routing is essential in IoT applications, which is performed using the proposed optimization, CWOA. The optimal selection of the routes for multicast routing is enabled using the objective function depending on the trust and energy factors that chooses the effective nodes for establishing the routes for data transmission. Based on the energy and trust update, the secure nodes are selected and which improves the secure communication from the attacks. The analysis using 50 and 100 nodes in the simulation environment reveals that the proposed method acquired better performance in comparison with the existing methods. The analysis is based on two attacks, black-hole and DDoS attacks. The analysis with 50 nodes revealed that the proposed method attained a minimal delay of 0.2729, maximal detection rate of 0.6726, maximal energy of 66.4275, and maximal throughput of 0.4625 in the presence of nodal attacks. On the other hand, in the absence of the attacks, the proposed method acquired 0.3491, 71.0567, and 0.8649 as delay, energy, and throughput with 50 nodes in the simulation environment. Likewise, the analysis using 100 nodes reported better results in terms of the performance metrics. The detection rate of the proposed CrowWhale-ETR is 9.7762% better when compared with the existing method, FAST + FAMOUS. The future dimension of the proposed multicast routing will be relied on utilizing various types of optimizations to determine the optimal routes to enable effective routing. Also, the proposed method will be compared with many other related works to verify the effectiveness.

References

1. Shin, V. S., Kim, J., Kwon, S., & Daemin, I. Y. (2017). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access, 5*, 11100–11117.
2. Askarzadeh, A. (2016). A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm. *Computers and Structures, 169*, 1–12.

3. Huang, J., Duan, Q., Zhao, Y., Zheng, Z., & Wang, W. (2017). Multicast routing for multimedia communications in the internet of things. *IEEE Internet of Things Journal, 4*(1), 215–224.
4. Surendran, P., & Valsalan, P. (2018). IoT based breath sensor for mycobacterium tuberculosis. *Journal of Advanced Research in Dynamical & Control Systems, 10*(15 SI), 670–674.
5. Pan, M.-S., & Yang, S.-W. (2017). A lightweight and distributed geographic multicast routing protocol for IoT applications. *Computer Networks, 112*, 95–107.
6. Vivekanand, V., & Thushara, V. T. (2016). Ultra resource constrained adaptive multipath routing for meteorological sensor networks. In *Advanced networks and telecommunications systems (ANTS), Bangalore, India*.
7. Grilo, A. M., & Heidrich, M. (2013). Routing metrics for cache-based reliable transport in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking, 2013*, 139.
8. Le, Q., Ngo-Quynh, T., & Magedanz, T. (2014). RPL-based multipath routing protocols for internet of things on wireless sensor networks. In *International conference on advanced technologies for communications (ATC), Hanoi, Vietnam*.
9. Carbajo, R. S., Carbajo, E. S., Basu, B., & Mc Goldrick, C. (2017). Routing in wireless sensor networks for wind turbine monitoring. *Pervasive and Mobile Computing, 39*, 1–35.
10. Krishnamoorthy, N., Kalaimagal, R., Gowri Shankar, S., & Abdul Asif, N. S. (2018). IoT based smart door locks. *International Journal on Future Revolution in Computer Science & Communication Engineering, 4*(3), 151–154.
11. Sha, M., Gunatilaka, D., Chengjie, W., & Chenyang, L. (2017). Empirical study and enhancements of industrial wireless sensor-actuator network protocols. *IEEE Internet of Things Journal, 4*(3), 696–704.
12. Gaikwad, K. S., & Waykar, S. B. (2017). Detection and removal of node isolation attack in OLSR protocol using imaginary nodes with neighbour response in MANET. In *2017 International conference on computing, communication, control and automation (ICCUBEA)* (pp. 1–5).
13. Jin, Y., Gormus, S., Kulkarni, P., & Sooriyabandara, M. (2016). Content centric routing in IoT networks and its integration in RPL. *Computer Communications, 89–90*, 87–104.
14. Shende, D. K., & Nikhil, S. (2018). IoT based geographic multicast routing protocol with DPA through WSN. *International Journal of Creative Research Thoughts, 6*(2), 578–584.
15. Thangarajan, R., Krishnamoorthy, N., & Mythili, M. (2019). Classification of signal versus background in high- energy physics using deep neural networks. In *International conference on emerging current trends in computing and expert technology COMET*.
16. Arul, V. H., Sivakumar, V. G., Marimuthu, R., & Chakraborty, B. (2019). An approach for speech enhancement using deep convolutional neural network. *Multimedia Research (MR), 2*(1), 37–44.
17. Kostin, A. E., Fanaeian, Y., & Al-Wattar, H. (2016). Anycast tree-based routing in mobile wireless sensor networks with multiple sinks. *Wireless Networks, 22*(2), 579–598.
18. Javaid, N., Cheema, S., Akbar, M., Alrajeh, N., Alabed, M. S., & Guizani, N. (2017). Balanced energy consumption based adaptive routing for IoT enabling underwater WSNs. *IEEE Access, 5*, 10040–10051.
19. Matam, R., & Tripathy, S. (2016). Secure multicast routing algorithm for wireless mesh networks. *Journal of Computer Networks and Communications, 3*, 1–13.
20. Almobaideena, W., Krayshana, R., Allanb, M., & Saadeha, M. (2017). Internet of things: Geographical routing based on healthcare centers vicinity for mobile smart tourism destination. *Technological Forecasting & Social Change, 123*, 342–350.
21. Wang, Bo, Chen, X., & Chang, W. (2014). A light-weight trust-based QoS routing algorithm for ad hoc networks. *Pervasive and Mobile Computing, 13*, 164–180.
22. Kim, H. W. (2014). Low power routing and channel allocation method of wireless video sensor networks for internet of things (IoT). In *IEEE world forum on internet of things (WF-loT), Seoul, South Korea*.
23. Airehroura, D., Gutierreza, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications, 66*, 198–221.
24. Fouladlou, M., & Khademzadeh, A. (2017). An energy efficient clustering algorithm for wireless sensor devices in internet of things. In *Artificial intelligence and robotics (IRANOPEN), Qazvin, Iran*.
25. Chang, H.-Y. (2017). A connectivity-increasing mechanism of ZigBee-based IoT devices for wireless multimedia sensor networks. *Multimedia Tools and Applications, 78*, 1–18.
26. Porambage, P., Braeken, A., Schmitt, C., Gurtov, A., Ylianttila, M., & Stiller, B. (2015). Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications. *IEEE Access, 3*, 1503–1511.
27. Chen, C.-H., Lin, M.-Y., & Guo, X.-C. (2017). High-level modeling and synthesis of smart sensor networks for industrial internet of things. *Computers and Electrical Engineering, 61*, 48–66.
28. Di Marco, P., Athanasioua, G., Mekikisa, P.-V., & Fischionea, C. (2016). MAC-aware routing metrics for the internet of things. *Computer Communications, 74*, 77–86.
29. Li, G., Zhang, D. G., Zheng, K., Ming, X. C., Pan, Z. H., & Jiang, K. W. (2013). A kind of new multicast routing algorithm for application of internet of things. *Journal of Applied Research and Technology, 11*(4), 578–585.
30. Nisha, S., & Balakannan, S. P. (2017). An energy efficient self organizing multicast routing protocol for internet of things. In *Proceedings of the IEEE international conference on intelligent techniques in control, optimization and signal processing (INCOS), Srivilliputhur, India* (pp. 1–5).
31. Zhu, L., Jigang, Wu, Jiang, G., Chen, L., & Lam, S.-K. (2018). Efficient hybrid multicast approach in wireless data center network. *Future Generation Computer Systems, 83*, 27–36.
32. Wang, J., Liu, Z., Shen, Y., Chen, H., Zheng, L., Qiu, H., et al. (2016). A distributed algorithm for inter-layer network coding-based multimedia multicast in internet of things. *Computers & Electrical Engineering, 52*, 125–137.
33. Mirjalili, S., & Lewis, A. (2016). The Whale optimization algorithm. *Advances in Engineering Software, 95*, 51–67.
34. Nipanikar, S. I., & Hima Deepthi, V. (2019). Enhanced Whale optimization algorithm and wavelet transform for image steganography. *Multimedia Research (MR), 2*(3), 23–32.
35. Yadav, A. K., & Tripathi, S. (2017). QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs. *Peer-to-Peer Networking and Applications, 10*(4), 897–909.
36. Das, A., & Islam, M. M. (2012). SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 261–274.
37. Kumar, R., & Kumar, D. (2016). Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network. *Wireless Networks, 22*(5), 1461–1474.
38. Dhumane, A. V., & Prasad, R. S. (2017). Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT. *Wireless Networks, 25*, 1–15.
39. Long, N. B., Choi, H.-H., & Kim, D.-S. (2016). Energy-aware routing scheme in industrial wireless sensor networks for internet

of things. In *Systems emerging technologies and factory automation (ETFA), Berlin, Germany*.

Dipali K. Shende (born 1982) received her M.E. in VLSI and Embedded (2011) from Savitribai Phule Pune University. She pursing her Ph.D. from Savitribai Phule Pune University in Internet of Tings domain. Having altogether Experience of 15 years in educational field and core industry. Associated as Assistant Professor (E&TC) in Sinhgad Institute of Technology, Lonavala, Pune since 2008. Her excellence in Embedded Development and Teaching profession. In 2018 she received "Best Teacher Award" for academic year 2017–2018 from Sinhgad Institute of Technology at Institute level. She has been conferred with National Best Teacher Award "Adarsh Vidya Rastriya Puraskar in year 2018" at Ahmedabad Gujrat. Her First patent titled "System To Alarm Freshwater Contamination Based on Intelligent Device with IoT-Based Multicast Routing" published in Indian patent Journal (Jan 2020) toward her research work. Her keen interest is in Internet of Things, WSN, and Embedded System Design. She had more than 25 International and National publications. She is also reviewer of International Journal of Creative Research Thoughts (IJCRT) and Innovative Research in Engineering. More than 10 workshops conducted and expert talks delivered in area of Embedded and IOT.

S. S. Sonavane Principal at Indira College of Engineering and Management, Parandwadi, Pune. Completed B.E. (Electronics) from University of Pune, M.E. (Electronics) from BAMU, Aurangabad and Ph.D. (Electronics Engg.) from IIT, Dhanbad in 2009. He is having 22 years of experience in educational field and served in many well-known organizations. Currently he is working as Dean R&D and Professor (E&TC) at Indira College of Engineering and Management, Parandwadi, Pune. He has a successful academia and published two books at International level (Austria and one in Germany). He had more than 75 International and National publications on his name in reputed peer Reviewed Journals. He is the registered Ph.D. guide in SPPU, Pune. He is also Reviewer of many Electronics International Journals including IEEE Sensor Journal and IEEE Communication Letters. He had successfully completed two Research Projects funded by University of Pune.