International Journal of Uncertainty,
Fuzziness and Knowledge-Based Systems
Vol. 29, Suppl. 2 (December 2021) 297–315

DOI: 10.1142/S021848852140016X

World Scientific
www.worldscientific.com

Black-Hole Attack Mitigation in Medical Sensor Networks Using the Enhanced Gravitational Search Algorithm

Rajesh Kumar Dhanaraj
School of Computing Science and Engineering,
Galgotias University, India
d.rajeshkumar@galgotiasuniversity.edu.in

Rutvij H. Jhaveri
Department of Computer Science and Engineering,
Pandit Deendayal Petroleum University, India
rutvij.jhaveri@sot.pdpu.ac.in

Lalitha Krishnasamy
Department of Information Technology,
Kongu Engineering College, India
klalitha.it@kongu.edu

Gautam Srivastava*
Department of Mathematics & Computer Science,
Brandon University, MB, Canada
Research Centre for Interneural Computing,
China Medical University, Taichung, Taiwan
srivastavag@brandonu.ca

Praveen Kumar Reddy Maddikunta
School of Information Technology and Engineering,
VIT, Vellore, Tamilnadu, India
praveenkumarreddy@vit.ac.in

Received 9 April 2021
Revised 26 May 2021

In today's world, one of the most severe attacks that wireless sensor networks (WSNs) face is a Black-Hole (BH) attack which is a type of Denial of Service (DoS) attack. This attack blocks data and injects infected programs into a set of sensors in a group to capture packets before reached to the target. Therefore, raw data in the BH region is thwarted and is unable to reach its destination. The network is susceptible to various

*Corresponding author.

types of attacks as it is accessible to all types of users and minimizing the energy depletion without compromising the network lifetime is an NP-hard problem. Even though numerous protocols came into effect to overcome the BH attack and to enhance the security of packet delivery in WSNs, Simulated Annealing Black-hole attack Detection (SABD) based Enhanced Gravitational Search Algorithm (EGSA) is yet another implemented strategy to reduce the BH attacks. EGSA-SABD detects and isolates the BH infectors in WSNs. Initially, sensor nodes are hierarchically clustered using similar residual energy to reduce energy consumption. Then, the BH attack possibility in a deployed node is evaluated to find the existence of BH nodes in the region. In the end, EGSA-SABD is employed to detect and quarantine BH attackers in WSNs. The performance of EGSA-SABD is evaluated with certain metrics such as BH attack detection probability rate (BHatt_Prate), energy consumption (E_c), Duration of BH attack detection (Attduration), Packet delivery ratio (P_{dr}). Based on the experimental observations, the EGSA-SABD outperforms the BHatt_Prate by 13% and also reduces the energy consumption by 21%.

Keywords: Black-hole attack; wireless sensor networks; medical data; clone attack; residual energy.

1. Introduction

Wireless Sensor Networks (WSN) are made up of a set of sensors that organize themselves in a network and communicate with other nodes without interference. The major task of any sensor node includes sensing, processing data, and transmitting it to the coordinator/Sink nodes efficiently. WSN are expected to control node failure as well as to withstand ever-changing environmental conditions. Due to the advancements in technology, healthcare applications are increasingly dependent on data generated from several medical sensors to gather information and also to monitor patient health. In the Internet of Medical Things (IoMT), various sensor devices are fixed on patients that can sense vital health information.[1] The sensed information must be sent to nearby gateways and/or communication channels. If there are no proper security mechanisms, confidential data may be leaked to attackers.[2,3] Figure 1 depicts various types of attacks in IoMT. In IoMT architecture, the sensor nodes capture the patient data and send it to the nearest cluster head, and from the cluster head the data is sent to the sink node.

A Black-Hole (BH) attack is shown in Fig. 2. Black-Hole can be represented by a malicious node, which uses the routing protocol to maintain the smallest route to the destination node. Consider a malicious node C. When node A is forwards Route Request (RREQ) packets, the nodes B, C and D are going to receive it. Node C is a malicious node, so it does not verify with routing table for the desired route to node E. Meanwhile, node E directly forwards back a Route Reply (RREP) packet. But, node A collects the RREP packet from C prior to the RREP in B and D node. Node A accepts that the routes through M is the shortest route and deliver some packet to the destination through it. When node A forwards data to M, it consumes the entire data and performs like a Black-Hole. A BH attack is a kind of Denial of Service (DoS) attack where malicious nodes (MN) transmit a bogus response to the source about a quickly reached path. The initiator establishes the link using

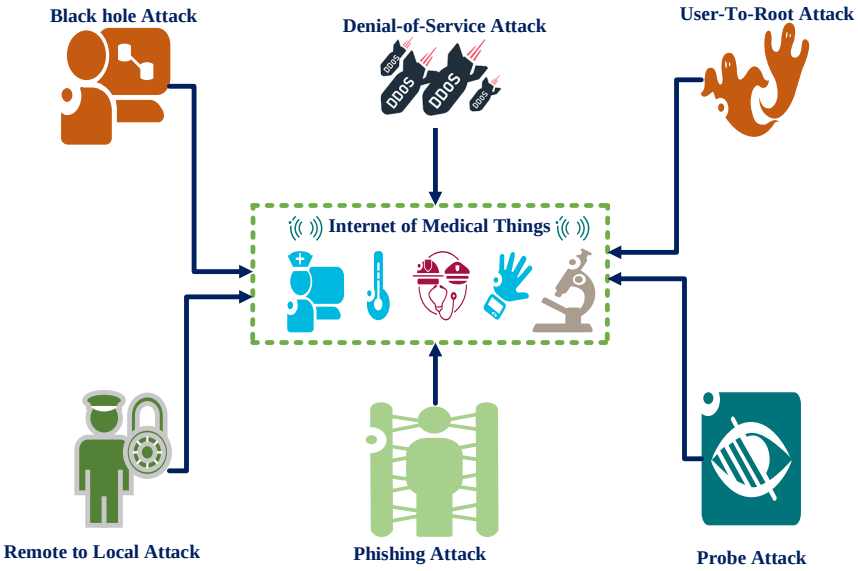

Fig. 1. Types of attacks in IoMT environment.

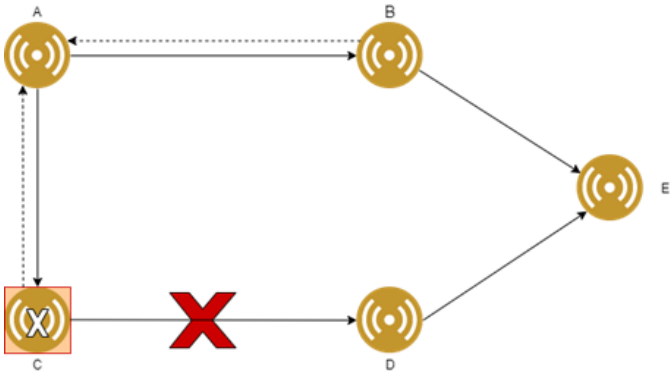

Fig. 2. Black-hole attack.

sent data to the address specified in the response. These packets will be corrupted or eradicated instead of reaching the target. Hence, BH attack detection will be a considerable issue in WSNs. At present, most of the research works have been designed for detecting, isolating, and preserving BH attacks in WSN. In Ref. 4, to detect intruders in advance, a method called Advanced Detection of Intrusions on Sensor Networks (ADIOS) was discussed to reduce the side-effects of BH attack in WSN but did not address the various DoS attacks and their detection mechanisms. To identify and isolate BH attacks in mobile ad hoc networks (MANET), a detection approach named Novel Honeypot Based Detection and Isolation (NHBADI) was

designed in Ref. 5 that utilize Honey pot methodology. It increases the security and decreases the overheads in both network and routing in addition to packet drops ratio. However, the NHBADI Approach consumes more time. Proactive Alleviation Procedure was developed in Ref. 6 that integrates three different procedures such as detection of a hole, degree of duration, and sensitive guards to detect the malicious nodes in MANET. This Proactive Alleviation is productive concerning cost and achieves guaranteed QoS services. However, the PDR is not attained at the expected level.

A new technique represented in Ref. 7 utilizes unmanned aerial vehicles (UAVs) to attain effective and fast detection of BH attacks with adequate EC.[8] However, this method takes more energy for BH attack detection. A solution against BH attacks that depends on fuzzy rules was presented in Ref. 9 to discover the corrupted node which in turn reduces data loss. A new method was presented in Ref. 10, to perform detection and isolation of BH nodes in SN. From that, the BH node is detected via observing fake reply packets sent by the nodes and it is eliminated from the network. A link-state optimized routing algorithm (OLSR) was investigated in Ref. 11 that identifies and isolates different types of misbehavior nodes utilizing a routing path between two nodes. OLSR protocol is proficient to notice the attackers on the path without raising the network traffic overhead. In Ref. 12, a novel approach was designed to detect BH attacks in WSN. An efficient intrusion detection mechanism with hierarchical energy was developed in Refs. 13 and 14 to safeguard sensors from BH attackers which results in improved security and energy saving. However, the performance of this intrusion detection system against other BH security mechanisms remained unaddressed. An EDRI-based approach was implemented in Ref. 15 to identify and eradicate the corrupted nodes in MANET which works based on AODV. This protocol procures a data routing table with extended specifications to fix the corrupted nodes in the chosen path by employing additional control packets. EDRI reduces overhead due to excess packets, delay and brings down false positives in the scope of security mechanism. However, the detection of all types of malicious nodes in the network remained unaddressed. The above-said practices are taken into account, a framework is proposed here namely, the EGSA-SABD model for healthcare applications to discover and segregate the BH attackers in WSNs. The major contributions of the EGSA-SABD model include the following,

(1) To cluster the SN in WSNs and to reduce the energy utilization of the data collection process in healthcare applications, Residual Energy-based hierarchical clustering is performed in the EGSA-SABD model.
(2) To discover the presence of BH attack nodes in WSNs proposed EGSA-SABD model utilizes the possible Black-hole attacks based on location on Cluster Nodes.
(3) To detect and segregate the BH attackers in WSNs, the GSA-based Simulated Annealing model is employed in the EGSA-SABD model.

The remaining portions of this work are arranged in the following order: Section 2 explains an ephemeral review of some closely interrelated works about BH attack detection, isolation, prevention. The proposed EGSA-SABD model is clearly described in Section 3. Section 4 presents the experimental setting of the proposed model. Section 5, discusses the investigational results which show the effectiveness and efficiency of the algorithm, and Section 6 concludes the work with future directions.

2. Related Works

An effective Mutable Black Hole Unearthing Mechanism A mechanism for detecting Black-Hole which is mutable and unearthing was designed in[16] through clustering in addition to classification. A Survey of different BH Detection Techniques was presented in WSNs are described in.[17–19] In,[20] A BFO Based Optimized Positioning technique was developed to examine the BH impact on data transmission and to optimize the Sink location which in turn enhance the delivery ratio with multiple Sinks. Yet another intrusion with improvised detection system to shield WSN network from BH attacks was implemented in Ref. 21. In all the works described from the papers,[16,21] optimizing the deployed node position and to avoid the BH attack was described but yet to address the energy consumption issues and the balancing of BH attack nodes along with the network operations.

An improved AODV protocol to process the data packets were given in Ref. 22 to identify channeling misbehavior and alert the network to decrease additional overhead. However, the hybrid detection method and integrating benefits of proactive and reactive routing is yet to be addressed. In Ref. 23, a review on BH attack and security against BH attack was described. To overcome the existing cooperative BH attack issues, a Reliability analysis mechanism was planned in Ref. 24 via AODV routing protocol. Besides, the Reliability analysis mechanism assists in attaining maximum reliability utilizing reducing the complexity of the system. However, the other type of attacks that affect the network was not considered in the reliability analysis mechanism. In Ref. 25, a new method was introduced to find BH attack using different BS and a checking agent-based technology to detect the existence of BH nodes in WSN. However, message complexity and EC are more. An energy preserving detection mechanism was designed in Refs. 26 and 27 for detecting BH, DoS attack which results in minimum EC, improved throughput, reduce E2E delay and maximum PDR of the network. In Ref. 28, A secure and trust-based efficient protocol was presented to secure against particular and cooperative BH attacks which combine trust metric estimation to ensure secure path establishment. This paper addresses the above-said issues with possible solutions.

Once the BH attack node is detected in the network, instead of rerouting the data, the clone nodes will be deployed to carry out the work of malicious node as given in Ref. 14. The threat model will be implemented with active and passive attacks and authenticated replicas are created to overcome the security issues. But,

the clone node should be detected and informed to the Sink and it's a cumbersome task if the replicas increased due to the network scale. The traffic patterns to route the data without get caught by the malicious node is another major issue and the optimal routing algorithm[29] is to be implemented with hierarchical clustering. A GIS based optimal routing transportation is implemented in Refs. 30 and 31 which applies the modified Dijkstra's algorithm to solve the stochastic network routing problem. But the best route to be always searched when a malicious node found which increases the complexity and EC is also high. There are numerous routing protocols that are implemented for detecting the BH attacks and rerouting mechanism was implemented to prevent the data loss. The main objective of these implementations is to avoid and or to detect the BH attacks which in turn to improve the security of sensor data. The major focus of detecting BH attacks are, DoS attack which results in minimum Energy Consumption, improved throughput, reduce End to End delay and maximum Packet Delivery Ratio of the network which is NP-hard problem. This motivated the research to bring the network balancing while reducing the BH attacks.

3. EGSA based Simulated Annealing Black-Hole Attack Detection (EGSA-SABD)

The Enhanced Gravitational Search Algorithm based Simulated Annealing Black-Hole Attack Detection (EGSA-SABD) model is designed to identify and segregate the BH attack nodes. In a BH attack, an MN wrongly exhibits the best paths (e.g. the shortest route) from the source to reach the target while performing the path-discovering process. An MN intends to ruin the path-discovering procedure or to interrupt the packets being sent to the Sink node. EGSA-SABD model utilizes EGSA based Simulated Annealing model to discover and quarantine the BH

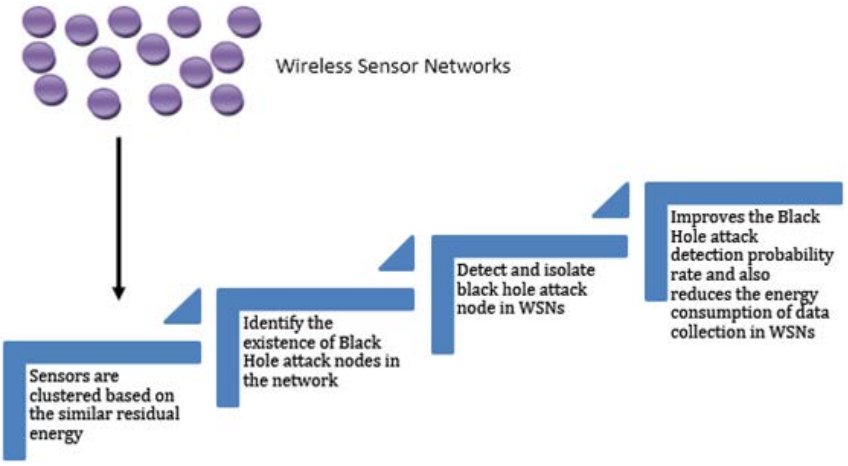

Fig. 3. The Overall Architecture Diagram of EGSA-SABD Model.

nodes in the WSN. The overall architecture diagram of the EGSA-SABD model for BH attack detection and isolation is illustrated in Fig. 3. In Fig. 3, initially, the EGSA-SABD model implements residual energy-based hierarchical clustering for grouping the nodes into clusters, using similar residual energy of each node. Then, the possibility of BH attack based on location and nodes in a cluster are performed to discover the presence of BH attack nodes in step 2. In step 3, EGSA based Simulated Annealing prototype is presented to discover and quarantine the BH attack nodes. This helps to increase the BHAtt_Prate and reduces the energy consumption of data collection efficiently as shown in step 4.

3.1. *Residual energy-based hierarchical clustering*

The EGSA-SABD model exploits residual energy based hierarchical clustering for minimizing the EC of data collection in WSNs. During the residual energy based hierarchical clustering process, the SN in WSN is clustered using similar RE for reducing the EC of data collection.[32,33] The EGSA-SABD model has used a hierarchical clustering approach for clustering sensor nodes (SN) in WSNs. Cluster Head (CH) is elected using a hierarchical clustering approach from the group of SN through a Cluster ManageR (CMR) which in turn is transmitted to the Sink using next hop CMR. Each SN in WSN is clustered into various clusters during the residual energy based hierarchical clustering process using similar RE.[34] The CMR is located in a fixed position (i.e. static) in a sensor network. Then, every Member of a Cluster (CM) connects to its head directly when performing the data collection process. The CMR preserves their nodes ID and RE. The CMR reselects the CH when the RE of CH is lower than the threshold level based on higher RE. During data transmission, the CMR located in the specified area gathers data obtained from its CH and to CMR in the next hop. Thus, CMR in each hop transmits the data to the Sink with an efficient routing mechanism. In clustering, one node functions as CH, and the remaining nodes operate as CM. In the collection of SN, CH is selected through a Residual Energy-Based Hierarchical Clustering algorithm that is depending on EC. When the CH's energy level is below than threshold energy, then CMR chooses the new CH. In a collection of SN, A node that has a greater energy level is chosen as the CH. The communication established between CMR is structured that minimizes the sending energy of node while transmitting information to the BS from sensors. Figure 4 illustrates the Residual Energy-based Hierarchical Clustering process.

In Algorithm 1, Residual Energy-Based Hierarchical Clustering Algorithm efficiently collects the aggregated data from the different SN in WSNs with the optimized EC. This algorithm depicts how the No. of clusters and also CH are attuned dynamically. By selecting CH in WSN, the energy spent towards collecting data is equally provided among the nodes. This helps to diminish the EC efficiently. Since CMR selects CH with the routing table, that comprises information about the SN (CLUSTER_ID, RESIDUAL ENERGY). The data transmitted from CMR to CMR

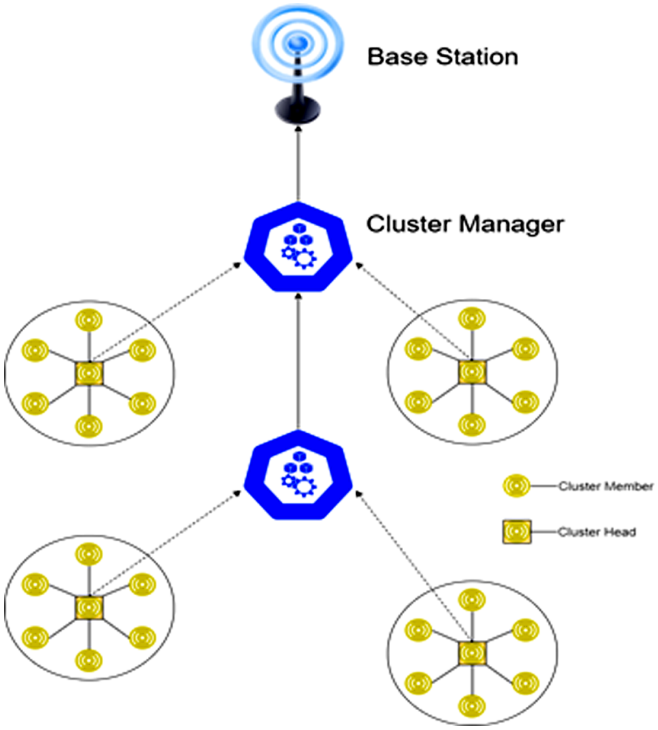

Fig. 4. Architecture diagram of residual energy-based hierarchical clustering process for data collection.

Algorithm 1: Residual Energy-Based Hierarchical Clustering.

Assign threshold energy E_{th}=20J
while *Energy (current CH)* $< E_{th}$ **do**
    The CMR transmits a control message to select a CH
    Each sensor updates the present RE to CMR
    CMR selects RE_{max} node as a new CH and broadcasts the message
    All the CM update its new CH in their initial path
for *each sensor nodes* SN_i **do**
    while $E_{th} < 25$ **do**
        if $E_{th} <= 25$ && $E_{th} > 15$ **then**
            assign E_{th} = 15J;
        else
            assign E_{th} = 5J;
        Continue the process until all nodes become clusters

via next-hop until reaches the Sink. Thus, the EGSA-SABD model carried out the data collection process effectively with lesser EC.

3.2. *Possibility of black-hole attacks based on location in cluster nodes*

Possibility of Black-hole attacks based on location in Cluster Nodes is done when clustering the SN in WSNs, to discover BH attacks on clustered nodes. Since the presence of BH attack nodes to be identified in WSN, the location and RE of SN is considered for the same. BH attack takes place in different ways. Based on similar RE, the EGSA-SABD model analysis the presence of BH attack in clustered nodes. When performing the data collection, each node SNode in WSNs transmit its presence (SNode_{ID}, $\text{SNode}_{\text{row, col}}$) ($\text{SNode}_{ID}$), to Sink BS via new SN (i.e. neighboring nodes). Here SNode_{ID} signifies sensor nodes ID where $\text{SNode}_{\text{row , col}}$ signifies the SN position denoted as row, colrow, col respectively. Figure 5 depicts the BH attack observed on clusters using similar RE.

A node's physical presence is verified by Sink with the collected data. If BS attains two different locations SNode_{ID1}, $\text{SNode}_{\text{row, col}}$ and SNode_{ID2}, $\text{SNode}_{\text{row.col}}$ with the same node ID SNode_{ID2}, $\text{SNode}_{\text{row,col}}$ with same residual energy $\text{SNode}_{ID1} = \text{SNode}_{ID1}$, but with different location, then BS confirms that any of the normal node turned into a BH attack node. Algorithm 2 explains how the BH attack is identified in the network.

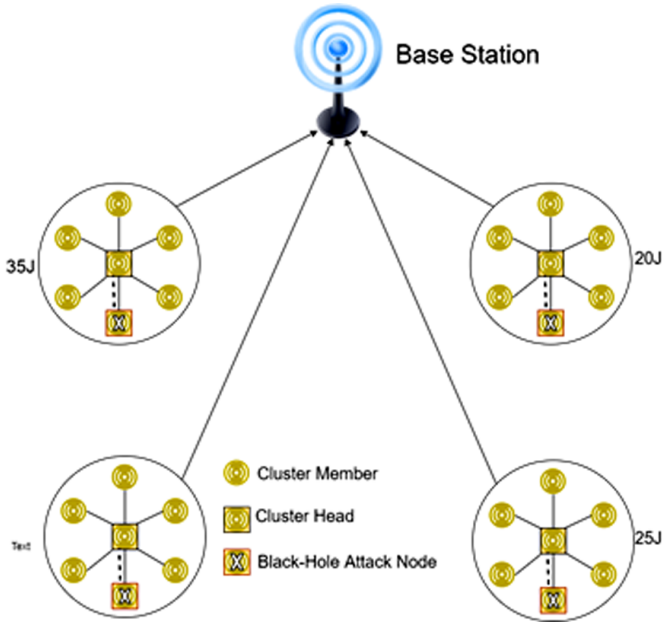

Fig. 5. Structure of Black Hole Attack in Clusters with similar RE.

Algorithm 2: BH Attack on Clustered Nodes.

Input: Base Station 'BS', Sensor Nodes '$SN_i = SN_1, SN_2, \ldots, SN_n$', Sensor Node ID '$SN_{ID} = SN_{ID1}, SN_{ID2}, \ldots, SN_{IDn}$', Location information '$(SN_{\text{row,col}})$', Residual energy '$RE(SN_{ID})$'
Output: Improves BH attack detection probability
for *each cluster* **do**
  for $SN_i \leq nSN_i$ **do**
    Sensor node transmits SN_{ID}, location information '$SN_{\text{row,col}}$ ' to the base station
    if $SN_{IDi} == SN_{IDj}$ && $RE(SN_{IDi}) == RE(SN_{IDj})$ && $SN_{IDi_{\text{row,col}}} <> N_{IDj_{\text{row,col}}}$ **then**
      Confirm the presence of BH attack node;
    else
      Fix the present node as normal node;

In Algorithm 2, a BH attack on clustered nodes is present when the two SN hold the same node ID and RE but with a different location. In this case, the BS marked either of the SN as the BH attack node. The next step is to choose the onlooker node which identifies the BH attack efficiently which is described in the upcoming section.

3.3. *Nodes EGSA based simulated annealing*

After clustering, the EGSA-SABD technique utilizes EGSA based Simulated Annealing model for finding the witnessed node to detect and separate the BH attacker node in WSN. The Gravitational Search Algorithm discussed in Ref. 35 contains global searchability. But, this algorithm lacks a local search mechanism. Conversely, Simulated Annealing Algorithm in Ref. 36 achieves local optimal solution. However, this algorithm does not good in global searching. Hence, the proposed EGSA-SABD model incorporates the Gravitational Search Algorithm (to identify the node with BH attack) followed by Simulated Annealing (to separate the attacked node in WSNs) to offer the search capabilities in terms of global as well as local. Initially, the EGSA-SABD model describes the BH attack node detection process through Enhanced Gravitational Search Algorithm after that the optimized annealing prototype is described. Let us assume WSNs comprises of nn SN (i.e. masses) where the location of i_{th} node is formalized as,

$$P_i = P_i^1, P_i^2, \ldots, P_i^k, \ldots, P_i^n \tag{1}$$

From above Eq. (1), P_i^k, denotes the position of i_{th} SN in k_{th} dimension. The gravitational force performing on masses i from masses j at an exact time t will be

formulated as below,

$$\text{Force}_{ij}^{k} = \text{Grav}(t) * \frac{\text{Mass}_{pi}(t) * \text{Mass}_{aj}(t)}{\text{Distance}_{ij}(t) + \epsilon} \tag{2}$$

From above, Eq. (2), $\text{Mass}_{pi}(t)$ and $\text{Masss}_{aj}(t)$ denotes the passive as well as active interactive mass associated to the mass of SN i and j respectively. The gravitational constant is indicated with $\text{Grav}(t)$ using a constant ϵ. Distance among SN i and j at time t is described by Distance $_{ij}(t)$. To acquire stochastic characteristics, total force is supposed to act on SN i with the dimension e is weighted randomly with sum of e_{th} component of forces used from the other SN which is formulated as,

$$\text{Force}_{i}^{\epsilon} = \text{ran Force }{}_{ij}^{k}(t), j = 1, j \neq i \tag{3}$$

From above, Eq. (3), *ran* represents the random No. of periods 0,1. So, based on law of gesticulation, the speed of SN i in a time t in k_{th} element is formulated as,

$$ACC_{i}^{\epsilon}(t) = \frac{\text{Force}_{ij}^{k}}{\text{Internal Mass}_{i}(t)} \tag{4}$$

From above, Eq. (4) Internal Mass $_i(t)$, indicates the initial mass of SN i in a time t. Inertia masses and gravitational forces are computed to estimate the fitness value for finding the witness node. A SN has greater mass signifies high efficient node. Using fitness map function, the equality of gravitational mass and inertia mass values are computed as like Refs. 37 and 38. This can be attained as given below.

$$m_i(t) = \frac{\text{Fitness}_i(t) - \text{ Worst } (t)}{\text{Best}(t) - \text{Worst}(t)} \tag{5}$$

$$M_i(t) = \frac{m_i(t)}{\sum_{r=1}^{n} m_r(t)} \tag{6}$$

From Eq. (5) and Eq. (6), Fitness $_i(t)$ signifies the value of fitness 'i' SN at 't' time and 'Best(t)' and 'Worst(t)' value is achieved as follows. To reduce the minimization issue, the 'Best(t)' and 'Worst(t)' is formulated as given below,

$$\text{Best } (t) = \min \text{ Fitness }_n(t) \tag{7}$$

$$\text{Worst } (t) = \max \text{ Fitness }_n(t) \tag{8}$$

From Eq. (7), Eq. (8), the 'Best(t)' and 'Worst(t)' is analyzed for minimization issue. To address maximization issue, the 'Best(t)' and 'Worst(t)' is formulated as below,

$$\text{Best } (t) = \max \text{ Fitness }_n(t) \tag{9}$$

$$\text{Worst } (t) = \min \text{ Fitness }_n(t) \tag{10}$$

Therefore, the SN which has the best fitness value is assumed as a witness node that identifies the occurrence of BH attack on cluster nodes with similar RE.

Witness node presents the best fitness value. Once the BH attack node is identified, then it is isolated through a simulated annealing model that is explained in the following subsection.

3.4. *Simulated annealing model*

The simulated Annealing Model is used in the EGSA-SABD model to separate the detected BH attackers. During every step, the simulated annealing model assumes the neighbor Sensor node 'SNode' of the present SN. Next, it makes a decision that the system moves to 'SNode' or staying at 'SNode' for segregating the node with BH attack. This process is reiterated until the detected attack node gets segregated in WSN. Algorithm 3 explains the simulated process of strengthening to segregate the identified node with BH in WSN.

Algorithm 3: Simulated Annealing Algorithm.

```
Input: Sensor Nodes SN_1, SN_2, ... SN_n
Output: Reduced DBHAD
for each cluster do
    for SN_i == 0 to n do
        Select a random neighbour SN_new ← Neighbor (SN_i)
        if Prob (RE (SN_i), RE (SN_new )) > Ran(0, 1) then
            Move to the next sensor node SNode_i ← SNode_new
            BH attack node does not present and outputs sensor node SNode_i
            and terminates test;
        else
            Move to the next sensor node SNode_new ← SNode_i
            BH attack node does not present and outputs sensor node
            SNode_new and terminates test;
```

As shown in Algorithm 3, the Simulated Annealing Algorithm begins from SN_i and the process is repeated until all the nodes are visited. Meanwhile, an arbitrarily selected fellow node of a given 'SN' is made. The annealing algorithm is designated by the Energy_Residual function that provides the RE to use, specifies the existence of SN in a current network. The request towards EGSA based Simulated Annealing in the EGSA-SABD model decreases the time of BH attack detection.

4. Experimental Setting

The EGSA-SABD model is employed using the `NS-2` Simulator, a well-known tool to the extent of the efficiency of the proposed work. The number of SN chosen for deployment varies from 50 to 350.[39] The CH node gathers the data from dissimilar SN which lies between the ranges of 9-–63 towards the BS node. In our

simulation, the data packet size may vary from 100 Kbytes to 512 Kbytes with the duration range of 500 sec to 1500 sec. The specification bounds used for conducting experiments are demonstrated in Table 1.

Table 1. Parameters used.

Parameters	Values
Deployment area	1200 m ∗ 1200 m
No. of nodes	50,100,150,200,250,300,350
Data block size	9, 18, 27, 36, 45, 54, 63
Communication Range	30 m
Initial Energy of a node	2 Joules
Execution time	500s to 1500s
No. of Iterations	20

The performance of the EGSA-SABD model is analyzed with the metrics namely BHADPR, EC, DBHAD, and PDR.

5. Results and Performance Study

The experimental results and performance of the EGSA-SABD model are evaluated and compared against existing methods namely ADIOS[4] and NHBADI Approach.[5]

5.1. *Degree of energy consumed*

The product of energy spent by a sensor node and the total number of SN constitutes Energy consumption (E_c) of the network. E_c rate is evaluated in Joules (J) and formulated as follows,

$$\mathrm{E}_c = \text{ energy spent by a SN } * \text{ total number of SN in a network} \tag{11}$$

From Eq. (11), the minimum energy requirement is calculated. From the observations, the method should be more efficient if the E_c of the network is lesser than the previous measures. EGSA-SABD model is tested with various scenarios from 50 to 350 random deployed nodes and each scenario is iterated 10 times. The results were brought in with the average of all the scenarios. From the Fig. 6, the proposed EGSA-SABD model provides lower E_c rate as compared to existing methods.[4,5] Moreover, when increasing the No. of SN, the E_c also increased invariably in all the approaches due to the exponential number of data packets. In ADIOS, the intruder verification is done often which consumes the energy and the same is reflected in BHBADI also which spends much energy on detecting the honeypot. However, the E_c rate of the proposed EGSA-SABD model is considerably lower because of inertia measurements as compared to existing works.[4,5] This is because the residual energy-based hierarchical clustering is utilized in the EGSA-SABD model, where

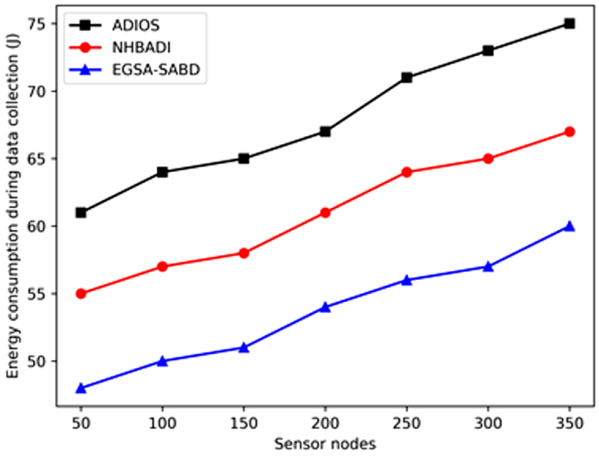

Fig. 6. Measurement of EC during Data Gathering.

SN is clustered through the similar RE which makes lesser the EC of data collection in WSNs. Therefore, the EGSA-SABD model minimizes the Ec rate for data gathering by 27% and 14% as against existing works,[4,5] respectively.

5.2. *Black hole attack detection probability rate* (*BHAtt_Prate*)

Black Hole Attack Detection Probability Rate is measured as a different ratio between the total number of SN and the node with BH attack in WSN. The BHAtt_Prate is calculated in percentage (%) and formalized as below,

$$\mathrm{BH}_{\mathrm{Att\_Prate}} = \frac{(SN_i - SN_{CN})}{SN_i} \tag{12}$$

From the Eq. (12), the BHAtt_Prate is achieved based on overall Sensor Node SN_i and the BH attack sensor nodes SN_{CN} during data collection. The ratio of BHAtt_Prate is directly proportional to the efficiency. The BHAtt_Prate of three methods is presented using a different number of SN ranges from 50–350. This scenario is depicted as a graph which is shown below in Fig. 7 with different deployed scenarios. The EGSA-SABD approach provides higher BHAtt_Prate as compared to other existing.[4,5] When increasing the No. of SN, the BHAtt_Prate also increased rationally irrespective of the methods. In ADIOS, the attack detection probability is based on the intruders identified by the network and NHBADI fixes the BH attack detection with redundant data received. However, BHAtt_Prate using the proposed EGSA-SABD model is considerably increased since the EGSA-SABD approach utilizes BH attack possibility based on location in a cluster, where probability detection gets improved. This results in improving the BHAtt_Prate in a significant manner. Hence, the EGSA-SABD model Increases the BHAtt_Prate by 17% and 8% as compared to existing works,[4,5] respectively.

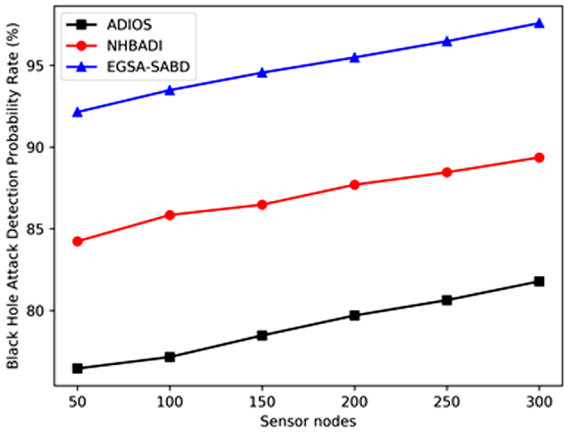

Fig. 7. Measurement of Black Hole Attack Detection Probability Rate.

5.3. *Measure of black hole attack detection time*

$\text{Att}_{\text{Duration}}$ processes the quantity of time to detect nodes with BH attack in WSNs. The efficiency of the indirectly proportional to $\text{Att}_{\text{Duration}}$. It is evaluated in terms of milliseconds (ms) and is formulated as follows,

$$\text{Att}_{\text{Duration}} = \text{Time checkBHnodes} \tag{13}$$

The results of $\text{Att}_{\text{Duration}}$ is analyzed with current and existing methods with different deployment strategies from 50–350. This scenario is depicted as a graph which is shown below in Fig. 8 with different deployed scenarios. Figure 8 illustrates $\text{Att}_{\text{Duration}}$ with diverse No. of SN using three methods. From Fig. 8, the EGSA-SABD model considerably reduces $\text{Att}_{\text{Duration}}$ as compared to existing.[4,5]

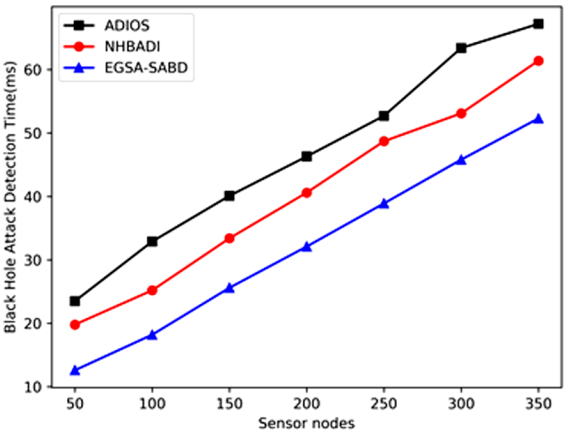

Fig. 8. Measuring the time of finding the Black Hole Attack.

The increase in the No of SN furthermore increases the in the current as well as existing algorithms.[40,41] However,the $\text{Att}_{\text{Duration}}$ is considerably lower in EGSA-SABD due to simulated annealing algorithm in EGSA-SABD model where the schedule is illustrates as $\text{Energy}_{\text{residual}}$ function that provide RE to employ, given the existence of SN in the network. Hence, EGSA-SABD model decreases $\text{Att}_{\text{Duration}}$ by 53% than ADIOS[4] and 30% as compared to NHBADI Approach.[5]

5.4. *Evaluation of packet delivery ratio*

PDR is measured as the proportion of the effectively received packets count at the BS to the No. of packets sent in total by the SN. It is evaluated in percentage (%) and is formulated as,

$$\text{Packet Delivery Ratio } (P_{dr}) = \frac{P_{\text{rec}}}{P_{\text{send}}} * 100 \tag{14}$$

From the Eq. (14), the P_{dr} is obtained using the packets received in number at the BS P_{rec} to the No. of packets sent in total by the SN P_{send} respectively. The efficiency of PDR with different scenarios is given here. The experimental results of PDR and its impact in all the methods compared is clearly depicted in Fig. 9. From Fig. 9, the EGSA-SABD model considerably increases P_{dr} as compared to existing.[4,5] In all the approaches, increase in SN count furthermore increases the P_{dr}. However, the P_{dr} in EGSA-SABD model is higher where SN with best fitness are chosen to witness the occurrence of BH attacks in cluster nodes. The PDR is the number of successful packets received to the Sink in ADIOS and redundant data are identified and removed which increases the PDR in NHBADI. Thus effectively isolate the detected BH attack node in WSNs as like Ref. 42. Therefore, EGSA-SABD model improves the P_{dr} by 14% and 7% as compared to existing works,[4,5] respectively.

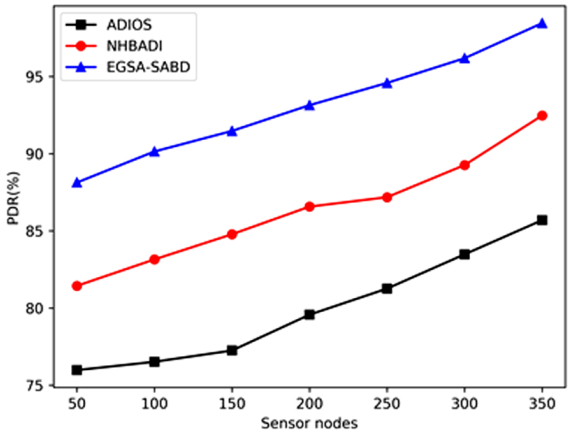

Fig. 9. Measurement of Packet Delivery Ratio.

6. Conclusion

An efficient framework called EGSA-SABD is introduced to detect and segregate BH attackers in healthcare applications based on WSN. The main goal of EGSA-SABD is to reduce energy consumption and to improve the delivery ratio of data and BHAtt_Prate with different node densities and packets. The nodes which have the same ID and residual energy but different locations are identified as BH nodes. Then any one of the two nodes is declared as a BH attacker by using cluster probability. The SN which has the best fitness value is assumed as a witness node that identifies the occurrence of BH attack on cluster nodes with similar RE. Witness node presents the best fitness value. Once the BH attack node is identified, then it is isolated through a simulated annealing model. With the experimental evaluation of the EGSA-SABD model, the BH attack detection probability rate provides precise results than the existing works. The simulation results show that the EGSA-SABD model improves the BHAtt_Prate by 13% and also reduces the E_c by 21% as against existing works.

Even though the EGSA-SABD model identifies the BH attack node and improves the attack detection rate and the energy conservation, it was implemented for the static model with very less number of nodes. This may not predict the BH attacks when the real time traffic flows are monitored in a dynamic environment. So, an alternate methodology like machine learning algorithms to find the real time traffic patterns and the way of replacing the attacked node to be used in large scale to make the solution effective in WSN.

References

1. A. R. Javed, L. G. Fahad, A. A. Farhan, S. Abbas, G. Srivastava, R. M. Parizi and M. S. Khan, Automated cognitive health assessment in smart homes using machine learning, *Sustainable Cities and Society* **65** (2021) 102572.
2. R. M. S. Priya, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary and M. Alazab, An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture, *Computer Communications* **160** (2020) 139–149.
3. A. R. Javed, M. U. Sarwar, M. O. Beg, M. Asim, T. Baker and H. Tawfik, A collaborative healthcare framework for shared healthcare plan with ambient intelligence, *Human-centric Computing and Information Sciences* **10** (2020) 1–21.
4. A. M. Abdalla, I. A. Saroit, A. Kotb and A. H. Afsari, Misbehavior nodes detection and isolation for MANETs OLSR protocoL, *Procedia Computer Science* **3** (2011) 115–121.
5. M. R. Babu, S. M. Dian, S. Chelladurai and M. Palaniappan, Proactive alleviation procedure to handle black hole attack and its version, *The Scientific World Journal* **2015** (2015) Article ID 715820.
6. A. Dorri, An edri-based approach for detecting and eliminating cooperative black hole nodes in MANET, *Wireless Networks* **23** (2017) 1767–1778.
7. H. Kalkha, H. Satori and K. Satori, Preventing black hole attack in wireless sensor network using HMM, *Procedia Computer Science* **148** (2019) 552–561.

8. R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta and S. Bhattacharya, Security and privacy of UAV data using blockchain technology, *Journal of Information Security and Applications* **55** (2020) 102670.
9. Y. M. Khamayseh, S. A. Aljawarneh and A. E. Asaad, Ensuring survivability against black hole attacks in MANETs for preserving energy efficiency, *Sustainable Computing: Informatics and Systems* **18** (2018) 90–100.
10. L. Krishnasamy, R. K. Dhanaraj, D. G. Gopal, T. R. Gadekallu, M. K. Aboudaif and E. A. Nasr, A heuristic angular clustering framework for secured statistical data aggregation in sensor networks, *Sensors* **20** (2020) 4937.
11. A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. A. Kumar, B. Panigrahi and K. C. Veluvolu, Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm, *Microprocessors and Microsystems* (2020) 103352.
12. H. Moudni, M. Er-rouidi, H. Mouncif and B. El Hadadi, Black hole attack detection using fuzzy based intrusion detection systems in MANET, *Procedia Computer Science* **151** (2019) 1176–1181.
13. S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay and P. Kar, Wormhole detection based on ordinal MDS using RTT in wireless sensor network, *Journal of Computer Networks and Communications* **2016** (2016) Article ID 3405264.
14. M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei and M. Alazab, A systematic review on clone node detection in static wireless sensor networks, *IEEE Access* **8** (2020) 65450–65461.
15. M. R. Babu and G. Usha, A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET, *Wireless Personal Communications* **90** (2016) 831–845.
16. P. Rani, S. Verma, G. N. Nguyen *et al.*, Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network, *IEEE Access* **8** (2020) 121755–121764.
17. P. S. Chatterjee and M. Roy, Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNS, *IET Wireless Sensor Systems* **8** (2018) 121–128.
18. C. Tang and D. Han, A low resource consumption clone detection method for multi-base station wireless sensor networks, *IEEE Access* **8** (2020) 128349–128361.
19. H. Wen, J. Luo and L. Zhou, Lightweight and effective detection scheme for node clone attack in wireless sensor networks, *IET wireless sensor systems* **1** (2011) 137–143.
20. D. Aneja, L. Kumar and V. Sharma, A cluster based approach for detection and protection of wormhole attack in wireless sensor network, *Sensor Letters* **17** (2019) 955–964.
21. P. Devi and B. Jaison, Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms, *Computer Communications* **152** (2020) 316–322.
22. Z. Duan, X. Wei, J. Han, Y. Lu and L. Shi, Simulated annealing-based reprogramming scheme of wireless sensor nodes, *Wireless Networks* **26** (2020) 495–505.
23. K. Lalitha, R. Thangarajan, S. K. Udgata, C. Poongodi and A. P. Sahu, GCCR: An efficient grid based clustering and combinational routing in wireless sensor networks, *Wireless Personal Communications* **97** (2017) 1075–1095.
24. S. Gomathi and C. G. Krishnan, Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol, *Wireless Personal Communications* **113** (2020) 1775–1790.

25. M. Jeyaselvi and C. Jayakumar, Distributed clone attack detection algorithm using mobility energy prediction in mobile wireless sensor networks, *Sensor Letters* **16** (2018) 965–972.
26. M. A. Merzoug, A. Boukerche, A. Mostefaoui and S. Chouali, Spreading aggregation: A distributed collision-free approach for data aggregation in large-scale wireless sensor networks, *Journal of Parallel and Distributed Computing* **125** (2019) 121–134.
27. D. C. Mehetre, S. E. Roslin and S. J. Wagh, Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust, *Cluster Computing* **22** (2019) 1313–1328.
28. D. S. K. Tiruvakadu and V. Pallapa, Honeypot based black-hole attack confirmation in a MANET, *International Journal of Wireless Information Networks* **25** (2018) 434–448.
29. Q.-V. Pham, S. Mirjalili, N. Kumar, M. Alazab and W.-J. Hwang, Whale optimization algorithm with applications to resource allocation in wireless networks, *IEEE Transactions on Vehicular Technology* **69** (2020) 4285–4297.
30. V. Moonsamy, M. Alazab and L. Batten, Towards an understanding of the impact of advertising on data leaks, *International Journal of Security and Networks* **7** (2012) 181–193.
31. S. Bahrami and M. J. Roorda, Optimal traffic management policies for mixed human and automated traffic flows, *Transportation Research Part A: Policy and Practice* **135** (2020) 130–143.
32. C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir and M. J. Piran, A metaheuristic optimization approach for energy efficiency in the IoT networks, *Software: Practice and Experience* **51**(12) (2020) 2558–2571.
33. P. K. R. Maddikunta, T. R. Gadekallu, R. Kaluri, G. Srivastava, R. M. Parizi and M. S. Khan, Green communication in IoT networks using a hybrid optimization algorithm, *Computer Communications* **159** (2020) 97–107.
34. P. K. R. Maddikunta, G. Srivastava, T. R. Gadekallu, N. Deepa and P. Boopathy, Predictive model for battery life in IoT networks, *IET Intelligent Transport Systems* **14** (2020) 1388–1395.
35. M. Wazid and A. K. Das, A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks, *Wireless Personal Communications* **94** (2017) 1165–1191.
36. O. Moh'd Alia, A dynamic harmony search-based fuzzy clustering protocol for energy-efficient wireless sensor networks, *Annals of Telecommunications* **73** (2018) 353–365.
37. M. Dener and O. F. Bay, Practical implementation of an adaptive detection-defense unit against link layer DOS attacks for wireless sensor networks, *Security and Communication Networks* **2017**.
38. M. Elmonser, H. B. Chikha and R. Attia, Mobile routing algorithm with dynamic clustering for energy large-scale wireless sensor networks, *IET Wireless Sensor Systems* **10** (2020) 208–213.
39. S. Gurung and S. Chauhan, Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET, *Wireless Networks* **25** (2019) 975–988.
40. O. Shree and F. J. Ogwu, A proposal for mitigating multiple black-hole attack in wireless mesh networks.
41. S. Anitha, P. Jayanthi and V. Chandrasekaran, An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks, *Measurement* **167** (2021) 108272.
42. P. Chinnasamy, S. K. Udgata, K. Lalitha and A. Jeevanantham, Multi-objective based deployment of throwboxes in delay tolerant networks for the internet of things environment, *Evolutionary Intelligence* (2020) 1–13.