IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 April 2024, accepted 10 June 2024, date of publication 18 June 2024, date of current version 27 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3416270

RESEARCH ARTICLE

Sinkhole Attack Detection by Enhanced Reputation-Based Intrusion Detection System

FADWA ABDUL-BARI AHMED MOHAMMED[1,2], **NAGHAM E. MEKKY**[1], **HASSAN SOLIMAN**[1], **AND NOHA A. HIKAL**[1]

[1]Department of Information Technology, Faculty of Computers and Information System, Mansoura University, Mansoura 35516, Egypt
[2]Department of Information Technology, Faculty of Engineering, University of Aden, Aden, Yemen

Corresponding author: Fadwa Abdul-Bari Ahmed Mohammed (f.awn@hotmail.com)

ABSTRACT Wireless sensor networks (WSNs) currently play an important role due to their variety of applications in several fields. Improving the overall WSN performance and avoiding its limitations and challenges have become the subject of many researchers. One of the main critical issues is transmitted data security. A sinkhole attack is one of the most dangerous attacks that can be used as a platform for starting several attacks. It has a direct influence on network performance in terms of information confidentiality, integrity, and even availability. An effective method to detect such an attack leads to improving the overall WSN performance as well as enhancing the sent data secrecy. This article introduces an enhanced intrusion detection system (IDS) to protect WSNs from sinkhole attacks. The IDS is modified with a reputation-based mechanism to make it compatible with WSN requirements. An artificial bee colony (ABC) optimization technique is implemented to improve the IDS performance. Noisy channels are added to take into consideration the nature of the WSN. The proposed system achieves more than 97% overall accuracy and a detection rate of 98% with a false positive rate of less than 1.7%, which seems superior to the results of previous works.

INDEX TERMS WSN, sinkhole attack, reputation-based IDS, ABC optimization technique.

I. INTRODUCTION

WSNs currently play an important role due to their various applications in several fields, whether civil or military. Therefore, it is no wonder that they have become the subject of many researchers to improve overall WSN performance and avoid the limitations and challenges. One of the main critical issues in WSNs is data transmission security [1], [2]. Signals are wirelessly transmitted in public, so that they can be captured and/or altered illegibly by an unauthorized agent such as an adversary.

A WSN is defined as a set of small-size, low-cost and resource-constrained nodes, that are known as sensors. The nodes have the capability of sensing, processing, and communicating with each other [3], [4], [5]. There are some node constraints including low computational power, restricted energy resources, and limited memory capacity.

WSNs may be positioned in an aggressive environment and left unattended, which makes this type of network vulnerable to numerous attacks, especially network layer attacks [6]. WSN network layer attacks pose a great threat to network functionality, and these types of attacks can obstruct the normal operation of WSNs. Some examples of such attacks include hello flood, black hole, sinkhole, wormhole, replication, and selective forwarding attacks [6], [7], [8], [9].

One of the famous damaging routing attacks is a sinkhole attack. It causes a serious threat to the WSN due to the nature of the sensor, such as weak computational power and low battery energy. This attack creates wrong information concerning the routing metric, which is subsequently sent to other nodes. Hence, the sinkhole node grabs the attention of the other nodes, and all the sent data will pass through it.

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

According to the false measurements caused by this attack, it can lead to inappropriate dangerous responses and can drain surrounding nodes' energy [5], [10], [11]. The sinkhole attack is an active attack [12] that can alter the sent data or even drop it.

Traditional security methods like encryption and authentication cannot be implemented directly in WSNs. Preventive methods also ultimately fail because of WSN's inherent vulnerabilities; all these reasons make deploying an intrusion detection system as a second line of defense of great importance. An IDS is a system responsible for monitoring a network's activities and can detect any type of undesired malicious activity [13], [14], [15].

Optimization techniques, especially swarm intelligence ones, are broadly applied in WSNs as a result of their optimal calculations and simple operations. These optimization techniques are used in WSNs because of the high dimensionality of WSNs, considering the number of nodes and restrictions regarding power limitations, etc. [16], [17].

A. PROBLEM STATEMENT

WSNs face different routing attacks. Among all routing attack types, sinkhole attacks are considered the most dangerous. Because:

- The sinkhole attack succeeds in directing the attention of the other nodes; hence the sent data will pass through it.
- The sinkhole attack is an active attack that can alter the sent data or drop it.
- The sinkhole attack can be used as a platform for starting several other attacks.

Therefore, there is a great necessity for an efficient detection method to avoid it.

B. CONTRIBUTIONS

The contributions completed in the proposed work are as follows:

- A reputation-based IDS is suggested for detecting a sinkhole attack efficiently.
- The reputation-based IDS is improved using an optimization technique.
- The proposed method takes into consideration the nature of WSN transmission by including noisy channels.
- The proposed method implements the artificial bee colony (ABC) optimization technique for detection due to the nature of WSN transmission.
- The proposed method applies more than one malicious node to test the system performance.
- The experimental results show an enhanced performance of the suggested system compared to that of previous related works.

The paper is organized as follows: section II describes the related topics' background, section III summarizes the related works, and section IV describes the methodology and th design of the proposed syste. The results and discussion are given in section V. Finally, the conclusion is given in section VI.

II. BACKGROUND

This section gives brief ideas about related topics such as WSN security, reputation-based IDS, and the ABC optimization technique.

A. WSN SECURITY AND SINKHOLE ATTACK

WSNs use tiny sensor nodes to sense the physical parameters of the surrounding environment and transmit the sensed data to a base station (BS). WSNs usually use the hierarchical clustering method to save the nodes' energy and prolong the network lifetime. The nodes are arranged into clusters, where each cluster has a cluster head (CH). The nodes inside the cluster communicate with the BS through the CH. The CH manages the nodes' communication, gathers the sensed data, aggregates them, and sends them to the BS. Many protocols are used for organizing the WSN into clusters, the most common one is LEACH [18].

WSNs can be positioned in a hostile environment which makes them vulnerable to different types of attacks. The WSN network layer is subjected to many threats. A sinkhole attack is considered one of the serious network attacks. It magnetizes all neighboring traffic to itself and drops it. This attack leads to a high data loss rate and WSN performance degradation [8], [18], [19].

The sinkhole is an insider attack in which the attacker compromises one of the legitimate network nodes. Then, this compromised node deceives other nodes by injecting false information into the routing information. Th sinkhol attack attracts almost all traffic from neighboring areas by making the compromised node attractive to others [6], [20], [21]. Such an attack disrupts the network.

The sinkhole attack is unpredictable; it has a different execution manner based on the routing protocol used. The compromised sensor node uses the routing metric to deceive its neighbors, as a result, all the data sent from its neighbors will pass through it instead of through the BS [18], [20], [21], [22]. Table 1 lists some technique examples for launching sinkhole attacks.

TABLE 1. Examples of different sinkhole techniques.

Routing Protocol	Sinkhole Technique
MintRoute	Strongest link quality
Tiny AODV	Minimum Number of Hop
DSR	Closer To The Destination
S-LEACH	Highest Energy Advertisement

The sinkhole node has more computational power and energy than other normal nodes. It has planned the situation so that it becomes the candidate CH or the final hop connection to the BS [5], [23].

The sinkhole attack is one of the most dangerous network layer attacks that can be used as a platform for starting several attacks such as wormhole attacks, acknowledged spoofing attacks, selective forwarding attacks etc. [5], [11], [18]. It is an active attack; hence, it has a direct influence on network performance regarding information confidentiality, integrity, and even availability. Therefore, an effective method to detect such an attack leads to improving the overall WSN performance as well as enhancing the sent data secrecy.

B. REPUTATION-BASED INTRUSION DETECTION SYSTEM

The implementation of ordinary security mechanisms cannot be performed directly for WSNs due to resource restrictions, so reputation-based IDS is used. It fits the WSN requirements, overcomes resource limitations, and at the same time provides transferred data confidentiality. It has been considered as an effective method for supporting WSN security [8], [13], [14].

1) INTRUSION DETECTION SYSTEM

An IDS can be defined as a system responsible for detecting, identifying, and responding to illegal or abnormal activities, it is widely used to provide valuable information security [15]. There are two types of IDS based on the detection method used: anomaly-based and signature-based.

Anomaly-based systems define normal users' activity models (behaviors) so that any deviation from these models is classified as anomalous. The advantage of an anomaly-based IDS is that its ability to detect new and unknown types of attacks. The disadvantage of it is that it increases the false positive rate. This type of IDS can be used to detect network layer attacks such as sinkhole attacks [24], [25].

On the other hand, the signature-based system functions with known attacks, using prior prepared models (signatures) of those attacks to recognize the intruder. The advantage of a signature-based IDS is that it does not increase the false positive rate like that anomaly-based IDS. The disadvantage of it is that it cannot detect new and unknown types of attacks. It can be used to detect well known attack patterns such as physical layer (jamming attacks).

Unfortunately, some errors negatively affect the performance of the IDS, these errors are false positive errors (FPE) and false negative errors (FNE). FPE occurs when the IDS misclassifies normal packets or activities and considers them attacks. On the other hand, FNE occurs when IDS considers an attack a normal activity [24], [25].

2) TRUST AND REPUTATION

Trust is the ability to precisely forecast another's behavior whereas reputation is not a forecast of the future, bu rather the familiarity of the past. Recently, trust and reputation techniques have been added to IDSs for WSNs to detect malicious node behaviors. A reputation-based system is a system that uses direct and indirect observations to calculate the trust value of a particular network node, whereas a trust-based system builds the trust value based on direct observation without any previous knowledge about the node's behavior [13], [26].

In the trusted-based system, the trust value of a node is calculated according to the deviations of key parameters at a specific protocol layer, because an attack impacts the protocol's parameters.

The nodes monitor other nodes' activity and observe any deviation. Based on the deviations of the parameters, the trust value can be evaluated and sent to the CH or BS. If the trust value is less than a predefined threshold value, then the node is considered abnormal [12], [13].

In the reputation-based system, attack detection requires a cooperative system that uses mutual trust calculations between all nodes. The trust values are calculated by concerning the direct trust and indirect trust evaluations [14], [26].

C. ARTIFICIAL BEE COLONY (ABC) OPTIMIZATION TECHNIQUE

An optimization method can be defined as the procedure of choosing the finest possible solution from the data that are obtained during the experimental process. Hence, for given optimized problem, there are various candidate solutions, these solution are then compared and balanced according to the required objective function [27]. Optimization techniques are used to find the maximum or minimum solution for a given problem. They are used for the detection problem because this process tries to find suspicious entities that minimize the total trust of a given system.

The ABC algorithm is one of the optimization techniques, it is considered as a swarm-based metaheuristic algorithm. The idea of this algorithm was motivated by the smart behavior of honey bees while they were looking for a food source [28]. There are three types of bees in the ABC based on their occupations; they are employed bees, onlooker bees, and finally scout bees. Each employed bee has one food source, whereas the onlooker bees watch the employed bees dance to pick a rich food source, the scout bees search for food sources randomly. The onlooker and scout bees are called unemployed bees.

There are three main components of ABC: employed bees, unemployed bees, and food sources. The employed and unemployed bees keep looking for rich food sources that are closest to their hive. First, all the food source locations are randomly discovered. Next, food source nectar is exploited by the employed bees with the help of onlooker bees; this process continues until ultimately the food resources become exhausted. Then, these exhausted sources are replaced by new ones randomly by scout bees.

In ABC, a food source position is considered as a possible problem solution. The amount of nectar in the food source represents the quality (fitness) of the given solution. The number of employed bees and the number of food sources are equal [16], [17], [28]. The pseudocode for ABC is shown in Table 2.

The artificial bees determine a population of initial solutions randomly and then develop them iteratively by implementing two strategies: moving toward improved solutions by a neighbor exploration mechanism and canceling the poor ones.

To apply ABC for sinkhole detection, first, the given problem must be converted to the situation of searching for the best possible solution (which contains the suspicious node ID) that minimizes the objective cost function (the total trust value in our case) and hence maximizes the fitness value.

TABLE 2. ABC pseudocode.

```
The Pseudocode for ABC
Input: Objective Function, Colony Size, Solution Number, Limit, and Maximum Iteration Number.

Initialize a random population of solutions within the colony size.
For each solution:
        •  Evaluate the Objective function.
        •  Compute the Fitness value.
Set the Trail counter of all solutions to zero.
    For t=1 to Maximum Iteration Number
        •  Perform the Employed Bee Phase for every solution.
        •  Calculate the probability for every food source.
        •  Perform the Onlooker Bee Phase to update some solutions.
        •  Memorize the best solution ever found.
        •  If Trail of any solution > Limit
              Perform the Scout Bee Phase for every unimproved solution.
              Replace the unimproved solutions.
        •  End if.
    End for

Output: best possible solution.
Note: the solution is equivalent to the food source
```

III. RELATED WORKS

Table 3 gives a brief summary about the related previous works for detecting sinkhole attacks. It lists the different methodologies used and the experimental results.

IV. METHODOLOGY AND DESIGN SYSTEM

The proposed work uses the trust-based strategy at nodes and the reputation-based IDS at the BS to detect sinkhole attacks. Every node computes the trust value of the neighboring nodes based on the consumed energy. Then, it sends that value to the CH. The CH checks whether there is an aggregation of that trust value for a particular node. After that, the CH sends this node trust value to the BS. The BS decides which node is a sinkhole by implementing the ABC algorithm. The BS uses the indirect trust value (reputation) from other nodes and uses its direct trust value based on traffic observations.

The proposed system is built based on monitoring WSN nodes' activities, building a trust matrix, and using a reputation strategy.

The ABC optimization technique is chosen among all other optimization techniques because it has some advantages, such as simplicity and flexibility in execution, due to the use of fewer control parameters compared to other techniques. It is based on basic mathematical and logical operations. ABC's efficiency lies in its ability to deal with stochastic nature objective functions. The optimal solution is obtained through a combination of several processes: cooperative operations in the employed bees phase, random calculations in the onlooker bees phase, and exploration of the search area in the scout bees phase.

The ABC optimization technique is used to enhance the detection process due to the nature of WSN transmission. Figure 1 illustrates the flowchart of the proposed algorithm.

A. NETWORK SCENARIO

The Sectored-LEACH (S-LEACH) routing protocol [3] was used with the proposed method. S-LEACH is an enhanced LEACH that increases the network lifetime and reduces overall energy consumption. The S-LEACH idea is dividing the communication area into sectors so that the transmission distance decreases, which leads to a reduction in the consumed nodes' energy. The S-LEACH has two phases, the setup phase and the steady state phase, the first phase is concerned with the next CH selection, and the second phase is related to transmitting sensed data to the C. The CH election process inside each sector relies on the nodes' residual energy. Each node sends its residual energy and a random number to all the other nodes within the same sector. The node that has the highest energy is directly chosen as the next CH, and the random number is used in the situation of energy equivalence.

The use of S-LEACH facilitates IDS implementation since every node declares its residual energy for the CH election process, in addition, dividing the communication area into sectors simplifies the detection process and reduces the detection time due to the small size of the monitored area.

B. EXPERIMENTAL ENVIRONMENT

The proposed method was achieved in MATLAB R2019a. A description of the experimental parameters is given in Table 4.

The proposed method considered the existence of noisy channels such that three noisy channels were applied randomly during WSN rounds and packet delivery failure occurred without an attack.

C. SINKHOLE ATTACK IMPLEMENTATION AND IDENTIFICATION

The sinkhole attack is applied in S-LEACH as follows: the compromised node sends a message to all other nodes within the same sector during the setup phase. The message declares that this node has the maximum energy so that it becomes the next CH according to the S-LEACH routing protocol [3],

TABLE 3. Previous works on sinkhole attack detection.

Authors, and Ref. No.	Routing Protocol	Number of Normal Nodes	Number of Sinkhole Nodes	Detection Method	Detection Rate	False Positive Rate
A. Bilal et al. [29] in 2022	Key Management Protocol	122	32	Anomaly-based Detection system based on Messages Exchange	94.86%	1.4%
R. Dhanaraj et al. [30] in 2021	Dynamic Source Routing	50–150	Not Given	Hybrid Detection Model Proportional Coinciding Score (PCS) is applied and the MK-Means algorithm	90%	Not Given
N. Al-Maslamani and M. Abdallah [23] in 2020	LEACH	100 - 1000	1	Weight Estimation and ABC algorithm	93% for 10 iterations 96.7% for 50 iterations 99.5% for 100 iterations	Not Given
K. Singh and A. Verma [31] in 2020	OLSRv2	50	10	A multi-criteria fuzzy system based on the node's behavior (fuzzy c-means Classification)	95%	Not Given
Z. Zhang et al. [32] in 2019	LEACH	100	1	Frequency of Attack occurrence, Optimal hops Number and Dynamic Programming	96.85%	4.33%
U. Ghugar et al. [33] in 2019	AODV	50	1–10	Trust-based IDS Statistical method (average and deviation)	96.83%	6.66%
N. Nithiyanandam et al. [21] in 2018	AODV	50-250	5-25	Hash Table, Voting Method, and Enhanced Particle Swarm optimization technique	94.63%	4.39%
J. Wang et al. [34]in 2017	AODV	50	1-10	Trust-based IDS and t-distribution to derive the results	95.53%	8.33%

[35]. Hence, in this proposed work, the energy consumption factor is taken to identify malicious activity at the node level [8], [14], [36]. Figure 2 displays the sinkhole attack implementation.

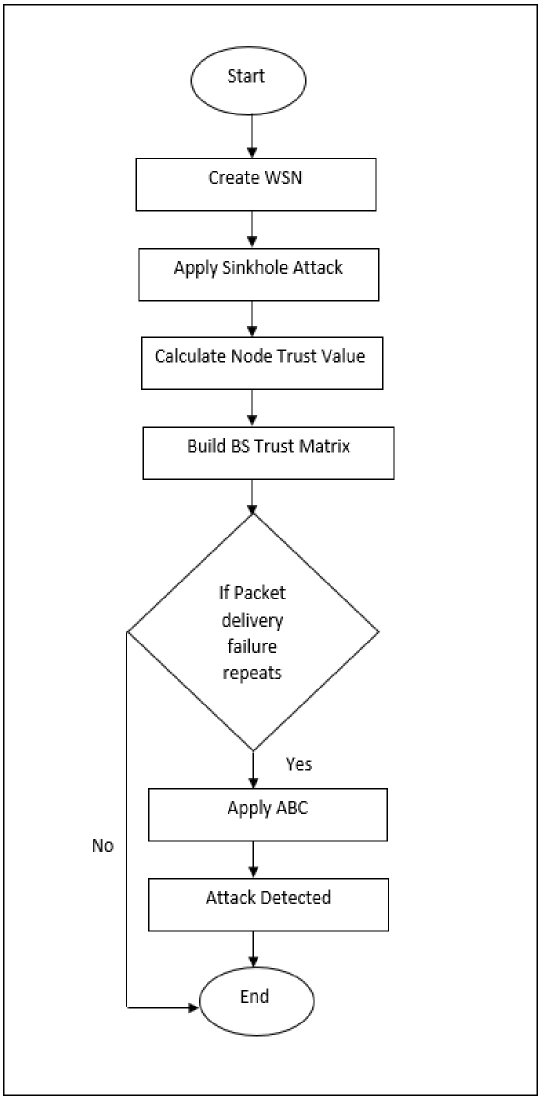

FIGURE 1. The proposed algorithm flowchart.

In Figure 2, the CH is represented by the X sign, and the data transfer to the CH is represented by the lines inside the cluster. The isolated nodes send the data directly to the BS. The BS is located at the center. The sectors' nodes are represented by different symbols, such that a distinct symbol is allocated for each sector. The circles represent sector 1 nodes, the stars represent sector 2 nodes, and so on [3]. The dashed lines denote the data transfer from CHs to the BS. A malicious node is represented by a red square shape. The malicious node is selected as th CH, so, there is no longer data transfer to the BS.

D. CONSTRUCTING REPUTATION-BASED IDS

To construct the reputation-based IDS, the trust value must be calculated first at the node level, and then sent to the BS. Second, the BS builds the trust matrix. Finally, ABC is applied at the BS if there is a suspicion of an attack occurring.

TABLE 4. Simulation parameters.

Parameter	Value
WSN Area	100m * 100m
Data Size	4000 bit
Routing Packet Size	100 bit
Initial Energy	0.5 j
BS Location	(50,50)
Bit Transmitting Energy	$50*10^{-9}$ j
Bit Receiving Energy	$50*10^{-9}$ j
Free Space Model Energy	$10*10^{-12}$ j
Amplification Energy	$0.0013*10^{-12}$ j
Data Aggregation Energy	$5*10^{-9}$ j
Nodes	50,100,150
Malicious Nodes	1, 20% of the Number of Nodes
Rounds	20
Noisy Channels	3
Routing Protocol	S-LEACH

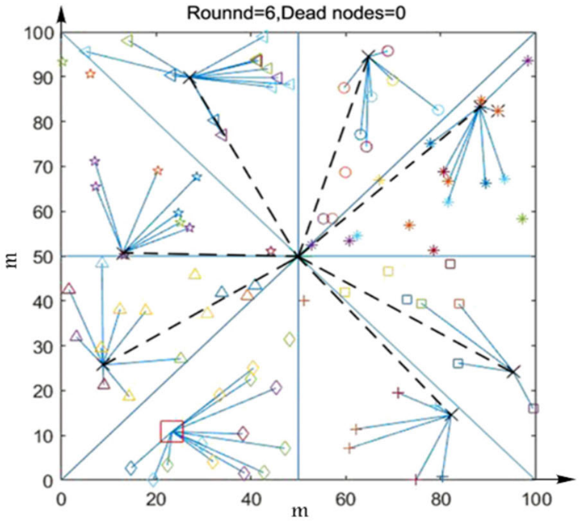

FIGURE 2. Sinkholeattack implementation.

The proposed system is implemented in two stages: the node level stage and the BS level stage.

1) CALCULATING THE NODE TRUST AT THE NODE LEVEL

The node energy consumption (Ec) is taken as a parameter to calculate the trust value. At the time interval (Δt), node j computes the energy consumed by neighbor node k. The Ec of node k has a relative deviation RD_{Eck} and is computed by (1) [33], [34], [37]:

$$RD_{Eck} = \frac{\Delta E_{ck}(t) - \Delta E_c(t)}{\Delta E_c(t)} \tag{1}$$

where:

ΔEck(t) is node k energy consumed during Δt i.e., ΔEck(t) = Eck(t) - Eck(t-1), such that Eck(t) is node k remaining energy at time t.

ΔE_c (t) is the average energy consumed by node j neighbors in the same sector at time t. It is computed by (2), where n is the number of j neighbors in the same sector:

$$\Delta E_c\,(t) = \frac{1}{n}\sum\nolimits_{k=1}^{n} E_{ck}\,(t) \tag{2}$$

The Trust Node Value is computed by (3) as follows:

$$\mathit{Trust\ Value\ of\ Node\ k} = \begin{cases} 1, & \mathit{if}\ RD_{ECK} > \mathit{Thresold} \\ -1, & \mathit{otherwise} \end{cases} \tag{3}$$

In Trust Value equation 3, if the $\mathrm{RD_{Eck}}$ of node k is greater than the threshold value, then node k is trustworthy and has the default trust value which is 1. If the $\mathrm{RD_{Eck}}$ of node k is less than or equal to the threshold value, then node k is untrusted and is considered a maliciou node, thus, its trust value is −1.

2) CALCULATING THE FINAL NODE TRUST VALUE AT THE BASE STATION LEVEL

The BS creates its own trust matrix for the network nodes. It consists of the node ID, sector number, node direct trust value, repetition of packet delivery failure, and indirect node trust value (reputation). The direct trust node value is computed based on the observation of packet delivery at the BS. Every node has a default trust value of one, each time the packet delivery fails, this value decreases by 0.1. Whereas the repetition of packet delivery failure for each node has a default value of zero and whenever the packet delivery fails, it increases by 1. Table 5 shows a sample of the BS Trust Matrix.

TABLE 5. A sample of BS trust matrix.

Nod e ID	Value	Sect or	Repetitio n	Reputatio n
1	1	1	0	1
2	-0.90	8	19	-1
3	0.90	4	1	1
4	1	7	0	1
5	-0.90	1	19	-1
6	1	8	0	1
7	1	3	0	1
8	0.90	4	1	1
9	1	8	0	1
10	1	1	0	1

As shown in Table 5, nodes 2 and 5 are malicious nodes. The direct trust value is -0.9 for both nodes because the repetition of packet delivery failure is repeated 19 times. The reputation value that is sent by other nodes is −1 for both nodes. On the other hand, nodes 3 and 8 are genuine nodes. The direct trust value is 0.9 because the packet delivery failure occurs only once due to a noisy channel. The reputation that is sent by other nodes is 1.

E. IMPLEMENTING THE ABC OPTIMIZATION TECHNIQUE FOR SINKHOLE DETECTION

The ABC is applied at the BS when the packet delivery failure repeats. To detect a sinkhole attack, ABC looks for a solution that minimizes the objective function and maximizes the fitness value. Table 6 describes the parameters used.

TABLE 6. ABC parameters.

Parameter	Value
Colony Size	Number of Nodes
Number of Food Sources	Colony Size /2
Number of Employed Bees	Colony Size /2
Abandonment Limit	Colony Size /2
Solution Dimension	Number of Malicious Nodes
Number of iterations	100

The ABC optimization technique starts by setting initial food sources (solution) randomly provided that they are within the colony size limits, every employed bee has one food source. After that, the employed phase begins. For every bee, a partner is chosen randomly to update the food source. When the new food source is updated, the objective and fitness functions are computed. Then, a greedy search occurs to ensure that the newly updated food source is better than the previous one. If there is no enhancement, the employed bee preserves the old source, otherwise, the new source is considered.

The objective function calculates the sum of the final trust values for a given solution by using (4).

$$OF = \sum\nolimits_{j=1}^{n} FT_j \tag{4}$$

given that:

$$\mathrm{FT_j = w_1DTV_j + w_2ITV_j} \tag{5}$$

where:

OF is the objective function

n is the number of elements in a given solution

$\mathrm{FT_j}$ is node j final trust value

$\mathrm{DTV_j}$ is node j direct trust value

$\mathrm{ITV_j}$ is node j indirect accumulated trust value

w_1 *and* w_2 are the weight parameters, the values of the individual parameters $w \in [0\ 1]$; and $w_1 + w_2 = 1$.

After calculating the objective function, the fitness value is computed for the employed bee according to (6).

$$Fit_{d=} \begin{cases} \dfrac{1}{1+OF_d}; & OF_d \geq 0 \\ 1+|OF_d|\,; & \mathit{otherwise} \end{cases} \tag{6}$$

where $\mathrm{Fit_d}$ is the fitness value for solution d.

In ABC, the relation between the objective function and fitness value is inversely propagated, when the objective function decreases the fitness value increases. The onlooker phase takes place after the employed phase, and the probability for every solution is calculated by (7).

$$\mathrm{Prob_d} = \frac{Fit_d}{\sum_{b=1}^{nb} Fit_b} \tag{7}$$

where:

$\mathrm{Prob_d}$ is solution d probability

$\mathrm{Fit_d}$ is solution d fitness value

nb is the number of solutions

Some solutions are updated in the onlooker phase based on their probability and a random number r, such that r ∈ [−1, 1]. If the solution probability is less than r, then the solution is updated [28]. If a given solution is no longer improved concerning the limit value, then the scout bee phase starts. In this phase, a new random solution is generated within the colony limit and no greedy search is applied.

V. RESULTS AND DISCUSSION

This section describes an analysis of sinkhole attack occurrence and detection in WSNs with various numbers of nodes (50, 100, and 150) and different numbers of malicious nodes (1, 10, 20, and 30). The performance metrics used to evaluate sinkhole attack detection include packet loss, overall accuracy, detection rate, and false positive rate. The experiment was conducted for 20 rounds. The results were collected and averaged.

A. PACKET LOSS

A sinkhole attack attracts the nodes to send their sensed data toward it and then drops it. The attacking node does not forward the data to the BS. This process affects the throughput of the WSN. The total number of packets received by the BS clearly decreased after the sinkhole attack was implemented. Figure 3 illustrates the number of packet losses after different sinkhole attacks.

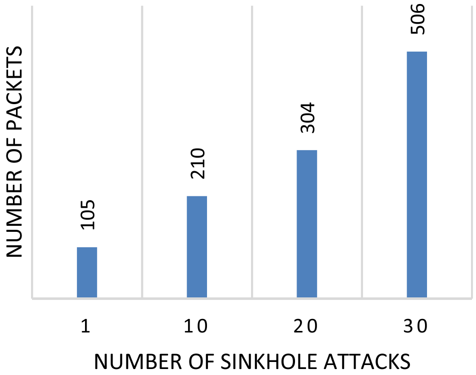

FIGURE 3. The number of packet losses.

It is clear from Figure 3 that when the number of sinkhole attacks increases, the number of packet losses also increases, which means that the total number of packets sent to the BS decreases. This can lead to bad effects on WSN performance and can cause great damage due to the loss of gathered information.

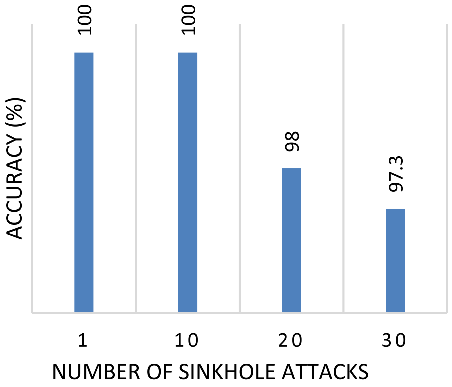

FIGURE 4. Average overall accuracy.

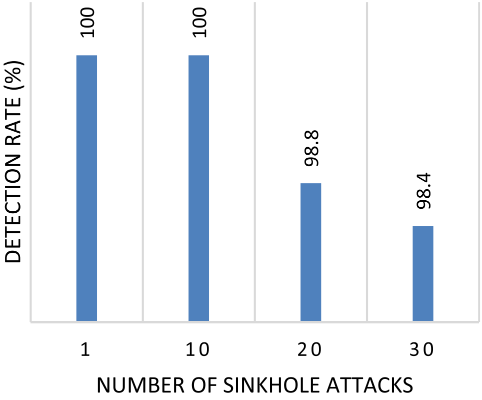

FIGURE 5. Average detection rate.

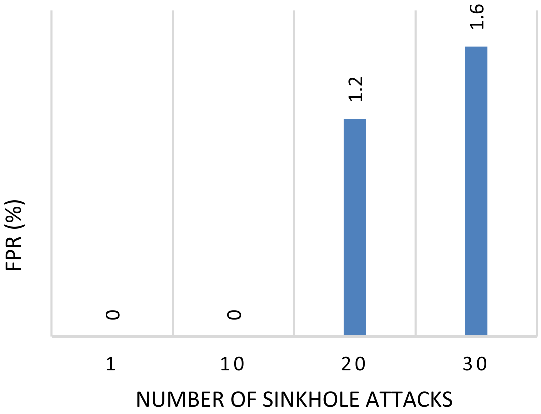

FIGURE 6. Average FPR.

B. OVERALL ACCURACY

Overall accuracy is the percentage of the actually classified nodes (whether they are normal or attackers) relative to the total number of nodes, i.e., the percentage of the sum of the true negatives and true positives divided by the total number of nodes. It is calculated by:

accuracy = (correctly classified nodes/ number of all nodes) ∗100

Figure 4 illustrates the average overall accuracy values of the proposed system for different numbers of sinkhole attacks.

The results show that the proposed system performs well such that the overall accuracy is high when different numbers of attackers and deployed nodes are used. The proposed system was tested with one sinkhole attack from 100 nodes and 20% attackers with different node numbers, i.e. 50,100, and 150. When the number of attackers and deployed nodes increases, the overall accuracy decreases.

C. DETECTION RATE

The detection rate or true positive rate (TPR) is the percentage of the number of attacks detected by the IDS to the number of all attacks that happened in the WSN. It is obtained by:

Detection rate = (number of attacks detected / total number of attacks presented) ∗ 100.

Figure 5 shows the average detection rates of the proposed system for different numbers of sinkhole attacks.

The detection rate is significant for measuring the performance of th IDS. Again, the proposed system was tested with different numbers of attackers and deployed nodes. The system performs well based on the obtained results. The detection rate generally reached high values. When the number of attackers and nodes increases, the detection rate decreases.

D. FALSE POSITIVE RATE (FPR)

WSNs gather continuous data on the monitored area to analyze them and make an accurate and fast decision. The false positive rate is significant for WSN performance. It describes the case in which a system fails to classify normal activities. An increase in the FPR causes a lack of gathered information and can disrupt the normal functionality of the network. It leads to generating inaccurate responses. High false positive rate values lead to a shortage in the monitored activities, resulting in wrong responses and significant damage.

The FPR is the percentage of normal nodes that are detected as attackers, and is calculated as follows:

FPR = Number of normal nodes wrongly categorized as attackers (false positive error) / total number of actual normal nodes. Figure 6 shows the average FPRs of the proposed system for different numbers of sinkhole attacks.

The FPR is essential for WSN performance. It is important to have small FPR values to maintain good performance. It is obvious from the results that the proposed system has low FPR values for different numbers of nodes and attackers.

E. COMPARISON WITH PREVIOUS WORKS

Table 7 summarises the key differences and improvements of the proposed method compared to the previous works. Figures 7 and 8 illustrate a comparison between the proposed work and related works concerning the detection rate

TABLE 7. Key differences of the proposed method compared to the previous works.

Authors, and Ref. No	Number of Attacks	Differences	Improvements of The Proposed Method
N. Al-Maslamani and M. Abdallah [23] Z. Zhang et al. [32]	1	Use only one attack Do not consider noisy channel	Add more attacks Take into consideration noisy channels Better detection rate Less false positive rate
K. Singh and A. Verma [31] U. Ghugar et al. [33] J. Wang et al. [34]	10	Do not consider noisy channel Use of trust–based IDS	Add more attacks Take into consideration noisy channels Use of both trust-based at nodes and reputation-based IDS at the BS Better detection rate Less false positive rate
N. Nithiyanandam et al. [21]	20	Do not consider noisy channel	Add more attacks Take into consideration noisy channels Better detection rate Less false positive rate
A. Bilal et al. [29]	30	Do not consider noisy channel Use of Anomaly-based IDS	Add more attacks Take into consideration noisy channels Use of a reputation-based IDS at the BS Better detection rate

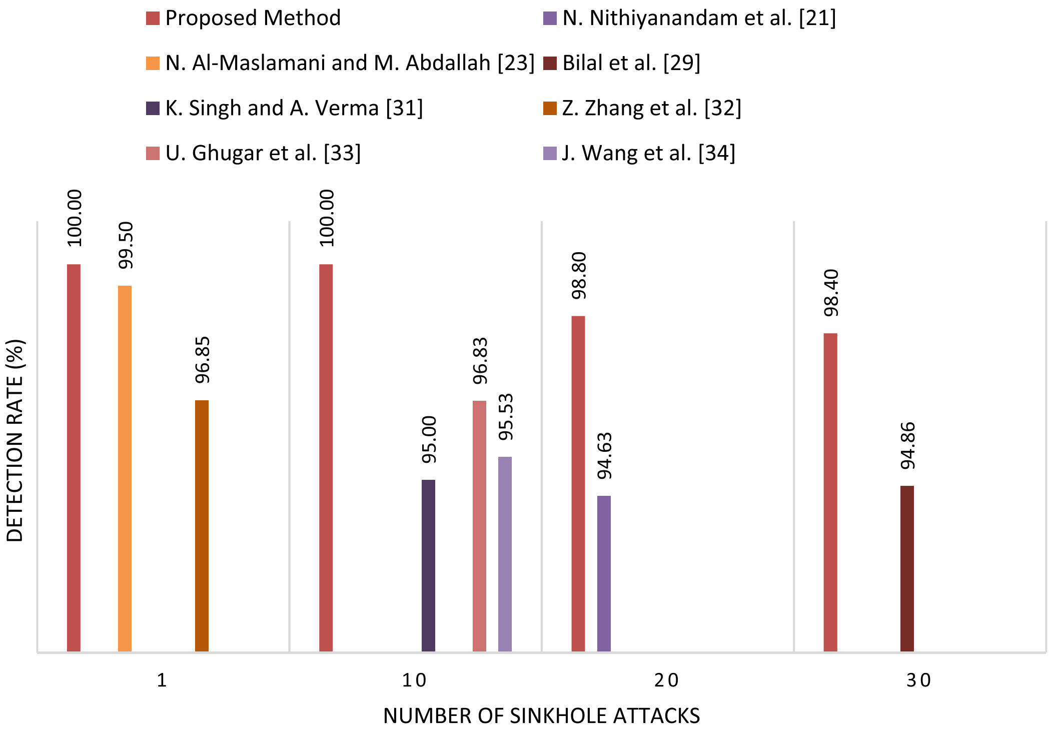

FIGURE 7. Detection rate comparison.

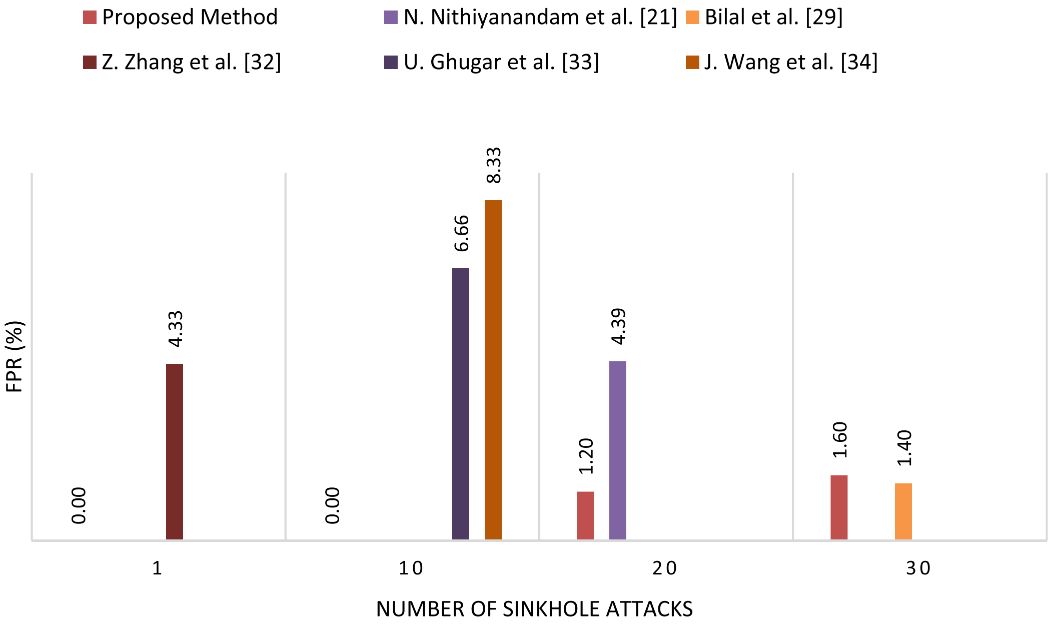

FIGURE 8. FPR comparison.

and false positive rate. Obviously, the proposed method outperforms the others.

Based on the obtained results and the previous works given in Table 3, for one sinkhole detection, the average detection rate is 100% and the FPR is 0%.

The proposed system achieves a better average detection rate than Al-Maslamani and Abdallah [23] where the average detection rate is 99.5%. The proposed method also achieves a better average detection rate and lower FPR compared with Zhang et al. [32] in which the average detection rate is 96.85% and FPR is 4.33%.

For 10, 20, and 30 sinkhole attack detections, the average detection rates are 100%, 98.8%, and 98.4%, respectively, and the corresponding FPRs are 0%, 1.2%, and 1.6%. The proposed system achieves better results regarding the average detection rate than Bilal et al. [29], Singh and

Verma [31], Ghugar et al. [33], Nithiyanandam et al. [21], and Wang et al. [34], where the average detection rates are 94.86%, 95%, 96.83%, 94.63%, and 95.53%, respectively. The proposed system also achieves better results regarding the FPR compared with Ghugar et al. [33], Nithiyanandam et al. [21], and Wang et al. [34], where the FPRs are 6.66%, 4.39%, and 8.33%, respectively.

VI. CONCLUSION

WSNs are potentially subject to a variety of vulnerabilities due to the nature of data transmission. Sent data security needs to be maintained. For that purpose, a reputation-based IDS was proposed. It seemed suitable for detecting intruders and insider malicious nodes for further measures to prevent them. The use of an IDS was modified with a reputation-based mechanism to make it compatible with the WSN requirements in addition to the implementation of the ABC optimization technique to enhance the IDS performance. The use of an optimization technique was appropriate to WSN requirements and activities.

The proposed system tried to address the limitations of existing methods by implementing more than one attack and different numbers of deployed nodes. It performed an enhancement in the detection process by implementing a trust-based strategy at the nods level based on simple operations to conserve nodes' energy besides a reputation-based strategy at the BS with a combination of ABC optimization technique for improving the accuracy of the detection process. Furthermore, noisy channels were added to simulate reality and distinguish real sinkhole attacks.

The results showed an enhancement regarding the security metrics such as overall accuracy and detection rate. The experimental results also showed a reduction in the false positive rate. The proposed system was superior to those of previous works, as obtained from the results.

Although the results of the proposed work were good, the proposed work has some limitations. This work was designed only for static sensor nodes; it is not suitable for mobile sensor nodes. The accuracy of the detection method might be affected by the use of the optimization technique.

In future work, node mobility can be taken in consideration when implementing the proposed system. Additionally, the proposed system can be expanded toward detecting other types of attacks such as bad-mouthing at the node level, where malicious nodes may send invalid trust values, and the possibility of applying blackhole or wormhole attack. Prevention methods can also be considered for further enhancement.

REFERENCES

[1] A. Potnis and C. S. Rajeshwari, "Wireless sensor network: Challenges, issues and research," in *Proc. Int. Conf. Future Comput. Technol.*, 2015, pp. 224–228, doi: 10.17758/ur.u0315268.

[2] U. Farooq, "Wireless sensor network challenges and solutions," Tech. Rep., 2019, doi: 10.13140/RG.2.2.22191.59043.

[3] F. A. B. Mohammed, N. Mekky, H. H. Suleiman, and N. A. Hikal, "Sectored LEACH (S-LEACH): An enhanced LEACH for wireless sensor network," *IET Wireless Sensor Syst.*, vol. 12, no. 2, pp. 56–66, 2022, doi: 10.1049/wss2.12036.

[4] A. Khalifeh, H. Abid, and K. A. Darabkh, "Optimal cluster head positioning algorithm for wireless sensor networks," *Sensors*, vol. 20, no. 13, p. 3719, Jul. 2020, doi: 10.3390/s20133719.

[5] A. D. Bello and O. S. Lamba, "How to detect and mitigate sinkhole attack in wireless sensor network (WSN)," *Int. J. Eng. Res.*, vol. 9, no. 5, pp. 98–105, May 2020, doi: 10.17577/IJERTV9IS050099.

[6] K. Avila, P. Sanmartin, D. Jabba, and J. Gomez, "An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN," *Wireless Pers. Commun.*, vol. 122, no. 4, pp. 3687–3718, Feb. 2022, doi: 10.1007/s11277-021-09107-6.

[7] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues," *Electronics*, vol. 10, no. 19, p. 2365, Sep. 2021, doi: 10.3390/electronics10192365.

[8] N. Dharini, N. Duraipandian, and J. Katiravan, "ELPC-trust framework for wireless sensor networks," *Wireless Pers. Commun.*, vol. 113, no. 4, pp. 1709–1742, Aug. 2020, doi: 10.1007/s11277-020-07288-0.

[9] E. Sula, "A review of network layer and transport layer attacks on wireless networks," *Int. J. Mod. Eng. Research.*, vol. 8, pp. 23–27, Dec. 2018. [Online]. Available: www.ijmer.com

[10] M. Nagaraj and R. Srinath, "Hybrid ant colony optimization for sinkhole detection in WSN," *Int. Res. J. Eng. Technol.*, vol. 8, no. 6, pp. 1022–1027, Jun. 2021. [Online]. Available: www.irjet.net

[11] S. Padmanabhan, R. Maruthi, and R. Anitha, "An experimental study to recognize and mitigate the malevolent attack in wireless sensors networks," *Global Transitions Proc.*, vol. 3, no. 1, pp. 55–59, Jun. 2022, doi: 10.1016/j.gltp.2022.04.013.

[12] J. He and F. Xu, "Research on trust-based secure routing in wireless sensor networks," *J. Phys., Conf.*, vol. 1486, Apr. 2020, Art. no. 022052, doi: 10.1088/1742-6596/1486/2/022052.

[13] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, 2017, pp. 1–6.

[14] T. Abdellatif and M. Mosbah, "Efficient monitoring for intrusion detection in wireless sensor networks," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 15, p. e4907, 2020, doi: 10.1002/cpe.4907.

[15] A. Jain, V. Jain, and K. Tripathi, "Trust based intrusion detection system architecture for WSN," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 6, pp. 700–703, Mar. 2020.

[16] S. Amaran, "Differential evolution with artificial bee colony optimization algorithm based sink hole detection in wireless sensor networks," *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 5, pp. 1761–1767, May 2020, doi: 10.30534/ijeter/2020/44852020.

[17] N. Nithiyanandam and P. Latha, "Artificial bee colony based sinkhole detection in wireless sensor networks," *J. Ambient Intell. Humanized Comput.*, pp. 1–14, Jul. 2019, doi: 10.1007/s12652-019-01404-0.

[18] S. R. Kumar, M. Thalaimalaichamy, and A. Umamakeswari, "Analysis of sinkhole attack in LEACH based wireless sensor network," *Int. J. Pure Appl. Math.*, vol. 116, no. 24, pp. 185–197, 2017. [Online]. Available: http://www.ijpam.eu

[19] N. Sidhu and M. Sachdeva, "Impact analysis of network layer attacks in real-time wireless sensor network testbed," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 8, 2020, doi: 10.14569/ijacsa.2020.0110885.

[20] M. Ali, M. Nadeem, A. Siddique, S. Ahmad, and A. Ijaz, "Addressing sinkhole attacks in wireless sensor networks—A review," *Int. J. Sci. Technol. Res.*, vol. 9, no. 8, pp. 406–411, Aug. 2020.

[21] N. Nithiyanandam, D. P. L. Parthiban, and B. Rajalingam, "Effectively suppress the attack of sinkhole in wireless sensor network using enhanced particle swarm optimization technique," *Int. J. Pure Appl. Math.*, vol. 118, no. 9, pp. 313–329, 2018.

[22] R. Stephen and D. L. Arockiam, "An enhanced technique to detect sinkhole attack in Internet of Things," *Int. J. Eng. Res. Technol.*, vol. 5, no. 13, pp. 1–4, 2017.

[23] N. Al-Maslamani and M. Abdallah, "Malicious node detection in wireless sensor network using swarm intelligence optimization," in *Proc. IEEE Int. Conf. Inform., IoT, Enabling Technol.*, Feb. 2020, pp. 219–224.

[24] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy and survey of intrusion detection system design techniques," 2018, *arXiv:1806.03517*.

[25] K. A. A. Omer and F. A. Awn, "Performance evaluation of intrusion detection systems using ANN," *Egyptian Comput. Sci. J.*, vol. 39, no. 4, pp. 32–42, 2015.

[26] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (FANETs)," *Int. J. Commun. Syst.*, vol. 31, no. 6, p. e3517, Apr. 2018, doi: 10.1002/dac.3517.

[27] N. P. Raut, A. B. Kolekar, and S. L. Gombi, "Optimization techniques for damage detection of composite structure: A review," *Mater. Today, Proc.*, vol. 45, pp. 4830–4834, Jan. 2021, doi: 10.1016/j.matpr.2021.01.295.

[28] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: Artificial bee colony (ABC) algorithm," *J. Global Optim.*, vol. 39, no. 3, pp. 459–471, Oct. 2007, doi: 10.1007/s10898-007-9149-x.

[29] A. Bilal, S. M. N. Hasany, and A. H. Pitafi, "Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices," *IET Commun.*, vol. 16, no. 8, pp. 845–855, May 2022, doi: 10.1049/cmu2.12385.

[30] R. K. Dhanaraj, L. Krishnasamy, O. Geman, and D. R. Izdrui, "Black hole and sink hole attack detection in wireless body area networks," *Comput., Mater. Continua*, vol. 68, no. 2, pp. 1949–1965, 2021, doi: 10.32604/cmc.2021.015363.

[31] K. Singh and A. K. Verma, "TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks," *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3173–3196, Oct. 2020, doi: 10.1007/s11277-020-07523-8.

[32] Z. Zhang, S. Liu, Y. Bai, and Y. Zheng, "M optimal routes hops strategy: Detecting sinkhole attacks in wireless sensor networks," *Cluster Comput.*, vol. 22, no. S3, pp. 7677–7685, May 2019, doi: 10.1007/s10586-018-2394-6.

[33] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, "LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–13, Jan. 2019, doi: 10.1155/2019/2054298.

[34] J. Wang, S. Jiang, and A. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors*, vol. 17, no. 6, p. 1227, May 2017, doi: 10.3390/s17061227.

[35] L. Panigrahi, "A trust based clustering routing scheme to enhance the security of WSNs," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, no. 9, pp. 1113–1121, Jul. 2019.

[36] X. Jin, J. Liang, W. Tong, L. Lu, and Z. Li, "Multi-agent trust-based intrusion detection scheme for wireless sensor networks," *Comput. Electr. Eng.*, vol. 59, pp. 262–273, Apr. 2017, doi: 10.1016/j.compeleceng.2017.04.013.

[37] U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, and S. K. Panda, "PL-IDS: Physical layer trust based intrusion detection system for wireless sensor networks," *Int. J. Inf. Technol.*, vol. 10, no. 4, pp. 489–494, Dec. 2018, doi: 10.1007/s41870-018-0147-7.

FADWA ABDUL-BARI AHMED MOHAMMED received the B.S. and M.S. degrees (Hons.) in information technology engineering from the University of Aden, Yemen in 2007 and 2014, respectively. She is currently pursuing the Ph.D. degree in information technology with the Faculty of Computer and Information Systems, Mansoura University, Egypt.

She is a Lecturer with the Department of Information Technology, Faculty of Engineering, University of Aden. Her research interests include information technology, with a special focus on information security technology and wireless sensor networks.

NAGHAM E. MEKKY received the B.Sc., M.Sc., and Ph.D. degrees in electronics engineering from Mansoura University, Mansoura, Egypt.

She was a Researcher with the Department of Electronics Communication Engineering, Mansoura University, for seven years, before joining the Misr Higher Institute for Engineering and Technology, Mansoura, in 2007, as an Assistant Lecturer. She is currently an Assistant Professor with the Department of Information Technology, Faculty of Computers and Information Systems, Mansoura University. Her research interests include image processing, semantic web, the IoT, and biomedical engineering.

HASSAN SOLIMAN received the B.Sc., M.Sc., and Ph.D. degrees in electronics and communications engineering from the Faculty of Engineering, Mansoura University, Mansoura, Egypt, in 1983, 1987, and 1993, respectively. From 2000 to 2012, he was an Associate Professor with the Faculty of Engineering, Mansoura University, where he has been a Professor and the Dean of the Faculty of Computer and Information Systems (FCIS), since 2012 and 2016, respectively. He is currently a Professor with the Information Technology Department, Faculty of Computers and Information, Mansoura University. He has authored/coauthored over 50 research publications in peer-reviewed reputed journals, book chapters, and conference proceedings. He advised more than 20 master's and Ph.D. graduates. His current research interests include semantic web, pattern recognition, computer networking, computer security, medical image analysis, and machine learning.

NOHA A. HIKAL received the B.Sc. and M.Sc. degrees in communications engineering from Mansoura University, in 1998 and 2002, respectively, and the Ph.D. degree in multimedia communications, in 2008. She is currently a Professor with the Department of Information Technology, Faculty of Computers and Information Sciences, Mansoura University. She has more than 20 research publications. Her research interests include WSN security, adhoc network security, cryptography, multimedia security, mobile sensing security, and image processing.