RESEARCH   **Open Access**

CrossMark

A novel jammer detection framework for cluster-based wireless sensor networks

P. Ganeshkumar[*†], K. P. Vijayakumar[†] and M. Anandaraj

Abstract

Jamming attack is a serious security threat in wireless sensor networks. Therefore, it is important to frame a mechanism to protect wireless sensor networks from various jamming attacks. Jammer intrusion detection and jamming detection are two separate issues. In this paper, a novel jammer detection framework to detect the intrusion of jammer and the presence of jamming in a cluster-based wireless sensor network is proposed. The proposed framework is novel in three aspects: whenever the cluster head receives a packet, it first verifies whether the source node is a legitimate, new node, or a jammer node. Second, when the source node is declared as a new one in the first step, then the framework validates whether the new node is legitimate node in the previous cluster or a jammer node by using cluster head code. Third, the framework observes the behavior of the newly joined node and the existing nodes to identify whether the nodes in the cluster is jammed or not. Additionally, it also classifies the types of jamming, if the presence of jamming is detected. Simulation result shows that the proposed framework performs extremely well and achieves jamming detection rate as high as 99.88 %.

Keywords: Wireless sensor networks, Threat, Jammer, Jamming, Cluster

1 Introduction

Wireless sensor network encompasses small sensor nodes. The sensor node includes sensing unit, computing unit, communicating components, and memory [1]. Sensor nodes are self-organized. These nodes are deployed in a region called sensor field to sense the environment. Sensor nodes are restricted by memory space, energy, and computational power. The sensor nodes work in an infrastructureless and dynamically changing environment [2] and route the collected data to the destination node for further interpretation.

Clustering results in a two-layer hierarchy where the cluster heads (CHs) form the higher layer and cluster members form the lower layer. Nodes are divided into clusters in the cluster-based wireless sensor networks. Each cluster contains a CH and cluster members (CMs). In a cluster, communication among CMs is carried out through CH and communication among CHs is carried out through the base station (BS). The CM may leave from a cluster and join in another cluster, and a new node may join in a cluster. The benefits of clustering are achieving energy efficiency by reclustering, decreasing collision, reducing the communication overhead, improving throughput, and network lifetime [3].

The sensor network is vulnerable to jamming attacks since the sensor nodes operate at a very low radio power [4] and use limited communication range between source and sink. The jammers initiate jamming attacks, and their objective is to prevent the communication between sensor nodes or corrupt legitimate transmissions of sensor nodes by causing intentional packet collisions at the medium. Therefore, wireless sensor networks are appropriate in their hunt for jammers. The sensor networks are enormously used in many applications from military to health care [1, 3, 5, 6]. Therefore, a mechanism is required to detect jammer intrusion and jamming in wireless sensor network (WSN). To detect jammer intrusion and jamming, first, the intrusion or entry of jammer has to be detected (by using verification and validation algorithm) then, jamming and its types are detected (by using auditing algorithm). In this paper, a novel jammer detection framework (which detects the intrusion of jammer and various types of jamming attacks) is proposed and evaluated. In the existing literature [7–10], various jamming

*Correspondence: drpganeshkumar@gmail.com
[†]Equal contributors
Department of Information Technology, PSNA College of Engineering and Technology, Kothandaraman Nagar, Dindigull, Tamil Nadu 624622, India

detection approaches are proposed for detecting jamming in the wireless sensor networks. However, to the best of our knowledge, none of the existing literature has considered the issue of jammer intrusion detection in sensor networks. Therefore, in this paper, the main idea is both jammer intrusion detection and jamming detection in the cluster-based wireless sensor networks. throughout this paper, jammer detection refers to (i) jammer intrusion detection and (ii) jamming detection.

To understand jammer intrusion detection, it is assumed that a legitimate member moves from one cluster to another cluster. At this juncture, the jammer impersonates as a legitimate member and enters into a new cluster posing to be as legitimate member. For example, when a member M1 moves from cluster C1 to cluster C2, then according to existing reassociation procedure, C2 has to validate with C1, whether M1 is a legitimate member in C1 or not. If C2 receives a reply from C1 stating that M1 is a legitimate node in C1, then C2 ascertains that M1 is a legitimate member. At this point of time, the jammer node poses to be M1 enters into the cluster C3. In order to check the legitimateness of M1, C3 queries C1 and obviously receives a reply that M1 is a legitimate node in C1. By posing to be a moving legitimate node, jammer node cleverly enters into C3. This problem has to be addressed. To alleviate this problem, in this paper, the idea of cluster head code (CHC) is deployed and it is described in Section 3.1.1. The jammer node is also referred as rouge node within the WSN. The reason to consider the rouge/jammer node in the WSN is given as follows: when a member M1 moves from cluster C1 to cluster C2, the jammer node posing to be M1 enters into the cluster C3. After entering into C3, the jammer node can jam the members of C3 that are within the communication range of the jammer node.

To understand jamming detection in cluster-based WSN, let a cluster with cluster head and cluster members be considered. In order to detect the presence of jamming in the network (to detect whether the cluster members are jammed or not), a mechanism is needed to monitor the behavior of the cluster members periodically. To address this, auditing algorithm is devised (Section 3.1.2). In the auditing algorithm, the behavior of the members are determined periodically by using two jamming detection metrics such as packet delivery ratio (PDR) and received signal strength indicator (RSSI). Auditing algorithm is implemented in CH. This algorithm computes the PDR, maximum PDR, and malicious level of CMs in the cluster periodically (say for every 0.1, 1, and 3 s, respectively). PDR alone is inadequate in determining the presence of jamming. Therefore, RSSI is used as an additional metric to detect the presence of jamming accurately. When the maximum PDR of a CM is lower than the PDR threshold (Section 2.5.2), then auditing

algorithm measures the RSSI of the corresponding CM. The measured RSSI is compared with the RSSI threshold (Section 2.5.2). If the measured RSSI is above the RSSI threshold value, then auditing algorithm assigns the malicious level as high. If the malicious level of the corresponding CM is thrice consecutively determined as high, then the auditing algorithm declares that the corresponding CM is jammed. The type of jamming is also identified if the presence of jamming is detected in the auditing algorithm.

The primary motivation of this novel jammer detection framework is to identify the intrusion of the jammer and the jamming attacks in the cluster. The key ideas of this framework are listed below:

- The proposed framework uses CH centric (network centric) approach for detecting jamming in the cluster-based sensor network. In this approach, the CH estimates the metrics PDR and RSSI to make decision about "jammed situation" or "non-jammed situation". The metrics PDR and RSSI for each node under a single cluster is implicitly known to the CH, and it is explicitly not necessary for the CH to collect metrics from the CMs. Due to this, processing and decision-making are carried out by the CH itself without help from the members unlike the existing system. In the existing system, packet send ratio (PSR), PDR, bad packet ratio (BPR), and bit error rate (BER) are termed as jamming induction metrics (JIM), and they are gathered from respective nodes as well as neighbor nodes and are based on the collected JIM where the decision on the presence of jamming is determined. In the proposed system, the identified JIM metrics are PDR and RSSI. PDR and RSSI of CMs are available within the CH itself, and it is not required to collect this metrics elsewhere from the CMs. Therefore, it can be claimed that the CM is not burdened (is not loaded heavily) in the proposed approach.
- As discussed above, in the proposed system, the communication overhead is reduced since CH by itself directly estimates the metrics for processing and decision-making (CH does not depend on its member for collecting the JIM), the communication overhead is reduced.
- In the proposed work, a new node may join in a cluster or an existing node may leave from a cluster. Therefore, it supports mobility unlike the existing system which does not support mobility. To support this, the modified medium access control (MAC) frame format is used. The modified frame format also authenticates the newly joining node in the cluster (Section 3.1.1).

The contributions of this paper are listed as follows:

- Jamming detection metrics (Section 2.3): Jamming detection level is bounded by threshold values of PDR and RSSI. That is, if PDR decreases below a given threshold value and RSSI is higher than its threshold value, then it can be ascertained that the jamming is present. Predicting this PDR and RSSI threshold is a crucial task in WSN. In this paper, appropriate statistical test (T test) is carried out to find and fix the threshold values.
- Statistical proof (Section 2.5): By using PDR and RSSI threshold, the presence of jamming can be determined. However, it is not sufficient to determine the presence of jamming alone, further it is necessary to determine the type of jamming launched (constant or deceptive or random or reactive jamming). In order to find the type of jamming launched in the network, T test is performed on the two sets viz PDR is not affected without jamming and PDR is affected after launching specific type of jamming. The T test proves that there is a significant difference between the two means. By using the mean PDR of a jammed member as reference value, the classification of jamming is performed (Table 1). In addition to this, chi-square test is performed to compare the performance of the anticipated result and the result obtained from simulation (Table 11).
- Jammer detection framework (Section 3): The jammer detection framework (JDF) detects the intrusion of the jammer and various types of jamming attacks. This framework works in three aspects. First, it performs verification whenever a packet is received. Next, whenever a node joins in a cluster then the framework uses cluster head code (CHC) in order to determine the presence of jammer (whether the node wishes to join in a cluster that is legitimate node or jammer node). Finally, the framework monitors the behavior of both the existing node and the newly joined node periodically to determine the presence of jamming.
- Authentication using CHC (Section 3.1.1): The proposed framework uses CHC to determine whether the new node belongs to the available cluster. Because the jammer node finds the loop hole and enters into the cluster during node mobility, that is, the jammer node may pose as a legitimate member

of other clusters and cleverly enter into the cluster as a legitimate node.

The rest of the paper is organized as follows: The system model is described in Section 2. Section 3 explains the proposed framework in three aspects: verification, validation, and auditing. Experiments and discussions on the results are presented in Section 4. Related work is discussed in Section 5. Finally, Section 6 concludes this paper.

2 System model
In this section, different types of jamming attack models are discussed first, and then the metrics used in the existing system are discussed. Next, the metrics used for detecting the presence of jamming in the proposed work is described. Finally, the system configuration is depicted for determining the effect of various types of jamming.

2.1 Jamming attack models
The proposed work employs four types of jamming models, namely constant, deceptive, random, and reactive jammers [7]. The constant jammers continuously generate packets on the medium to jam the communication completely and do not obey the procedures of the MAC layer. The deceptive jammer regularly provides packets (not random bits) on the communication channel. It is a dangerous type of jammer since deceptive jammer follows the MAC layer procedure. The random jammer produces the packets in a regular interval and switches between jamming and sleeping. This type of jammer sleeps for a period of R_S time and jams for a period of R_J time. The R_S and R_J values may either be fixed or be in random. As a result, the random jammer can reduce the power consumption by switching between sleep and jam modes. During jam period, the random jammer may operate as constant or deceptive jammer. The reactive jammer listens to the communication channel and generates fake packet when transmission happens.

2.2 Jamming detection metrics in existing literature
The jamming detection metrics used in the existing literature are PSR [7], PDR [7], BPR [8, 9], signal-to-noise ratio (SNR) [8], energy consumption amount (ECA) [9], and BER [8, 10]. The definition of these metrics are given as follows: The PSR is measured by the source node which is defined as the ratio of the number of packets actually sent by the node to the number of packets intended to be sent by the node. The PDR is computed either by source node or destination node. The PDR is defined as the ratio of the total number of packets successfully sent by the node to the total number of packets sent by the node. The BPR is computed at destination node, and it is defined as the ratio of the number of bad packets received by a

Table 1 Types of jamming

Types of jammer	Average PDR (in %)	PDR range (in %)	RSSI (in db)
Constant	9.76	0–10	−93.141
Deceptive	28.81	25.6–53.5	−93.141
Random	57.9	53.6–73.75	−93.141
Reactive	22.21	11–25.5	−93.141

node to the total number of packets arrived at destination node. The SNR is defined as the ratio of the received signal power in a node to the received noise power in a node. The ECA is defined as the amount of energy consumed in a particular time for a wireless sensor network. The BER is computed as the ratio of the number of damaged bits to the number of total bits received by a node for the duration of a transmission session.

The metrics PSR and PDR are used in [7] to identify the jamming attack. From the results, it is observed that the PSR and PDR encounter problems in deciding about jamming and its types. Then, two algorithms are devised (signal strength consistency check and location consistency check). The first algorithm uses the PDR and signal strength in order to determine the presence of jamming. The second algorithm uses the PDR and location of its neighbors to determine the presence of jamming. The estimation of PSR is a complex task. Additionally, this approach needs localization technique or hardware such as GPS to identify the neighbor's location. The BPR and the SNR metrics are used in [8] to detect various jamming attacks. The approach used in [8] causes communication overhead since every node in the network has to report the data periodically to the BS. The metrics PDR, BPR, and ECA are used in [9] to detect the presence of jamming. The BPR and ECA are estimated by nodes; accordingly, the nodes are burdened. The metrics BER and RSS are used in [10] for detecting jamming attacks. But it is difficult to compute the BER by a sensor node, since a sensor node needs to collect a huge amount of data. This method cannot classify various types of jamming attacks. It is clear from the existing jamming detection metrics that there is no metric or combination of metrics that determines jamming and its types in both physical and data link layer. Therefore, a kind of jamming detection metric and its suitability in WSN are needed to be explored.

2.3 Jamming detection metrics in the proposed system
In the proposed system, the jamming detection metrics, namely PDR and RSSI, are selected for detecting the presence of jamming in a wireless sensor network. The PDR alone is not sufficient to detect the presence of jamming. Therefore, it is essential to consider an additional metric to detect the presence of jamming and different types of jamming correctly. The metric RSSI is considered as an additional metric as discussed in Section 2.2. The advantages of selecting these metrics are discussed as follows:

1. The PDR is an excellent metric since the CH can measure it by itself accurately without much computational overhead, and PDR can identify the presence of all types of jamming attacks both at physical and data link layers.

2. The CH can easily measure RSSI either by using formulae as per the chosen propagation model (in the proposed work, free-space propagation model is chosen) or by the node's RF power meter.
3. In the proposed system (Section 3), the CH estimates the metrics (PDR, RSSI) and makes decision about "jammed situation" or "non-jammed situation". The metrics PDR and RSSI for each node under a single cluster is known to the CH implicitly, and it is explicitly not needed for the CH to collect the metrics from the nodes. Due to this, processing and decision-making are done by the CH itself without needing help from the members. Therefore, it can be claimed that the CM is not burdened (is not loaded heavily).
4. In the proposed system, the metrics PDR and RSSI are used in detecting the presence of jamming and its types to an extend of 99.9 %. The metrics PDR and RSSI are defined in the next section. The suitability of considering these metrics in the WSN environment is illustrated in Section 2.5.

2.4 Description of PDR and RSSI
This section describes the metrics that are used in this paper to detect the presence of jamming attack. The metrics PDR and RSSI are considered in the proposed system. The PDR is computed by a source node (CH). The PDR is defined as the ratio of the total number of packets successfully (the packets for which acknowledgement is received) sent by the node to the total number of packets sent by the node. The PDR is expressed as follows:

$$\text{PDR} = \text{Pss/Ps} \qquad (1)$$

where Pss is number of packets successfully sent by the source, Ps is the total number of packets sent at the source. The RSSI is defined as the ratio of received signal strength to the reference power. The received signal strength value can be converted into RSSI [11] as given below:

$$\text{RPr} = \text{TPs.Gt.Gr} \left[\frac{\beta}{4\pi d} \right]^2 \qquad (2)$$

$$\text{RSSI} = 20 \log \left(\frac{\text{RPr}}{\text{Pref}} \right) \qquad (3)$$

where RPr is the remaining power at the receiver, TPs is the transmitted power at the sender, Gt is the gain of the transmitter, Gr is the gain of the receiver, β is wave length, d is distance between the sender and receiver, and Pref is the reference power.

2.5 Statistical proof
In this section, it is essential to determine first whether various types of jamming influence PDR or not by performing the statistical test (T test). Next, T test is used to fix the PDR threshold. The T test proves that there is a

significant difference between the two population means (i.e., observed PDR during jamming-free scenario and observed PDR after the launching of jamming). By using the mean of samples, the PDR threshold is fixed. Lastly, by using PDR and RSSI threshold, the presence of jamming is determined. However, it is not sufficient to determine the presence of jamming alone, but further it is necessary to determine the type of jamming launched (constant or deceptive or random or reactive jamming). In order to find the type of jamming launched in the network, T test is performed on the two sets viz observed PDR during jamming-free scenario and observed PDR after launching a specific type of jamming. The T test proves that there is a significant difference between the two means. Therefore, by using the mean PDR of the jammed member as reference value, the types of jamming are classified (all the T tests are performed by using samples obtained from our simulation).

2.5.1 Jamming and PDR

The T test is performed to verify whether the jamming infuences PDR or not by using few samples. The simulation is carried out in Section 4. At first, the constant jamming is commenced. Then, two group of samples are taken from the simulation with respect to the absence and presence of jamming in the sensor network. The T test is done on these samples to signify whether there is a variation between the two population means (that is, PDR is not affected during the absence and presence of jamming) or not. Similarly, the simulation is repeated for other types of jamming.

The null hypothesis signifies that there is no difference between the two population means (i.e., PDR is not affected during the absence and presence of jamming). The alternate hypothesis signifies that there is a difference between the two population means (i.e., PDR is not affected in the absence of jamming and PDR is affected in the presence of jamming).

T test is done on 40 samples (20 samples in the absence of jamming and 20 samples in the presence of jamming) of PDR acquired from the CMs, CM1, CM2, CM3, CM4, and CM5. The degree of freedom (df) is computed as 38 ($s1 + s2 - 2$), and the significance level (p) is 0.001 with the corresponding t values 49.2, 68.7, 72.2, 0.6, and 2.1 for 99.9 % of confidence interval. $s1$ indicates the total number of samples measured in the absence of jamming, and $s2$ denotes the total number of samples in the presence of constant jamming. The result passes the t test. The t value of members CM1, CM2, CM3, CM4, and CM5 is 49.2, 68.7, 72.2, 0.6, and 2.1, respectively. The t table value of T test is 3.65. It is identified that the t value of the CMs, CM1, CM2, and CM3, exceeds the table value. This signifies that the PDR of CM1, CM2, and CM3 is reduced due to jamming, whereas the members CM4 and CM5

are not affected by constant jamming. Thus, it proves the significance of alternate hypothesis for constant jamming. The level of significance is 0.001. This indicates that the reliability of the result is 99.9 %, i.e., the obtained result is considered to be correct by 99.9 % and the chance of attained result to be wrong is 0.1 %. Similarly, the T test is repeated for other types of jamming (deceptive, random, and reactive).

2.5.2 PDR and RSSI threshold

PDR is employed to realize the incidence of jamming. Therefore, it is necessary to identify the association between PDR and jamming. It is well known that jamming is inversely proportionate to PDR. An analysis is done to find out the snapping point at which the jammer influences the PDR to decrease. In the proposed system, the snapping point at which the jammer influences the PDR to diminish is fixed as the threshold value (in simulation) to forecast the presence of jamming.

CH periodically monitors the PDR. If the computed PDR is lesser than the PDR threshold, then CH will state that jamming has taken place. The test is done with four samples of PDR acquired from CMs CM1, CM2, CM3, CM4, and CM5 to fix the threshold. The degree of freedom is 3, and the significance level (p) is 0.001 with the corresponding t value at 13.1 for 99.9 % of confidence interval. The result passes the t test. The t table value of T test is 12.92. It is identified that the t value (13.1) exceeds the t table value (12.92). This shows that there is significance and therefore the PDR threshold (PDR threshold) is fixed as 74.75.

The factors other than jamming such as collision and congestion can also influence the data transmission and cause the PDR value to become low. Therefore, PDR is used in conjunction with RSSI in order to detect the presence of jamming. The CH frequently measures the RSSI value and fixes the RSSI threshold. If the CH estimates lower PDR value than the PDR threshold, then CH also compares an estimated RSSI value against the RSSI threshold. If the observed PDR value is lower than the PDR threshold and the RSSI value is higher than the RSSI threshold, then it can be ascertained that the node is jammed. The average RSSI (db) threshold (RSSI threshold) value is fixed as -93.141 for 20 m [12].

2.5.3 Types of jamming

The CH compares the observed PDR and RSSI against the PDR range and RSSI as shown in the Table 1 to make a distinction between various types of jamming. Table 1 consists of three fields such as average PDR, PDR range, and RSSI. The average PDR represents the average PDR value of CMs CM1, CM2, and CM3 from the T test of various types of jamming (for example, in the constant jamming, the average PDR value is considered

as discussed in Section 2.5.1. Similarly, the experiment is repeated for other types of jamming). The PDR range for various types of jamming is considered from the *T* test (in simulation). For example, in the constant jamming, the PDR range is considered as in Section 2.5.1. Similarly, the experiment is repeated for other types of jamming. The RSSI is fixed as discussed in Section 2.5.2.

2.6 System configuration

The system set-up consists of four clusters and a BS as shown in the Fig. 1. Each cluster consists of six nodes (one CH and five CMs). The communication range of each node in the network is 20 m. CM communicates with other CMs in a cluster through CH and CHs communicate with other CHs through BS. CM moves between clusters.

To illustrate the proposed system, a jammer is launched deliberately in the cluster CH21. The proposed system is installed in the CH and BS. To understand the interactions of the jamming detection metrics (Section 2.3) and to measure the impact of a jammer in various scenarios (Section 4.2), simulations are performed as per described in Section 4. The simulation is done by using various models as discussed in Section 2.1. In the simulation, a jammer is launched in the first cluster (CH 21). This cluster consists of a cluster head (CH21) and five members such as CM1, CM2, CM3, CM4, and CM5. From the simulation result, it is observed that CH21 identifies that the members CM1, CM2, and CM3 are jammed and the members CM4 and CM5 are not jammed. It is also evident from the simulation result that the CH has the ability to make a distinction between various types of jamming (Section 2.5.3). Based on the simulation, it is justified that the CH has the

Fig. 1 Wireless sensor network with a jammer node. The *node in black box* indicates CH, the *nodes without box* specify CMs, and the *red node* represents the jammer node. The *line* indicates a communication between CH and CM. The arrow denotes communication between CHs and BS. The CH21and members 1 to 5, CH22 and members 6–10, CH23 and members 11–15, and CH24 and members 16–20 are divided into four clusters, respectively. The nodes with *colored box* indicate jammed members

ability to identify the jammed members and BS has the ability to identify the jammed CHs.
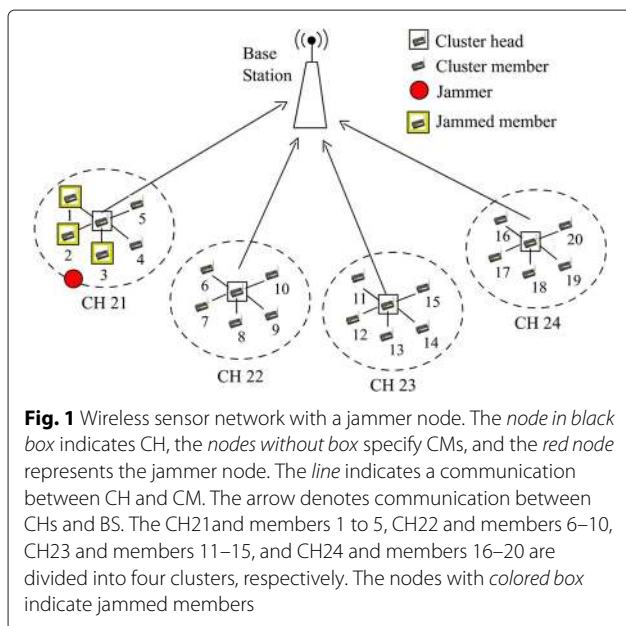
3 Jammer detection framework

In this section, first, innovation, research idea, and description of the problem statement are described. Next, the modules in the jammer detection framework such as verification and validation (jammer intrusion detection) as well as auditing (jamming detection) are discussed. Then, the databank used in the proposed system is defined. Finally, verification and validation steps as well as auditing step of the jammer detection framework are described.

The important innovation,research idea, and the description of the problem statement of this article are listed in the following. In spite of this, the motivation, objective, and contribution of the paper is well described in Section 1.

1. In the existing literature [7–10], several jamming detection approaches were proposed for flat WSN. In [13], the authors proposed jamming detection approach for cluster-based WSN. Thus, in the existing literature, only jamming detection is carried out. The issue of jamming detection is completely different from jammer detection. Jamming detection refers to the detection of the presence or absence of jamming in the network. Jammer intrusion detection or simply jammer detection refers to the detection or identification of the entry of jammer node in the cluster. To the best of our knowledge, none of the existing literature has considered the issue of jammer intrusion detection or jammer detection in cluster-based WSN. Therefore, in this paper, the main idea is to first detect the jammer intrusion into the cluster (Section 3.1.1: verification and validation algorithm) and then to perform jamming detection in the cluster in the cluster-based WSN (Section 3.1.2: auditing algorithm). The proposed system works in two aspects: first, it prevents the entry of jammer into the cluster and, second, it continuously monitors the members inside the cluster to determine whether the members are jammed or not. That is, first, the proposed JDF prevents the entry of the jammer into the cluster. But due to any unexplained or unaddressed random error, if the jammer enters into the cluster then, a monitoring mechanism is needed to monitor the cluster member to determine whether the members are jammed or not. To address this, the cluster head of the proposed system performs jamming detection inside the cluster. Therefore, the proposed JDF comprises two components: verification and validation algorithm for jammer intrusion detection and auditing algorithm for jamming detection within the cluster member.

2. The threshold value and/or the parameter of the jamming detection metrics in the existing literatures is set up based on the reference value published in [7]. Unlike

in existing literatures, in the proposed system, statistical test (T test) is performed for the following: (i) To examine and determine the appropriate jamming detection metric (among PDR, PSR, RSSI) for identifying the presence of jamming (Section 2.5.1), (ii) to find the threshold value of PDR (Section 2.5.2), and (iii) to classify various types of jamming (Section 2.5.3).

3. In this paper, a performance metric called undetection ratio (UDR) is introduced. To the best of our knowledge, none of the existing literature had defined and used this metric UDR. UDR explains that the CH does not detects a node as abnormal when the node is really jammed (that is, the CH does not detect the jammed node or CH fails to detect a jammed node). The detailed explanation is given below.

The reason behind choosing the metric UDR in this paper is explained as follows: in the existing literature, false positive rate or false discovery ratio or false detection ratio (FDR) was used and defined as the ratio of the number of nodes incorrectly identified by the system to the number of nodes actually falling under that group. There is no clear definition of false detection in the existing literature. In general, there are two scenarios in false detection: (i) detects a node as abnormal though that node is normal (false positive) and (ii) does not detect a node as abnormal when the node is jammed (false negative). It is found from the existing literature that the FDR denotes the first scenario (false positive), and there is no explanation about the second scenario (false negative). Therefore, in this paper, the detection of sensor nodes is classified into (i) true detection, (ii) false detection, and (iii) undetection. True detection, false detection, and undetection are based on true positive, false positive, and false negative, respectively. In true detection, the CH detects a node as abnormal when the node is jammed. In false detection, the CH faultily detects a node as abnormal though that node is normal. In undetection, the CH does not detects a node as abnormal when the node is really jammed (that is, the CH does not detect the jammed node or CH fails to detect a jammed node) (Section 4.3).

For example, consider there are ten nodes in which five nodes are jammed and five nodes are normal.

- In first scenario, if the jamming detection system detects five nodes as jammed when five nodes are really jammed, then the TDR is computed as 1 (that is, $5/5 = 1$). The system neither detects a node as abnormal though that node is normal nor detects a node as normal when the node is jammed. Hence, the FDR and UDR are computed as 0.
- In second scenario, in real scenario, five nodes are jammed out of six nodes. In the simulation, if the system detects six nodes as jammed when only four nodes are really jammed, then the TDR is computed

as 0.8 (that is, $4/4 + 1 = 0.8$). (That is, the number of correctly detected jammed nodes/the number of correctly detected jammed nodes + the number of nodes that are detected as not jammed but they are actually jammed). In this scenario, the FDR is computed as 0.4 (that is, $2/(2 + 3) = 0.2$). (That is, the number of nodes are detected as jammed but they are normal/the number of nodes that are detected as jammed but they are normal + the number of correctly detected normal nodes, but the nodes are normal). In this scenario, the UDR is computed as 0.2 (that is, $1/(4 + 1) = 0.2$. That is, the number of nodes that are detected as normal but they are abnormal/ the number of correctly detected jammed nodes + the number of nodes that are detected as normal but they are abnormal).

For a fair jamming detection system, the TDR must be equal to 1 and FDR and UDR must be equal to 0.

3.1 Jammer detection framework model

The JDF is proposed for cluster-based wireless sensor networks. The main idea of the JDF is to perform both jammer intrusion detection by using verification and validation, and jamming detection using auditing. Figure 2 illustrates the key modules of the framework.

The JDF is implemented in all CH/BS. When this framework receives a packet, then it detects whether the source node is a legitimate node or jammer node or new node using three steps namely: (1) verification, (2) validation, and (3) auditing. Every CH has to maintain look-up tables for verification, validation, and auditing. The look-up tables employed in JDF are cluster member and head (CMH) table, jammer table, CHC table, cluster member CHC (CM_CHC) table, flag table, PDR table, maximum PDR (MaxPDR) table, and malicious table. All these look up tables are kept inside a data bank.

The verification step (first step) in JDF uses the MH table and Jammer table. The main intention to maintain the MH table and jammer table is to determine the type of source node and identify whether the source node is a legitimate node, new node, or a jammer node. When the source node moves from one cluster to another, then validation step (second step) in the JDF has to authenticate whether the source node belongs to any of the available cluster or not. In order to authenticate the source node and to determine the presence of a jammer node, the validation step maintains two tables such as CHC table and CM_CHC table. In order to monitor the behavior of CMs, the auditing step (third step) in the JDF maintains four tables such as flag table, PDR table, MaxPDR table, and malicious table. The tables used in the auditing step are not shown in Fig. 2.
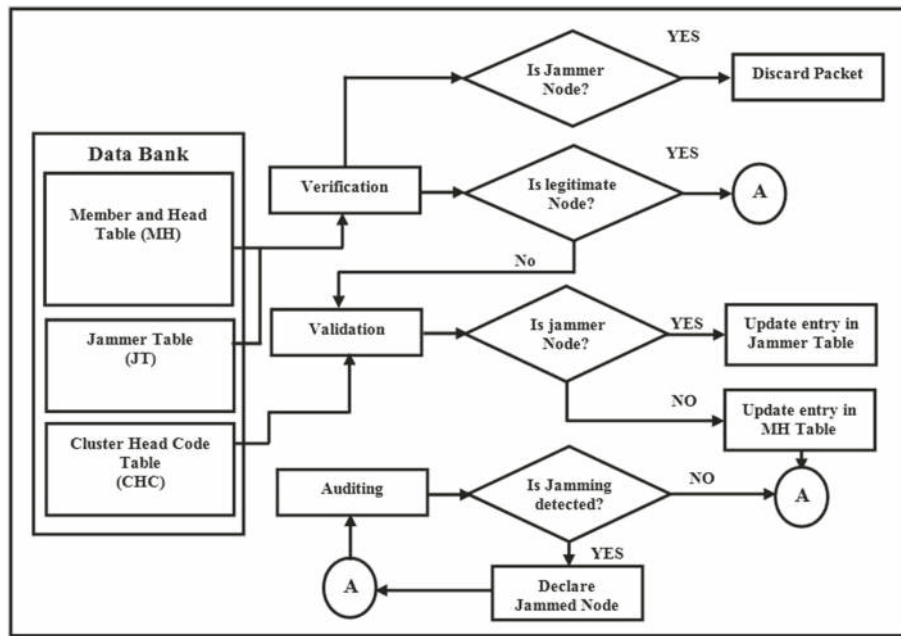
Fig. 2 Jammer detection framework. The framework represents three steps: verification, validation, auditing, and the databank. The databank consists of various look-up tables used by this framework

The description and use of each table is explained as follows:

1. The CMH table contains two fields: Node ID and node type as shown in Table 2. The node ID represents the identity (address) of the nodes. Node type represents the type of the source node (CH, CM, or BS). The objective of this table is to determine the type of the source node.
2. The Jammer table includes two fields such as S.No. and node ID as shown in Table 3. The S.No. represents the corresponding records' entry number. The node ID represents the identity (address) of the jammer node. The source node is declared as jammer node, if address of the source node is found in the jammer table.

3. The CHC table is formed by two fields namely: cluster heads and CHC as shown in Table 4. The cluster heads field denotes the CHs available in the network. The CHC represents each CH's CHC (Section 3.1.1). This table is used by each CH to authenticate the source node, when a source node moves from one cluster to the other or when a source node wishes to join in a cluster.
4. The CM_CHC table includes two fields such as cluster head and CHC as shown in Table 5. The cluster head represents the CH in which the corresponding CM has been associated. The CHC denotes the CHC provided by the CH in which the corresponding CM is associated.
5. The flag table contains two fields, namely CM_N and flag, as shown in the Table 6. The CM_N field represents the address of the members in the cluster, and flag represents either the value T or F, where T denotes a successful delivery of a packet of the corresponding CM and F denotes an unsuccessful (F is determined if there is no acknowledgement within the specified time interval) delivery of a packet. The JDF updates the flag entry with the value either T or F in this table.

Table 2 CMH table

Node ID	Node type
1	M
2	M
3	M
–	–
21	H
22	H
–	–
50	B

Table 3 Jammer table

S.No.	Node ID
1	25

Table 4 CHC table

Cluster heads	CHC
21	5
22	2
23	4
24	6

Table 6 Flag table

CM_N	Flag (T or F)
1	F
2	F
3	F
4	T
5	T

6. The PDR table consists of two fields such as CM_N and CM_PDR as shown in Table 7. The CM_N field denotes the address of the CM and the CM_PDR field represent the packet delivery ratio of each member in the cluster. The JDF computes this CM_PDR value periodically (every 0.1 s) by observing the entries from Table 6.

7. The MaxPDR table is formed by two fields such as CM_N and CM_MPDR as shown in Table 8. The CM_N field represents the address of the CM, and CM_MPDR represents the maximum packet delivery ratio of each member in the cluster. The JDF calculates this CM_MPDR value periodically (every 1 s) by observing the entries from Table 7.

8. The malicious table contains three fields such as entry no., CM_N, and level as shown in Table 9. The entry no. field represents records' entry number. The CM_N field represents the address of the CM, and level denotes the malicious level of each member in the cluster. The JDF computes the value of Level periodically (every 3 s) by observing the entries from Table 8 and expresses the value as high, normal, and low. In order to do this, the following three rules are followed:

   1. If MaxPDR.MPDR is lesser than PDR_Threshold and RSSI is greater than RSSI_Threshold, then its malicious level is assigned as high.
   2. If MaxPDR.MPDR is equal to PDR_Threshold, then its malicious level is assigned as normal.
   3. If MaxPDR.MPDR is greater than PDR_Threshold, then its malicious level is assigned as low, where MaxPDR.MPDR represents the maximum value of PDR from the corresponding entries of each member in the cluster (every 1 s).

The verification step verifies whether the source node is CM, BS, a new node, or a jammer node by referring the

MH table and Jammer table. If the source node is authorized as a legitimate node by the framework, then the framework proceeds with auditing step (step three). Or else, if the source node is found in the jammer table, then the framework declares the source node as the jammer node. Otherwise, the framework declares the source node as a new node (source node is not found in the jammer table) and proceeds with the validation step (step two).

The validation step performs the following function. If the source node is declared as a new node in the verification step, then the CHC is used to determine whether the new node belongs to any of the available CH or not. If the source node belongs to any of the available cluster then, the framework proceeds with auditing step (step three). Otherwise, the framework declares the source node as the jammer node and proceeds with the auditing step.

The third step of the framework is the auditing step. The auditing step determines the behavior of the members in a cluster by observing the CM's PDR and RSSI periodically. In order to do this, the framework maintains the following tables viz: flag, PDR, MaxPDR, and malicious table. The observed PDR and RSSI values are stored in these tables (Section 3.1.2). The observed PDR and RSSI values are compared with their respective thresholds. If the behavior of a member is found as unusual (if PDR is lower than its threshold and RSSI is greater than its threshold as explained in Section 3.1.2), then the member is declared as jammed.

3.1.1 Verification and validation

The responsibility of verification and validation algorithm is to detect the jammer intrusion in the cluster-based WSN. The first step of the framework is the verification step. The verification step is responsible for making decision about whether the source node is a legitimate node, a

Table 5 CM_CHC table

Cluster head	CHC
21	5

Table 7 PDR table

CM_N	CM_PDR
1	pdr1
2	pdr2
3	pdr3
4	pdr4
5	pdr5

Table 8 MaxPDR table

CM_N	CM_MPDR
1	mpdr1
2	mpdr2
3	mpdr3
4	mpdr4
5	mpdr5

new node, or a jammer node. The verification step refers to the CMH table and jammer table as shown in Tables 2 and 3, respectively.

The second step of the framework is the validation step. This step has to authenticate whether the new node (declared as new node by step one) belongs to any of the available CH or not. Validation is used as security mechanism to perform authentication. For this, validation step uses the CHC.

If the node belongs to any of the available CH (that is, if this step receives valid CHC from new node as response), then this step declares the new node as legitimate node. If this step does not receive or invalid CHC from a new node as response, then it declares the new node as jammer node.

The main intention to use the CHC is to determine whether the new node belongs to the available cluster or not. Because when a legitimate node moves from one cluster to another cluster, the jammer node finds this as a loop hole and enters into yet another cluster by impersonating the moving legitimate node. That is, jammer node may pose as a legitimate member of other cluster and cleverly enter into yet another cluster as legitimate node. The example of this scenario is discussed below.

The CHC is deployed to avoid the jammer intrusion in the network. The modified 802.15.4 MAC and beacon are used for distribution of CHC to CMs and other CHs, updation of CHC in CMs and CHs, recovery of CHC,

Table 9 Malicious table

Entry no.	CM_N	Level
1	1	High
2	2	High
3	3	High
4	4	Low
5	5	Normal
6	1	High
–	–	–
–	–	–
–	–	–
15	5	High

and to perform the process of node authentication. The data authentication is out of the scope of authorŠs objective. Therefore, the data authentication approaches are not discussed in this paper.

CHC is simply a random sequence number but if this CHC is broadcasted in clear by the CH to CMs, then the jammer node may see this CHC and use it to enter into another cluster by impersonating like a legitimate CM. Therefore, CHC should be broadcasted securely to CMs. To alleviate this problem, the technique proposed in [14, 15] can be applied along with the JDF.

The motivating factor behind the use of CHC, to authenticate a new node in the validation step is discussed by comparing the reassociation of cluster members in the existing and the proposed system.

- In existing approach, if a CM moves from one cluster to another cluster, then reassociation procedure is carried out. The process of reassociation in the existing approach is illustrated by using the scenarios shown in Fig. 1.
- In Fig. 1, it is assumed that the CM6 likes to join in the CH24 from CH22. According to the existing reassociation procedure, CH24 validates whether CM6 is a member of CH22 by querying CH22. If CH22 replies that the CM6 is a legitimate member, then CH24 can complete the validation step by stating CM6 as a legitimate member. Finally, CM6 joins CH24.
- During this scenario, when CM6 moves from CH22 to CH24. The jammer node finds loop hole and enters into the picture. At this junction, the jammer node poses to be CM6 and can send joining or join request to CH21. Then, according to the existing reassociation procedure, CH21 has to validate with CH22. For this, CH21 queries CH22 by asking whether CM6 is a legitimate member in CH22. CH22 replies that CM6 is a legitimate member. Posing to be CM6, cleverly the jammer node enters into CH21. Although the CM6 has become a member in CH24, the jammer posing to be as CM6 has become a member in CH21. That is, unfortunately, CH21 allows jammer node to join with it. This problem has to be corrected. To alleviate this problem, in the proposed JDF, the CHC is used to authenticate a newer node.
- The overall idea of implementing the authentication (validation) is achieved by using CHC and is described based on the following steps: (i) formation of CHC, (ii) distribution of CHC to CMs, (iii) distribution of CHC to CHs, (iv) updating of CHC in CMs, (v) updating of CHC in CHs, (vi) recovery of CHC by CH if the CHC is lost, and (vii) authentication. Now, each one is discussed in detail as follows:

1. Initially, every CH has to generate CHC. CHC is a random number. The generated CHC is stored in the CHC table as shown in Table 4. The CHC table consists of information such as the identifier of every CH available in the network and the CHC of the corresponding CHs. Then, the CH broadcasts the generated CHC to its CMs and also to all the CHs in the network through BS. In order to do this, it uses augmented beacon frame and MAC frame of IEEE 802.15.4. The CHC is generated periodically by the CHs to protect the CHC from the jammer. In order to protect the CHC, the security mechanism discussed in [14, 15] can be used. However, in this paper, the security mechanism discussed in [14] is implemented along with JDF. So this protects the CHC from eavesdropping, snooping, interception, and modification attacks.

2. In order to provide the generated CHC to all its members, CH broadcasts a beacon frame to its members. The beacon frame says to all the CMs that the subsequent MAC frame includes CHC.

3. In order to provide the generated CHC to other CHs available in the network, the CHC is put into MAC frame as payload and is sent to all CHs available in the network via BS.

4. If the CM receives the MAC frame, then the CM extracts the CHC. The extracted CHC is stored in the CM CHC table as shown in Table 5.

5. If the other CHs receive MAC frame, then the CHs extract the CHC. The extracted CHC is stored in the CHC table as shown in Table 4.

6. It is necessary for the CH to recover the CHC, if the CHC is lost. To obtain the CHC, the CH requests for CHC from the corresponding CH. Based on the reception of the request from the requested CH, the corresponding CH responses with its CHC. Now, the corresponding CH stores the received CHC in Table 4.

7. In the verification step (step one), if a source node is declared as a new node, then the CH demands CHC from the source node by sending beacon frame. Based on reception of the beacon frame, the source node replies with its CHC. Now, the CH compares the received CHC against the entry available in the CHC table (Table 4). If the received CHC is matched with an entry available in Table 4, then the source node belongs to the available CHs. Otherwise, the source node is declared

as a jammer node. Then, it proceeds with the auditing step. Because the newly joined node or the existing node in a cluster has a chance to become a jammer node in the future. The CHC is incorporated in the MAC frame format. To implement this, the 802.15.4 MAC frame format and beacon frame format are modified (i.e., the reserved field in the MAC and beacon frame format is utilized to incorporate the CHC) as follows:

- The MAC frame payload can hold the random number which represents CHC.
- The two bits of MAC frame reserved field can hold the value between 0 and 3. From the values 0, 1, 2, and 3, the values 0 and 1 are used. The value 0 denotes that the CH provides its CHC to other CHs, and the value 1 denotes that the respective CH demands for CHC from other cluster heads through BS.
- Beacon frame reserved field will consist of the value either 1or 0. The value 1 denotes that the CH will provide its CHC in the MAC frame. The value 0 denotes that CH demands for CHC from its member or new node.

3.1.2 Auditing

The former step is responsible for declaring whether the source node is a jammer node or it belongs to any of the available cluster. The auditing step is responsible for monitoring the existing members behavior and a newly joined member. The auditing step decides whether the newly joined member or existing members are in normal state or unusual state depending on their behavior. This uses PDR and RSSI to find out the behavior of members.

Jamming detection and jamming classification are different modules in the auditing algorithm. The auditing algorithm detects the presence of jamming, and if jamming is present, then the classification is performed based on various types of jamming. Classification of jamming cannot be performed before identifying the presence of jamming. Therefore, in the proposed JDF, first, jamming is detected (based on the results of statistical test), and then if jamming is present, classification of jamming is done (based on the results of statistical test). Thus, statistical tests are employed for both jamming detection and classification but the methodology followed for jamming detection and classification is completely different as detailed below.

The CM_PDR and CM_MPDR of each CM is calculated by CH as shown in Tables 7 and 8, respectively. The CM_PDR is computed periodically (every 0.1 s) by referring the Table 6 and the measured CM_PDR is stored in Table 7. The CM_MPDR is computed (every

1 s) by observing the CM_PDR entries from Table 7 and computed CM_MPDR is stored in Table 8. If the CM_MPDR is above or equivalent to the PDR threshold, then JDF ascertains the member's behavior as low or normal and declares that the member is not jammed (usual). If the CM_MPDR is lower than the PDR threshold, then JDF directly cannot justify that the corresponding CM is jammed. Because the PDR may be affected by other factors. Therefore, PDR alone is inadequate to determine the presence of jamming. It is necessary to use an additional metric RSSI (RSSI threshold is fixed as discussed in Section 2.5.2) to detect the presence of jamming correctly. When the CM_MPDR is lower than the PDR threshold, then JDF measures the RSSI of the corresponding CM. The measured RSSI is compared against the RSSI threshold. If the measured RSSI is above the RSSI threshold, then JDF assigns the malicious level (level) as high. If the malicious level of the corresponding CM is determined as high for three times, then the corresponding CM is declared as jammed.

In addition to jamming detection, the auditing algorithm also performs classification of jamming. The type of jamming is identified if the presence of jamming is detected in the auditing algorithm. The classification of jamming is done by comparing the observed maximum PDR value (from Table 8: MaxPDR table) with the PDR range (from Table 1: types of jamming table in Section 2.5.3). The PDR range for various types of jamming is formulated from the T test. The PDR range is estimated with the probability 0.001, and the PDR range varies based on various probabilities. The auditing algorithm used in the auditing step for detecting the presence of jamming and classifying the type of jamming is given below:

Auditing algorithm
Evaluation of PDR

1. Snooze till the timer elapses (for every 0.1 s)
2. $i = 1$
3. While ($i \leq m$) (m denotes the total number of members in a cluster)
   .   1. Find an entry equivalent to CM_N_i from flag table (Table 6)
   .   2. Calculate the CM_PDR of each CM_N_i from the found entry
   .   3. Modify the calculated CM_PDR in PDR (Table 7)
   .   4. Increment : $i = i + 1$
4. End while
5. Return

Evaluation of maximum PDR

1. Snooze till the timer elapses (for every 1 s)

2. $i = 1$
3. While ($i \leq m$) (m denotes the total number of members in a cluster)
   .   1. Find an entry equivalent to CM_N_i from PDR table (Table 6)
   .   2. Calculate the CM_MPDR of each CM_N_i from the found entry
   .   3. Modify the calculated CM_MPDR in MaxPDR (Table 7)
   .   4. Increment : $i = i + 1$
4. End while
5. Return

Evaluation of maliciousness level

1. Snooze till the timer elapses (for every 3 s)
2. Set $E = 1$ (E denotes the records entry number in Table 9)
3. $j = 1$
4. while($j \leq 3$)
   .   1. while ($i \leq m$)
   .   1. Find an entry equivalent to CM_N_i from MaxPDR table (Table 8)
   .   2. If (MaxPDR.CM_MPDR < PDR_Threshold)
   .   1. CH estimates the RSSI of corresponding CM
   .   2. If (RSSI > RSSI_Threshold)
   .   1. Malilcious.Level = High (Malicious.Level as in Table 9)
   .   3. If (MaxPDR.MPDR = PDR_Threshold)
   .   1. Malicious.Level = Normal
   .   4. If (MaxPDR.MPDR > PDR_Threshold)
   .   1. Malicious.Level = Low
   .   5. Modify the Malicious.Level in entry (E) of malicious table (Table 9)
   .   6. Increment the value of E by one
   .   2. End while
   .   3. Snooze till timer elapses (for every 1 s)
5. End while
6. Return

Jamming detection

1. Snooze till the timer elapses (for every 3 s to detect the jammed node)
2. $i = 1$
3. while($i \leq m$)
   .   1. For every entry in the malicious Table (Table 9)
   .   1. Find an entry that is same as CM_N_i from Table 9
   .   2. If (Malicious.Level is High)
   .   1. Declare CM_N_i is jammed
   .   2. Invoke jamming classification ()
3. Return

Jamming classification :

1. Jamming classification ()
2. If (MaxPDR.CM_MPDR ≥ 0 and MaxPDR.CM_MPDR ≤ 10)
   . 1.declares that the constant jamming is performed
3. If (MaxPDR.CM_MPDR ≥ 11 and MaxPDR.CM_MPDR ≤ 25.5)
   . 1.declares that the reactive jamming is performed
4. If (MaxPDR.CM_MPDR ≥ 25.6 and MaxPDR.CM_MPDR ≤ 53.50)
   . 1.declares that the deceptive jamming is performed
5. If (MaxPDR.CM_MPDR ≥ 53.6 and MaxPDR.CM_MPDR ≤ 74.75)
   . 1.declares that the random jamming is performed
6. Return

In the auditing algorithm, evaluation of PDR, maximum PDR, maliciousness level, and jamming identification/jamming classification are run concurrently in order to detect the presence of jamming and classify them. It is observed that the CH by itself computes the metrics, processes, and makes decision about "jammed situation" or "non-jammed situation". Therefore, the CMs are not loaded for evaluation of jamming detection metrics such as PDR and RSSI, processing, and decision-making unlike the existing approaches.

3.1.3 Posterior action on jamming

The novel jammer detection framework is proposed to detect the intrusion of jammer and the presence of jamming in the cluster-based wireless sensor network. The proposed system detects jammer intrusion and jamming, but it does not describe the post-characterization action in the WSN. The post-characterization action is out of scope of the author's objective. In order to carry out the post-characterization action, the existing defense/countermeasure technique described in [16–22] can be applied along with JDF.

4 Experiments and discussion
4.1 Simulation setup

Firstly, a cluster of six members (M1, M2, M3, M4, M5, and CH21) are considered including CH as shown in the Fig. 1. In Fig. 1, it is identified that the CMs M1, M2, and M3 are jammed. The cluster head CH21 and CMs M4 and M5 are not jammed. The CH identifies about jammed and non-jammed members, whereas identification of jammed CHs or non-jammed CHs are performed by BS. Then, different types of jammer are integrated to analyze the traffic in normal scenario and jamming scenario (Section 4.2). In Fig. 1, three members (M1, M2, and M3) are affected by a jammer and two members (M4 and M5) are not affected by a jammer. The input parameter details are used for

simulation with respect to the sensor networks as given in Table 10.

4.2 Discussions

The simulation is done for 600 s as given in Table 10. At the outset, the simulation is carried out by excluding the jammer. After that, the simulation is continued with different types of jammers. (Initially, the constant jammer is launched, then a set of samples is considered without jamming and after launching of jamming in the network. Similarly, the simulation is repeated for other types of jamming).

To illustrate the normal scenario and jamming scenario with different types of jammers, five set of samples of PDR are taken from the simulation results. In Figs. 3, 4, 5, 6, 7, and 8, the X-axis denotes the cluster members and the Y-axis denotes PDR. The variety of color bars in Fig. 3 indicates different PDR samples (samples are taken from the simulation results) during normal scenario (when jammers are not introduced). From Fig. 3, it is evident that the PDR of every cluster members in the normal scenario is greater than the PDR threshold. Next, various jammers such as constant, deceptive, random, and reactive are introduced in the sensor network. The varieties of color bars in Figs. 4, 5, 6, and 7 indicate different types of jamming (constant, deceptive, random, and reactive). The simulation setup for this scenario is made in such a way that three CMs (CM1, CM2, and CM3) are affected by the jammer and two CMs (CM4 and CM5) are not affected by a jammer. The PDR distribution of cluster members during different types of jamming: with PDR threshold at 74.75 % and with the probability of 0.001 (Section 2.5.1), with PDR threshold at 77 % and with the probability of 0.01 (Section 4.3), with PDR threshold at 73.75 % and with the probability of 0.05 (Section 4.3), with PDR threshold at 62.5 % with the probability of 0.1 (Section 4.3) is shown in Figs. 4, 5, 6, and 7, respectively. From the figures, it is

Table 10 Simulation setup

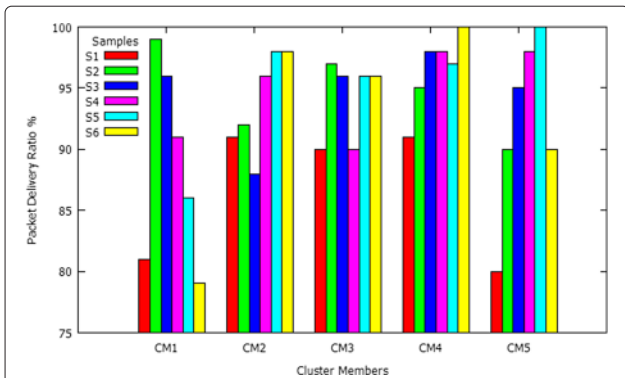| Parameters	WSN	Jammer
No. of nodes	5, 50, and 100	1
Sensor nodes	MRF24J40	MRF24J40
Mode of transmission	Simplex unicast	Simplex broadcast
Packet size	1024 bytes	Variable
Transmission rate	20–100 packets/s	Variable
Transmission range (m)	20	20
Propagation model	Free space	Free space
Simulation time (s)	600	600
MAC protocol	None	None
Jammer type	–	Constant, deceptive, random, and reactive

Fig. 3 PDR distribution of CMs during the normal scenario. Representation of PDR distribution in cluster members (CM1, CM2, CM3, CM4, and CM5) during the normal scenario (sensor network does not include jammer). The PDR of CMs: CM1, CM2, CM3, CM4, and CM5, is above PDR threshold 74.75, 77, 73.75, and 62.5 % with probabilities 0.001, 0.01, 0.05, and 0.1, respectively
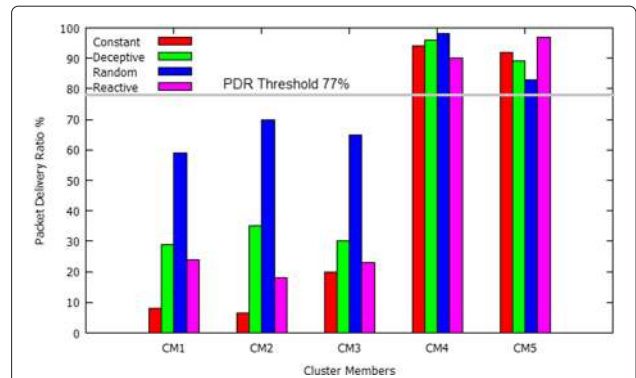

Fig. 5 PDR distribution of CMs during various types of jamming with probability 0.01. Representation of PDR distribution in cluster members (CM1, CM2, CM3, CM4, and CM5) during various jamming with the probability $p = 0.01$. The PDR of CMs: CM1, CM2, and CM3, is less than the PDR threshold 77 % and that of CM4 and CM5 is above PDR threshold 77 %

noted that the PDR of CM1, CM2, and CM3 in all the cases are lesser than the PDR threshold due to the influence of jammer. But the PDR of CM4 and CM5 in all the cases are greater than the PDR threshold (because the members CM4 and CM5 are not jammed).

In Fig. 8, the average PDR of CM1, CM2, CM3, CM4, and CM5 for different types of jamming (constant, deceptive, random, and reactive) with various probabilities is considered. From Fig. 8, it is evident that theoretically the constant jammer jams the entire transmission on the channel, since the constant jammer constantly injects the data packets on the communication medium. But in practice, negligible data transmission takes place. The data packets transmitted by CMs to CH are eradicated continuously by the constant jammer. Thus, the effect of jamming by the constant jammer is determined to

be above 90 % with respect to the average PDR of various probabilities. The jamming effectiveness number is determined based on the averages over the resulting PDR percentage for the CMs: CM1, CM2, and CM3. The deceptive jammer jams the data transmission similar to constant jammer, but the deceptive jammer is aware of the existing protocol in the network. Therefore, the deceptive jamming effect is determined to be around 71 % with respect to average PDR of various probabilities. The data transmission is randomly jammed by the random jammer. The random jammer sleeps and jams the data transmission at random time intervals. From the simulation result, it is noted that the random jamming effect is around 42 % with respect to average PDR of various probabilities. The reactive jammer is also aware of the communication protocol in the network like the deceptive jammer. The
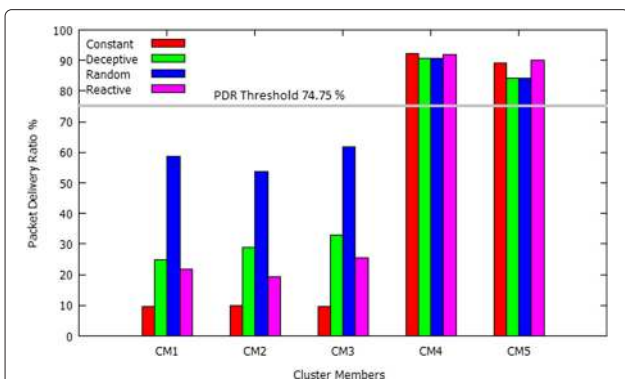

Fig. 4 PDR distribution of CMs during various types of jamming with probability 0.001. Representation of PDR distribution in cluster members (CM1, CM2, CM3, CM4, and CM5) during various jamming with the probability $p = 0.001$. The PDR of CMs: CM1, CM2, and CM3, is lesser than the PDR threshold 74.75 % and that of CM4 and CM5 is above PDR threshold 74.75 %
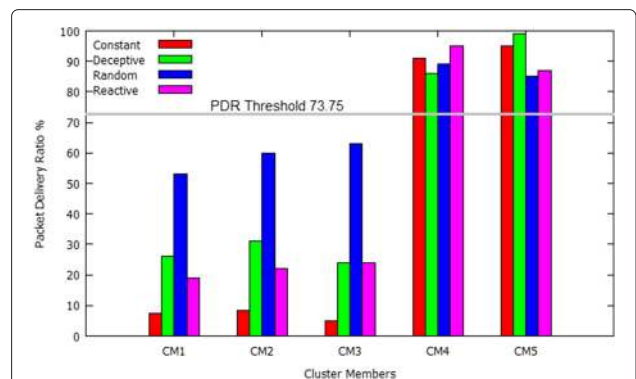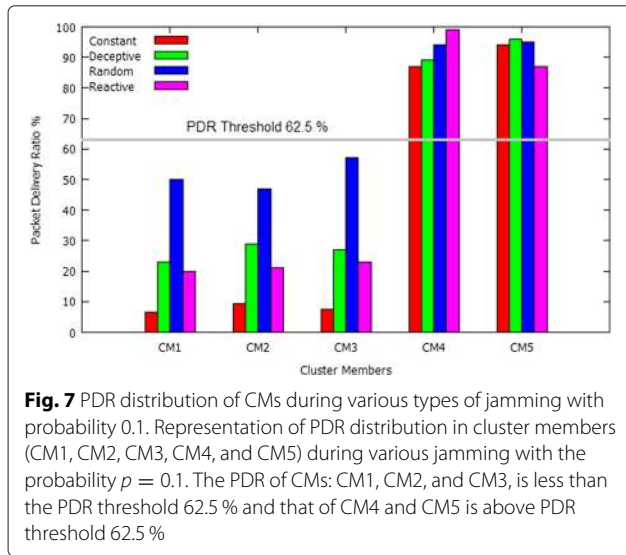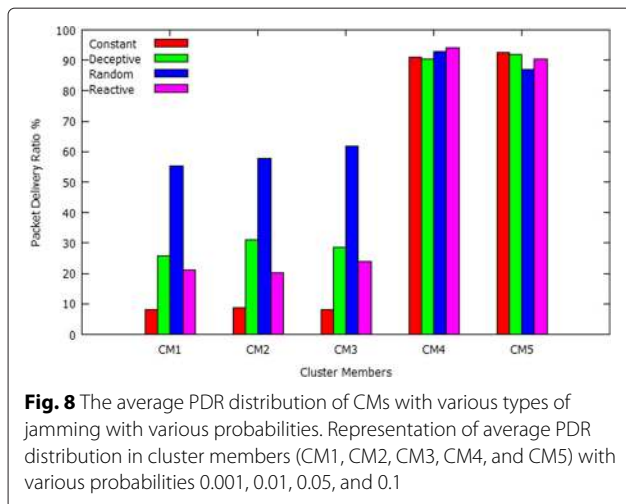

Fig. 6 PDR distribution of CMs during various types of jamming with probability 0.05. Representation of PDR distribution in cluster members (CM1, CM2, CM3, CM4, and CM5) during various jamming with the probability $p = 0.05$. The PDR of CMs: CM1, CM2, and CM3, is less than the PDR threshold 73.75 % and that of CM4 and CM5 is above PDR threshold 73.75 %

Fig. 7 PDR distribution of CMs during various types of jamming with probability 0.1. Representation of PDR distribution in cluster members (CM1, CM2, CM3, CM4, and CM5) during various jamming with the probability $p = 0.1$. The PDR of CMs: CM1, CM2, and CM3, is less than the PDR threshold 62.5 % and that of CM4 and CM5 is above PDR threshold 62.5 %

reactive jammer listens to the transmission medium continuously and initiates to jam the medium during data communication. The average effect of reactive jamming is shown around 80 % with respect to various probabilities.

From Fig. 8, it is evident that the constant jammer (with various probabilities) poses severe security thread than other jammers. But in reality, the sensor nodes and the jammers in the sensor network are limited with energy. Constant jammers will drain the battery quickly because of continuously injecting the data into the medium. Reactive jammer injects data packet to destroy the original data packet transmitted by the normal node. In contrast to constant jammer, the reactive jammer injects the data packet only when it senses the original data packet in the medium. Due to this, the lifetime of the reactive jammer with respect to energy consumption is certainly higher than the constant jammer. Therefore, from the attackers

Fig. 8 The average PDR distribution of CMs with various types of jamming with various probabilities. Representation of average PDR distribution in cluster members (CM1, CM2, CM3, CM4, and CM5) with various probabilities 0.001, 0.01, 0.05, and 0.1

point of view, it is concluded that the reactive jammer (consumes energy only when the normal node is transmitting the data) is more effective than a constant jammer with respect to energy constraint.

4.3 Performance evaluation metrics

Generally, the CH identifies whether its members are in usual or unusual condition. The CH may not identify the member as in unusual condition or CH may inaccurately identify the CM as in usual condition. In order to detect the CMs accurately as in usual condition or in unusual condition, the detection of CMs may be categorized into (i) true detection, (ii) false detection, and (iii) undetection. The true detection is defined as CH that accurately detects the member as unusual when that member is jammed. The false detection is defined as CH that wrongly detects the member as unusual though that member is usual. The undetection is defined as CH that wrongly detects the member as usual although the member is actually jammed.

The factors that are used to compute the performance metrics, namely true detection ratio (TDR), false detection ratio (FDR), and undetection ratio (UDR), are given as follows:

1. True positive indicator (TP) represents the number of accurately detected jammed members.
2. True negative indicator (TN) represents the number of accurately detected usual members, but the members are actually not jammed.
3. False positive indicator (FP) represents that the members are jammed but they are actually not jammed.
4. False negative indicator (FN) represents that the members are not jammed but they are actually jammed.
5. True positive ratio (TPR) is the number of accurately detected jammed members to the total number of members actually jammed.
6. True negative ratio (TNR) is the number of accurately detected usual members (members who are not jammed) to the total number of usual members.
7. False positive ratio (FPR) is the number of members inaccurately detected as jammed to the sum of members who are detected as jammed and number of members who are actually not jammed.
8. False negative ratio (FNR) is the number of members inaccurately detected as usual to the sum of members who are detected as not jammed and the number of members who are actually jammed.

In this paper, TDR , FDR , and UDR are computed based on the parameters TPR, FNR, FPR, respectively. TDR is defined as the ratio of the number of members that are

accurately detected by the CH to the number of members that are exactly affected by the jammer. The TDR is computed as follows:

$$TDR = TP/(TP + FN) \qquad (4)$$

FDR is defined as the ratio of the number of members that are inaccurately detected by the CH to the number of members that are not actually affected by the jammer. That is, a member is in usual condition but it has been wrongly detected as unusual. The FDR is computed as follows:

$$FDR = FP/(FP + TN) \qquad (5)$$

UDR is defined as the ratio of the number of members that are not detected by the CH to the number of members that are actually affected by the jammer. The UDR is computed as follows:

$$UDR = FN/(TP + FN) \qquad (6)$$

The JMR is defined as the ratio of the number of members successfully jammed by the jammer to the number of members falling within the coverage range of the jammer (number of members covered by the jammer). The JMR is computed as follows:

$$JMR = SJ/FJ, \qquad (7)$$

where SJ represents number of members successfully jammed by the jammer and FJ represents number of members falling within the coverage range of the jammer.

The chi-square test is used to measure the performance difference between experimental values (from simulation results) and anticipated values. The chi-square test is applied after the simulations. A cluster of hundred members (CM1 to CM99 and CH21) is considered. The simulation setup for this scenario is made in such a way that 15 members (CM1 to CM15) are affected by a jammer and the rest of the CMs are not affected by a jammer. The degree of freedom is calculated as 2 (as the number of groups are 3: normal, low, and high), and the level of significance is assumed to be 0.05 with the corresponding table value of 5.9915 for 95 % of confidence interval. The results are shown in Table 11 (result for one of the simulation is considered). In Table 11, CD denotes the members

correctly detected by JDF when the node is jammed, ID denotes the members who are incorrectly detected as abnormal by JDF when the node is in normal condition, and U denotes the members who are incorrectly detected as normal by JDF when the node is in abnormal condition.

The result passes the chi-square test as the total under $(E - A)^2/A$ is 0, which is lesser than the chi-square table value (5.991). Hence, there is no difference between the observed and anticipated values. The level of significance is 0.05. This states that the reliability of the result is 95 %, i.e., the obtained result is considered to be correct by 95 % and the chance of obtained result to be wrong by 5 %. Therefore, the result of the proposed system is significiantly encouraging.

As discussed before, the PDR threshold value is fixed as 74.75 % (based on the result of T test with the probability of 99.9). Various types of jamming is launched. The TDR, FDR, and UDR are determined based on the PDR threshold (74.75 %). The mean TDR and FDR from these simulations are collected for different jammed members under various configurations for different types of jammers such as constant, deceptive, random, and reactive jammers. In the simulation, the configuration is changed by changing the total number of members in the cluster as 5, 50, and 100. Figs. 9, 10, and 11 show the values of TDR, FDR, and UDR for different types of jammers under various configurations with probability $p = 0.001$. This states that the reliability of the result is 99.9 %, that is, the obtained result is considered to be correct by 99.9 % and the chance of obtained result to be wrong by 0.1 %.

Similarly, the T test is performed for other probabilities (p) such as 0.01, 0.05, and 0.1. The process of computing the t value for other probabilities is not included in the paper due to space constraint. However, the results are given as follows:

- T test is performed with four samples of PDR observed from members CM1, CM2, CM3, CM4, and CM5. The degree of freedom is computed as 3, and the level of significance is 0.01 with the corresponding t value being 5.9 for 99 % of confidence interval. The result passes the t test. The t table value of t test is 5.84. From the observation, it is

Table 11 Chi-square test result for one of the simulations

GML	MinC (E)	MbyA (A)	$\frac{(E-A)^2}{A}$	CD	ID	U	TDR = 100.CD/A (%)	FDR = 100.ID/A (%)	UDR = 100.U/A (%)
High	15	15	0	15	0	0	100	0	0
Normal	20	20	0	20	0	0	100	0	0
Low	65	65	0	65	0	0	100	0	0
Total	100	100	0	100	0	0	100	0	0

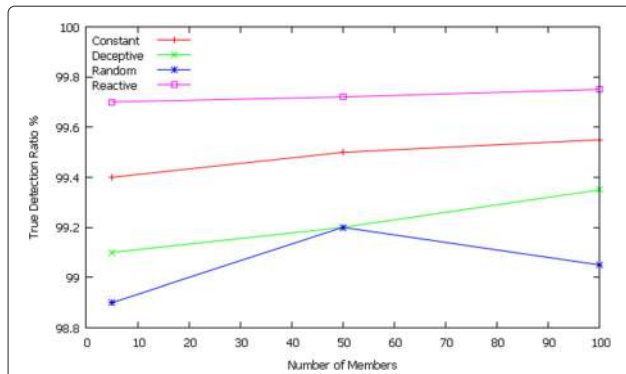**Fig. 9** TDR for different jamming of various configurations of $p = 0.001$
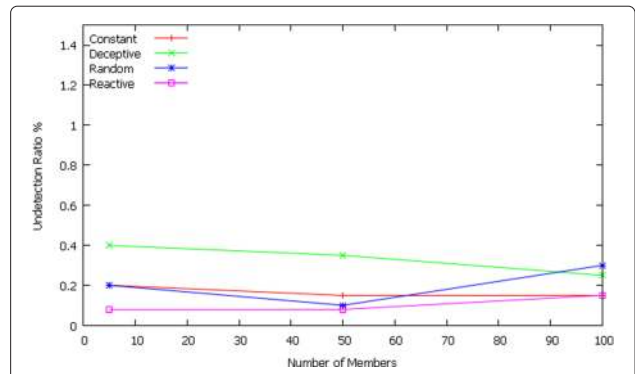

Fig. 11 UDR for different jamming of various configurations of $p = 0.001$

noted that the t value (5.9) exceeds the table value (5.84). This proves that there is significance and the PDR threshold is fixed as 77 %. Similar to the probability 0.001, the experiment is repeated for the probability 0.01. The mean TDR and FDR from these simulations are collected for different jammed members under various configurations for different types of jammers such as constant, deceptive, random, and reactive jammers. In the simulation, the configuration is changed by changing the total number of members in the cluster as 5, 50, and 100. Figs. 12, 13, and 14 show the values of TDR, FDR, and UDR for different types of jammers under various configurations with probability $p = 0.01$. This states that the reliability of the result is 99 %, that is, the obtained result is considered to be correct by 99 % and the chance of obtained result to be wrong by 1 %.

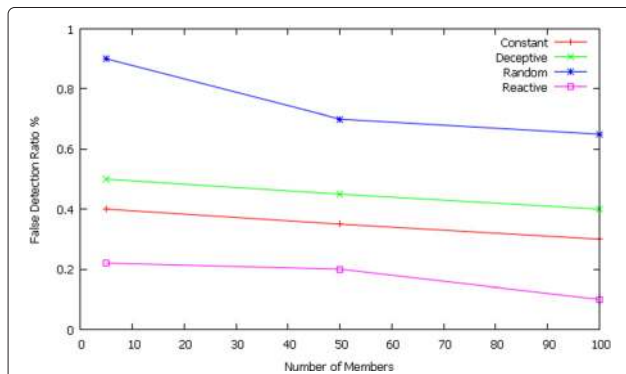- T test is performed with four samples of PDR observed from members CM1, CM2, CM3, CM4, and CM5. The degree of freedom is computed as 3, and the level of significance is 0.05 with the corresponding t value being 3.23 for 95 % of confidence interval. The result passes the t test. The t

table value of t test is 3.18. From the observation, it is noted that the t value (3.23) exceeds the table value (3.18). This proves that there is significance and the PDR threshold is fixed as 73.75 %. Similar to the probability 0.01, the experiment is repeated for the probability 0.05. The mean TDR and FDR from these simulations are collected for different jammed members under various configurations for different types of jammers such as constant, deceptive, random, and reactive jammers. In the simulation, the configuration is changed by changing the total number of members in the cluster as 5, 50, and 100. Figs. 15, 16, and 17 show the values of TDR, FDR, and UDR for different types of jammers under various configuration with probability $p = 0.05$. This states that the reliability of the result is 95 %, that is, the obtained result is considered to be correct by 95 % and the chance of obtained result to be wrong by 5 %.

- T test is performed with four samples of PDR observed from CMs CM1, CM2, CM3, CM4, and

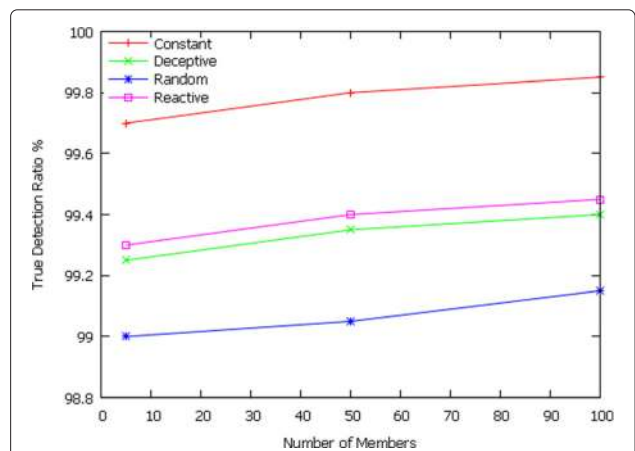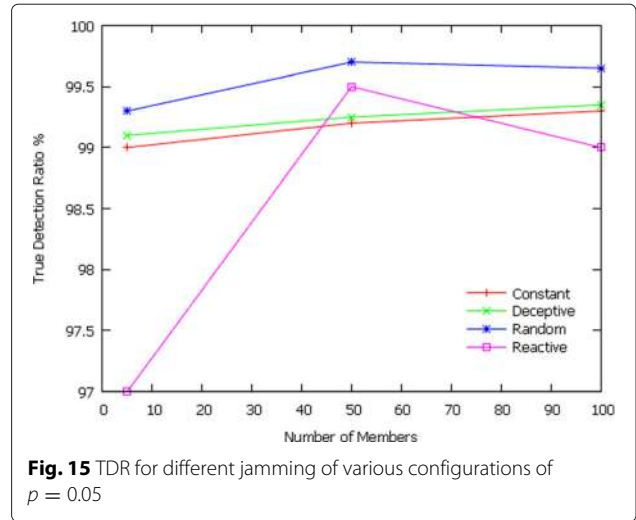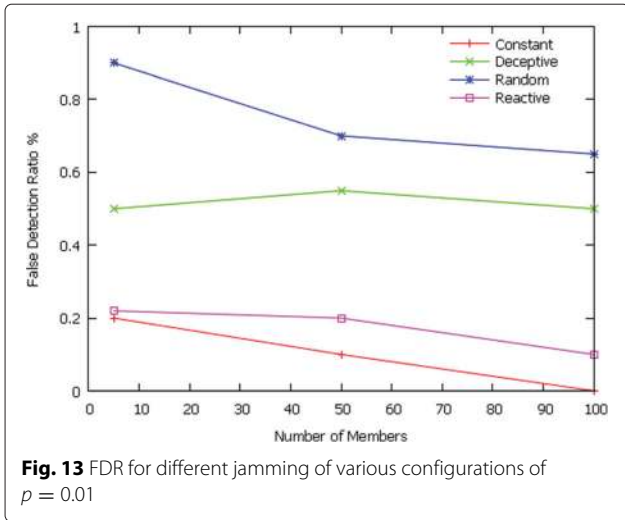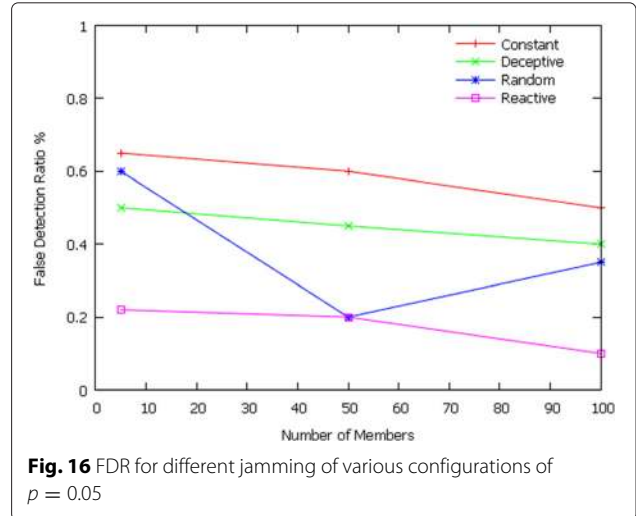**Fig. 10** FDR for different jamming of various configurations of $p = 0.001$

Fig. 12 TDR for different jamming of various configurations of $p = 0.01$

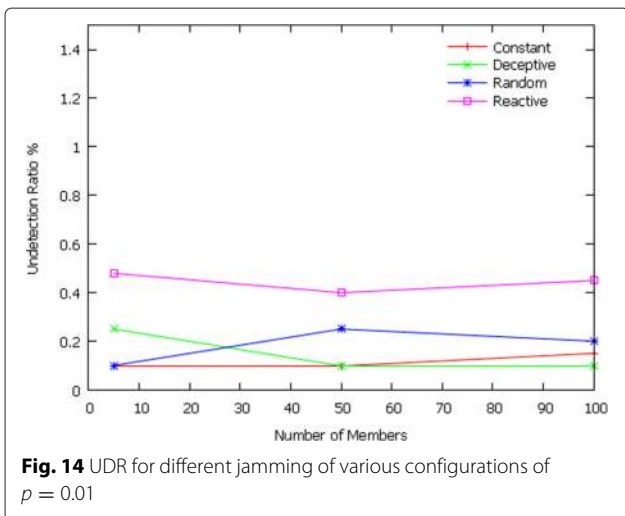**Fig. 13** FDR for different jamming of various configurations of $p = 0.01$

Fig. 15 TDR for different jamming of various configurations of $p = 0.05$
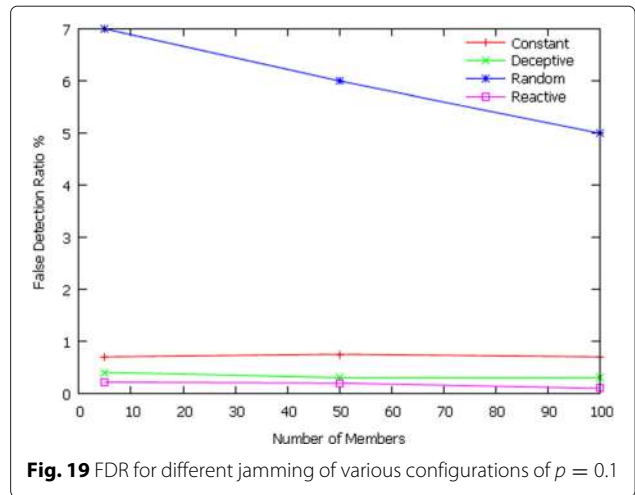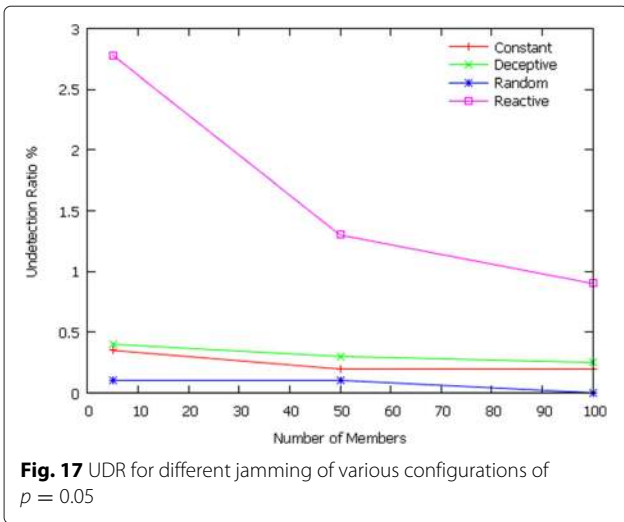
CM5. The degree of freedom is computed as 3, and the level of significance is 0.1 with the corresponding t value being 2.39 for 90 % of confidence interval. The result passes the t test. The t table value of t test is 2.35. From the observation, it is noted that the t value (2.39) exceeds the table value (2.35). This proves that there is significance and the PDR threshold is fixed as 62.5 %. Similar to the probability 0.05, the experiment is repeated for the probability 0.1. The mean TDR and FDR from these simulations are collected for different jammed members under various configurations for different types of jammers such as constant, deceptive, random, and reactive jammers. In the simulation, the configuration is changed by changing the total number of members in the cluster as 5, 50, and 100. Figs. 18, 19, and 20 show the values of TDR, FDR, and UDR for different types of jammers under various configuration with probability $p = 0.1$. This

states that the reliability of the result is 90 %, that is, the obtained result is considered to be correct by 90 % and the chance of obtained result to be wrong by 10 %.

Initially, the PDR threshold (PDR Threshold) is fixed based on the result of the T test discussed in Section 2.5.2. The PDR Threshold is fixed as 74.75, 77, 73.75, and 62.5 % for the confidence levels at 99.9, 99, 95, and 90 %, respectively. The proposed JDF is simulated based on various PDR Thresholds and RSSI Threshold, for measuring the performance in terms of performance evaluation metrics (TDR, FDR, and UDR). From the results, it is observed that the proposed system with confidence levels at 99.9, 99, and 95 % detect all types of jamming and the proposed system with confidence level at 90 % detects constant, deceptive, and reactive jammings and does not detect random jamming. It is also noted that among chosen confidence level for simulation, the proposed system with

Fig. 14 UDR for different jamming of various configurations of $p = 0.01$

Fig. 16 FDR for different jamming of various configurations of $p = 0.05$

Fig. 17 UDR for different jamming of various configurations of $p = 0.05$

Fig. 19 FDR for different jamming of various configurations of $p = 0.1$

confidence level at 99 % works well (TDR = 99.8 % and FDR = UDR = 0).

Now, the performance evaluation metrics of the proposed system is compared for confidence level at 99 % with the existing system [8]. From Table 12, it is noted that the proposed system for confidence level at 99 % works better than the existing system. The reliability of the proposed system result is 99 %. That is, the obtained result is considered to be correct by 99 % and the chance of obtained result to be wrong by 1 %. The proposed system for confidence level at 99 %.

To the best of our knowledge, none has considered jammer intrusion detection and jamming detection in the cluster-based WSN. But research work on jammer and jamming detection are carried out in other kinds of network such as IEEE 802.11b wireless network [23], IEEE 802.11 network [24], and IEEE 802.11 wireless LAN [25]. This lies as the motivating factor behind the design and

implementation of proposed JDF. However, in order to provide a holistic research insight on jammer and jamming detection, the proposed JDF is compared with recent research works on jammer and jamming detection in other modern networks as given in Table 13.

4.4 Energy consumption

Theoretical- and simulation-based energy consumption analyses of JDF are performed, and these analyses are bases to evaluate the trade-off within a WSN. The theoretical energy consumption analysis incudes (i) analysis on energy consumption in the normal scenario, (ii) analysis on energy consumption on jammer intrusion detection (JID), and (iii) analysis on energy consumption on jamming detection (JD).

Analysis on energy consumption based on theoretical model:

In sensor network, the node's energy is consumed due to data packet transmission, data packet reception, and computations performed by nodes. Theoretical energy
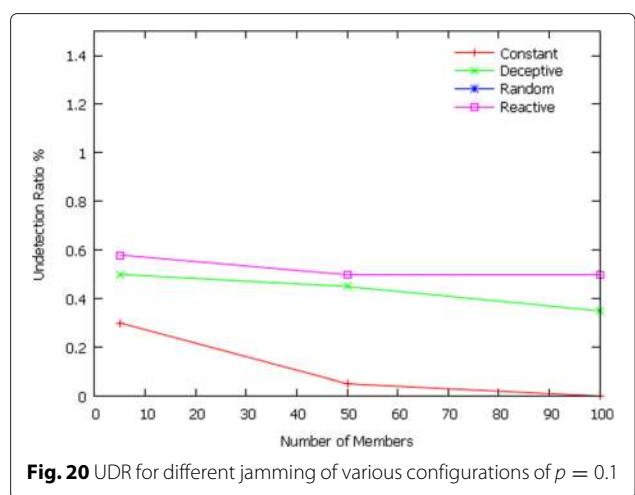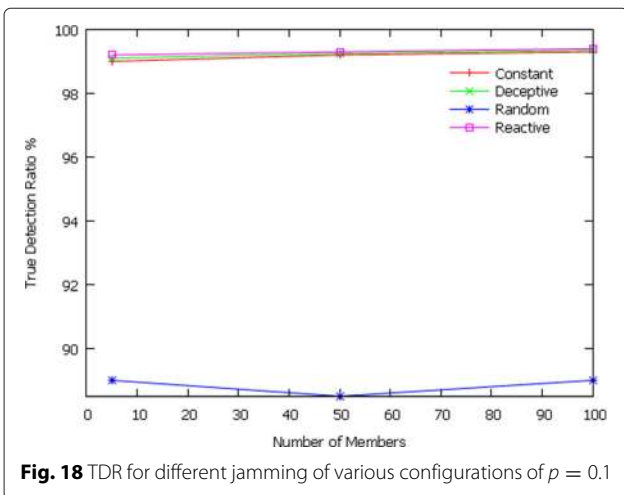

Fig. 18 TDR for different jamming of various configurations of $p = 0.1$

Fig. 20 UDR for different jamming of various configurations of $p = 0.1$

Table 12 Comparison of maximum TDR, minimum FDR, and UDR for various jammers for different probabilities and existing system

Probabilities		Types of jammer			
		Constant	Deceptive	Random	Reactive
$P = 0.001$	TDR	99.55	99.35	99.2	99.75
	FDR	0	0.5	0.65	0.1
	UDR	0.15	0.25	0.1	0.08
	FDR (JMR = 100)	0	0	0	0
	UDR (JMR = 100)	0	0	0	0
$P = 0.01$	TDR	99.88	99.4	99.15	99.45
	FDR	0	0.5	0.65	0.1
	UDR	0.15	0.25	0.1	0.08
	FDR (JMR = 100)	0	0	0	0
	UDR (JMR = 100)	0	0	0	0
$P = 0.05$	TDR	99.3	99.35	99.7	98.5
	FDR	0.5	0.4	0.2	0.1
	UDR	0.2	0.25	0	1.3
	FDR (JMR = 100)	0	0	0	0
	UDR (JMR = 100)	0	0	0	0
$P = 0.1$	TDR	99.3	99.345	89	99.4
	FDR	0.7	0.3	5	0.1
	UDR	0	0.35	4	0.5
	FDR (JMR = 100)	0	0	0	0
	UDR (JMR = 100)	0	0	0	0
Existing system (7)	TDR	99.5	99.5	99.1	99.25
	FDR (Jnr = 100)	0	0	0	0

Table 13 Comparison of the proposed system with the existing systems in various networks

S.No.	Types of network	Types of jammer	Detection metrics	True detection	False detection	Undetection
1	IEEE 802.11b wireless network [23]	Constant	PDR			
		Intelligent	Signal strength variation	Yes	Not clear	Nil
		Random	Pulse width			
		Reactive				
2	IEEE 802.11 network [24]	Constant				
		Deceptive	PDR	Yes	Yes	Nil
		Random				
		Reactive				
3	IEEE 802.11-based wireless LAN[25]	Jammer/cheater	Beacon access time	Yes	Not clear	Nil
4	Cluster-based WSN (proposed JDF)	Constant				
		Deceptive	PDR	Yes	Yes	Yes
		Random	RSSI			
		Reactive				

consumption is modeled by assuming the energy consumption for packet transmission, reception, and computation based on [26].

(i) *Analysis on energy consumption in normal scenario*:

In the proposed system, distance between the CM and CH, between cluster heads, and between cluster head and base station (BS) is considered as one hop as shown in Fig. 1. In general, energy consumed for transmission and reception of data packets in WSN (EC) is expressed as follows:

$$\text{EC} = n_1 E_t + n_2 E_r \tag{8}$$

where E_t is the energy in millijoules (mJ) to transmit a packet over one hop distance, E_r is the energy in mJ needed to receive a packet over one hop distance, n_1 represents the total number of data transmitted, and n_2 represents the total number of data received.

(ii) *Analysis of energy consumption for jammer intrusion detection component of JDF*:

To detect the jammer intrusion, the verification and validation algorithm uses CHC. The CHC is used for node authentication. When a new member enters into a cluster, the CH requests the CHC. So the CHC is transmitted by the member. The total energy consumption for jammer intrusion detection component (ECJIDC) of JDF is expressed as follows:

$$\text{ECJIDC} = n_1 E_t + n_2 E_r + N(n_1 \text{EN}_t + n_2 \text{EN}_r)H + \text{EP} \tag{9}$$

where N represents the number of data packets transmitted with respect to jammer intrusion detection, EN_t is the energy in mJ to transmit a CHC packet over one hop distance, EN_r is the energy in mJ needed to receive a CHC packet over one hop distance, EP denotes the energy in mJ based on computational cost of various modules in verification and validation algorithm, and H denotes the number of hops. In the case of jammer intrusion detection, CM transmits CHC to CH for authentication and the distance between CM and CH is considered as one hop distance. Therefore, the value of N and H is considered as 1. Energy consumption due to jammer intrusion detection component alone excluding energy consumption of regular data packet communication during normal scenario is given as follows:

Exclusive Energy Consumption due to $\text{JID} = \text{ECJIDC} - \text{EC}$
$$\tag{10}$$

(iii) *Analysis on energy consumption due to jamming detection component of JDF*:

In the auditing algorithm, the behavior of the members are determined periodically by using two jamming detection metrics such as packet delivery ratio (PDR) and received signal strength indicator (RSSI). Auditing algorithm is implemented in CH. This algorithm computes

the PDR, maximum PDR, and malicious level of CMs in the cluster periodically. The CH by itself computes the jamming detection metrics (PDR, RSSI), process, and makes decision about jammed and normal conditions. Hence, the CMs are not burdened in computation of jamming detection metrics, processing, and decision-making. Therefore, in the JD component of the proposed JDF, the CH consumes energy only to detect the presence of jamming (processing or computational energy), and the energy consumption due to data packet communication is completely ignored. Energy consumed by JD component (ECJDC) of JDF in joules is expressed as follows:

$$\text{ECJDC} = n_1 E_t + n_2 E_r + H + \sum_{i=1}^{M} \text{EP}_i + JI + JC \tag{11}$$

where M denotes the number of parameter to be computed by the auditing algorithm (PDR, maximum PDR, and malicious level), JI represents the energy consumption to identify the presence of jamming, and JC denotes the energy consumption to classify the type of jamming. The number of hops, H, is considered as 1. M is considered as 3 since the auditing algorithm computes only three parameters viz, PDR, maximum PDR, and malicious level.

Exclusive energy consumption due to JD component of JDF is given as follows:

Exclusive Energy Consumption due to $\text{JD} = @\text{ECJDC} - \text{EC}$
$$\tag{12}$$

Theoretical energy consumption analysis:

In Fig. 1, the CH21 has to send ten packets to every CM (total number of packets to be transmitted to its all CMs is 50). In the normal scenario, the CH receives acknowledgement for the transmitted packet. Therefore, in the corresponding cluster, the total number of packets to be transmitted to the CMs is 50 and total number of acknowledgement to be received from CMs is 50.

The sensing and communication range of the sensor node is fixed as 20 m, the energy consumption for data transmission and reception is considered as 0.526 and 0.11 mJ/packet, respectively, and the computational or processing energy consumption is considered as 0.1 mJ/module [26].

Using (8), the energy consumption in the normal scenario is computed as follows: $\text{EC} = 10*0.526+10*0.11 = 5.26 + 1.1 = 6.36$ mJ.

Using (9), total energy consumption for ECJIDC is computed as follows: (it is assumed that the CM5 likes to move from cluster CH21 to CH22. At this time, CM5 sends request to join in a new cluster. The new CH demands CHC from CM5. CM5 provides its CHC to new CH. New CH processes the CHC and declares whether the CHC is valid or not), $\text{ECJIDC} = 10*0.526 + 10*0.11 + 1*(2*0.526 + 2*0.11)*1 + 5 = 12.632$ mJ.

Using (10), the exclusive energy consumption due to JID is computed as follows:

Exclusive Energy Consumption due to JID $= 12.632 - 6.36$ mJ $= 6.272$ mJ.

Using (11), the total energy consumption for ECJDC is computed as follows. Consider the CH21. CH21 has to compute the parameters PDR, maximum PDR, and malicious level. To compute these parameters, separate modules are present in the auditing algorithm. Jamming identification is done based on the computed parameter (malicious level). Once the presence of jamming is detected, then classification of jamming is done with the help of classification module. ECJDC $= 10 * 0.526 + 10 * 0.11 + 1 + 0.9 + 0.5 + 0.1 = 8.86$ mJ.

Using (12), the exclusive energy consumption due to JD is computed as follows:

ExclusiveEnergyConsumptionduetoJD $= 8.86 - 6.36 = 2.5$ mJ

Theoretically, to illustrate the energy consumption of CHs without mobility and with mobility, three set of samples of energy is considered. In Figs. 21 and 22, X-axis denotes the cluster head and Y-axis denotes energy in mJ. The variety of color bars in Fig. 21 indicates the energy consmption of CHs due to JIDC component and JDC component without mobility. The simulation setup for the scenario (without mobility) is made in such a way that data communication is done between CH and CMs. At this time, CH by itself computes the jamming detection metrics to detect the presence of jamming in JIDC. From Fig. 21, it is evident that the energy consumption of CHs in the normal scenario and JIDC are same (that is, 6.36 mJ) and JDC is accurately 8.86 mJ. The variety of color bars in Fig. 22 indicates the energy consumption of CHs due to the JIDC component (when a CM desires to move from one cluster to another) and JDC component with mobility. The simulation setup for the scenario (with mobility) is made in such a way that data communication is done between CH and CMs. At this time, the CM5 desires to move from the present cluster to another cluster and
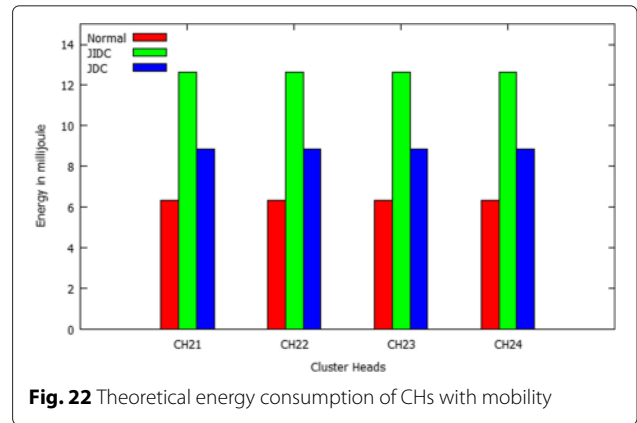

Fig. 22 Theoretical energy consumption of CHs with mobility

CH by itself computes the jamming detection metrics to detect the presence of jamming in JIDC. From Fig. 22, it is evident that the energy consumption of CHs in normal, JIDC, and JDC are accurately 6.36, 12.632, and 8.86 mJ, respectively.

The proposed JDF detects the jammer intrusion when a CM likes to move from the present cluster to another; also, it detects and declares the presence of jamming periodically say every 3 s. Therefore, the JDF consumes 12.632 mJ to detect the jammer intrusion and consumes 8.86 mJ to detect the presence of jamming. The simulation is done for 600 s as discussed in Section 4.2. At the outset, the simulation is carried out without mobility. After that the simulation is continued with mobility. (Initially, the constant jammer is launched then set of samples is considered without mobility and with mobility in the network. Similarly, the simulation is repeated for other types of jammer).

To illustrate the energy consumption of CHs without mobility and with mobility, a set of three samples of energy is considered. In Figs. 23 and 24, X-axis denotes the cluster heads and Y-axis denotes energy in mJ. The variety of color bars in Fig. 23 indicates the energy consumption of
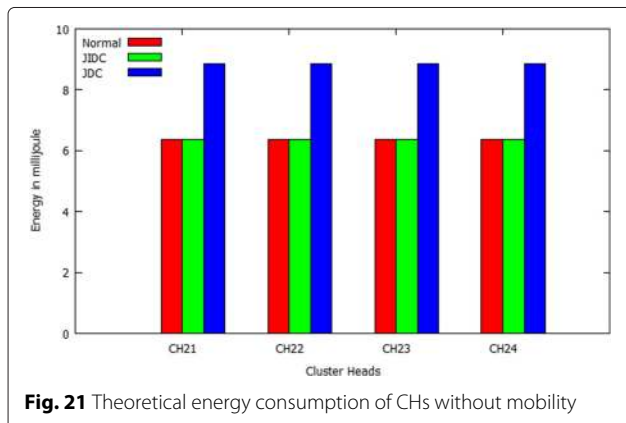

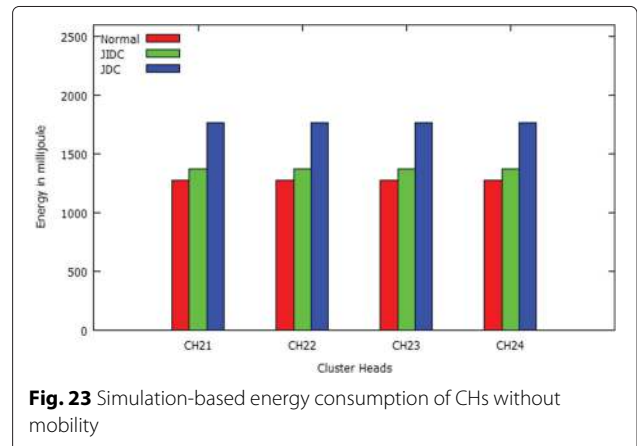**Fig. 21** Theoretical energy consumption of CHs without mobility

Fig. 23 Simulation-based energy consumption of CHs without mobility
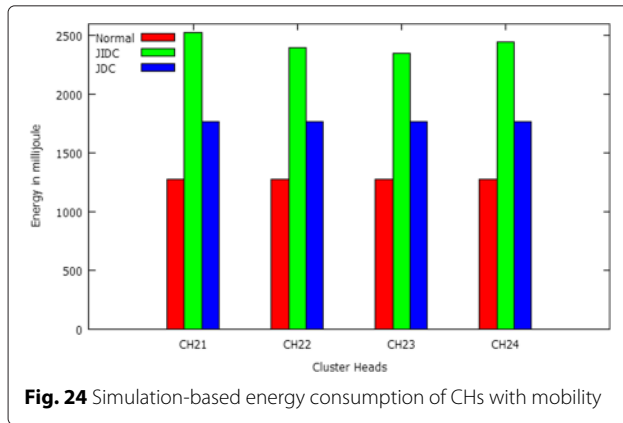
Fig. 24 Simulation-based energy consumption of CHs with mobility

CHs due to JIDC component and JDC component without mobility. The simulation setup for the scenario (without mobility) is made in such a way that data communication is done between CH and CMs. At this time, CH by itself computes the jamming detection metrics to detect the presence of jamming in JIDC. From Fig. 23, it is evident that the energy consumption of CHs in the normal scenario is 1272 mJ, JIDC is 1372 mJ (since it involves in generation, distribution, and updation of CHC) and JDC is around 1772 mJ (since every 3 s, it detects for the presence or absence of jamming). The variety of color bars in Fig. 24 indicates the energy consumption of CHs due to JIDC component (when a CM desires to move from one cluster to another) and JDC component with mobility. The simulation setup for the scenario (with mobility) is made in such a way that data communication is done between CH and CMs. At this time, the CM desires to move from present cluster to another cluster and CH by itselft computes the jamming detection metrics to detect the presence of jamming in JIDC. From Fig. 24, it is evident that the energy consumption of CHs in normal, JIDC, and JDC are around 1272, 2400, and 1772 mJ, respectively.

5 Related work

There are several attacks in the sensor networks which are categorized into routing attacks and data traffic attacks. The data traffic attacks are classified as jamming, wormhole, selective forwarding, sinkhole, and sybil attack [27, 28]. The jamming attack is focused in this paper.

Four types of jamming models, namely constant, deceptive, random, and reactive jammer, are presented in [7]. These jamming models are used in the wireless networks and are experimented for detecting the presence of jamming. The invented jamming detection mechanism was experimented by using MICA2 mote platform. Initially, the jamming detection metrics such as signal strength, carrier sensing time, packet delivery ratio, or packet sent ratio were used independently to detect the presence of jamming. It is noted from the experiments that one of the jamming detection metrics by itself cannot detect the presence of jamming. Hence, the consistency check mechanism is devised in order to enhance the detection. This uses packet delivery ratio to detect the presence of jamming and consistency check to assess whether the packet delivery ratio is affected by jamming. The signal strength or location information is used as a consistency check. The overheads in this mechanism are (i) the nodes are heavily loaded due to collection of neighbor node's metric and decision-making are done at node level; (ii) the collected neighbor node's metrics are stored and processed for decision-making; therefore, this leads to increased time and space complexity; (iii) communication overhead due to collection of neighbor node's metrics to make decision; (iv) if a node does not have neighbor node, then the presence of jamming cannot be determined precisely; and (v) the consistency check uses location information that entails GPS hardware or localization techniques.

The jamming detection mechanism used packets dropped per terminal and signal-to-noise ratio or bad packet ratio as jamming detection metrics to detect whether a node is affected due to jammer or not [8]. All the nodes in the network have to compute the jamming detection metrics and send it to the base station at a regular interval. Then, the base station makes decision about jammed or non-jammed condition. The overheads are (i) all the nodes in the network have to send the computed metrics to the base station for decision-making; thus, it leads to communication overhead, and (ii) this mechanism does not support mobility since the nodes are fixed in the network.

Two jamming detection algorithms are proposed to detect the presence of different jamming attacks in the sensor network [9]. The fundamental algorithm is referred as basic jamming detection mechanism, in which bad packet ratio, packet delivery ratio, and energy consumption metrics are used to determine the existence of jamming. In order to determine this, these metric values are compared with their corresponding thresholds. If the metric values are smaller than their threshold, then there is an existence of jamming. Otherwise, there is no jamming. Secondary algorithm referred as advanced jamming detection mechanism uses additional variables and flags in order to improve the fundamental algorithm in detecting jamming attacks. The limitations are (i) the computation of metrics and decision-making are made at node level and (ii) every node collects its neighbor node's metrics, stores, and makes decision for determining the presence of jamming. Therefore, this leads to increased time, space complexity, and communication overhead. A novel jamming detection approach is proposed to detect the presence of reactive jamming attacks. This approach used bit error rate and received signal

strength to detect the individual packet bit errors. In [10], predetermine knowledge, error correcting code or error detecting code, and wired node chains are discussed. The proposed approach are assessed statistically and experimented on COTS BT nodes and Tmote Sky node. However, this approach can detect only reactive jamming and cannot detect other jamming attacks.

The wireless sensor networks require a mechanism to detect the presence of jamming and secure the nodes from jamming since the sensor nodes are employed in dynamic environment. In [16], the jamming attacks and securing sensor networks from jamming are reviewed. The multimodal method was proposed to detect the presence of jamming. Two avoidance approaches were presented. The first entails the sensor networks tuning its operating frequencies, and the second approach is appropriate for mobile sensor networks and nodes are relocated themselves. The competition approach employs power control and code throttling to compete with the interferer by adjusting resources. In [17], the vulnerabilities of the wireless sensor network, various types of jamming attacks, and countermeasures against jamming were discussed. It is also classified into proactive, reactive, and mobile-agent-based countermeasures. In [18], a minimax robust detection framework is proposed to monitor the node's misbehavior in the MAC layer. It is discussed how an invader masks the event by jamming part of the nodes in the network [19]. In order to prevent the sensor nodes from the attacker, a suitable model is proposed, and it uses probabilistic wormholes that depend on wires, frequency hopping, and uncoordinated channel hopping. The monitor nodes are employed in the sensor network that detects the presence of jammer [20]. If the monitor node identifies the jammer node, then it sends a warning message beyond the jamming region. The proposed approach in [21] admits a receiver to detect the jamming, if it receives primary message excluding secondary message. The code tree approach offers input to the physical layer in order to evade the jammers. From the simulation results, it is observed that the jamming is effectively mitigated in the broadcast wireless system. And the monitors are deployed in wireless sensor networks and they employ an optimal sequence hypothesis test to detect the jamming condition [22]. A method is proposed to calculate the optimal strategies for jamming attacks and for securing network. Additionally pareto-dominated and risk-dominated strategies are proposed and numerical experiment is achieved.

The detection of jamming in the existing approaches is node centric or BS centric [7–10] where the individual nodes involve in collecting and processing the respective node's metric and neighbor nodes' metric such as packet send ratio (PSR) [7], packet delivery ratio (PDR) [7], signal-to-noise ratio (SNR) [8], bad packet ratio (BPR) [8, 9], energy consumption amount (ECA) [9], and bit error

rate (BER) [10]. These metrics are used either individually or collectively to make the decision about "jammed situation" or "non-jammed situation". Collectively, the metrics PSR, PDR, BPR, and BER are termed as jamming induction metrics (JIM). In the proposed system, the metrics PDR and RSSI are combinely considered to be the JIM metrics. The overhead in the existing approaches are (i) the complete processing and decision-making are done at the node level causing elevated time and space complexity (because collecting, storing, and processing JIM induce additional overhead); (ii) the presence of jamming is not detected precisely, if the node has no neighbor (because node would not have sufficient knowledge of neighbor nodes JIM, to determine the presence of jamming); and (iii) communication overhead (because JIM has to be collected from the neighbor nodes which injects additional traffic into the system). Therefore, a novel jammer detection framework with a nominal overhead and an acceptable detection rate is in need to be devised. This paper addresses this research gap by introducing a three-step novel jammer detection framework. In addition to jammer intrusion detection, jamming detection is also carried out in this paper.

6 Conclusions

A novel jammer detection framework is proposed to detect the presence of jammer and jamming in the cluster-based wireless sensor networks. The proposed jammer detection framework comprises the following three key elements: (i) The metric PDR is combined with the metric RSSI for jamming detection; (ii) statistical tests are performed to find out the threshold of detection metrics and to classify various types of jamming; and (iii) a three-step framework such as verification, validation, and auditing to detect both jammer intrusion and jamming. The proposed JDF performs well against the existing jamming detection approaches. The proposed jammer detection framework is simulated in NS2 simulator. The simulation is carried out to determine the TDR, FDR, and UDR for various confidence levels at 99.9, 99, 95, and 90 %. The proposed system with the confidence level at 99 % performs better than the proposed system with various confidence levels at 99.9, 95, and 90 %. Finally, the proposed system is compared with the existing system, and it is concluded that proposed system with confidence level at 99 % performs better than the existing system. The future work direction includes determining the position of jammer node in the cluster and posterior action on jamming.

References
1. IF Akyildiz, W Su, Y Sankarasubramaniam, E Cayirci, Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. E Shi, A Perrig, Designing secure sensor networks. IEEE Commun. **11**(6), 38-43 (2004)
3. L Xuxun, A survey on clustering routing protocols in wireless sensor networks. Sensors. **12**, 3–11153 (2012)
4. T Shon, Y Park, A hybrid adaptive security framework for IEEE 802.15.4-based wireless sensor networks. KSII Trans. Internet Inf. Syst. **3**, 6 (2009)
5. A Davis, C Hwa, in *IEEE Conference on Technologies for Homeland Security (HST)*. Airport protection using wireless sensor networks (IEEE, USA, 2012), pp. 36–42
6. G Saim, MH Rehmani, C Sunghyun, P Sung-Han, An efficient trajectory design for mobile sink in a wireless sensor network. Elsevier Comput. Electrical Eng. J. **40**(7), 2089–2100 (2014)
7. X Wenyuan, T Wade, Z Yanyong, in *Proceedings of the Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05*. Timothy Wood, The feasibility of launching and detecting jamming attacks in wireless networks (ACM, USA, 2005), pp. 46–57
8. S Misra, R Singh, SVR Mohan, Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Journal of Sensors, 3444–3479 (2010)
9. M Cakiroglu, AT Ozcerit, in *Proceedings of the 3rd International Conference on Scalable Information Systems*. Jamming detection mechanisms for wireless sensor networks (ICST, Belgium, 2008), pp. 1–8
10. S Mario, D Boris, C Srdjan, *Detection of reactive jamming in sensor networks*. (ETH Zurich D-INFK Technical Report 634, ETH, Zurich, Switzerland, 2009)
11. B Mrazovac, MZ Bjelica, D Kukolj, BM Todorovic, D Samardzija, B Mrazovac, *et al*, A human detection method for residential smart energy systems based on ZigBee RSSI changes. IEEE Trans. Consumer Electron. **58**(3), 819–824 (2012)
12. K Benkic, M Malajner, P Planinsic, Z Cucej, in *Proceedings of 15th International Conference on Systems, Signals and Image Processing, IWSSIP 2008*. Using RSSI value for distance estimation in wireless sensor networks based on ZigBee (IEEE, USA, 2008), pp. 303–306
13. KP Vijayakumar, P Ganeshkumar, M Anandaraj, A novel jamming detection technique for wireless sensor networks. KSII Trans. Internet Inf. Syst. **9**(10), 4223–4249 (2015)
14. A Perrig, R Szewczyk, JD Tygar, V Wen, DE Culler, SPINS: security protocols for sensor networks. Wireless Netw. **8**, 521–534 (2002)
15. H Lu, J Li, M Guizani, Secure and efficient data transmission for cluster based wireless sensor networks. IEEE Trans. Parallel Distributed Syst. **25**(3), 750–761 (2014)
16. W Xu, W Trappe, Y Zhang, Jamming sensor networks: attack and defense strategies. IEEE Netw. **20**(3), 41–47 (2006)
17. A Mpitziopoulos, D Gavels, C Konstantopoulos, G Pantziou, A survey on jamming attacks and countermeasures in WSNs. IEEE Commun. Surv. Tutorials. **11**(4), 42–56 (2009)
18. S Radosavac, JS Baras, in *Proceedings of ACM WiSe'05*. A framework for MAC protocol misbehavior detection in wireless networks (ACM, USA, 2005), pp. 33–42
19. M Cagalj, S Capkun, J-P Hubaux, Wormhole-based anti-jamming techniques in sensor networks. IEEE Trans. Mobile Comput. **6**(1), 1–15 (2007)
20. M Li, I Koutsopoulos, P Radha, Optimal jamming attack strategies and network defense policies in wireless sensor networks. IEEE Trans. Mobile Comput. **9**(8), 1119–1133 (2010)
21. JT Chiang, Y-C Hu, Cross-layer jamming detection and mitigation in wireless broadcast networks. IEEE/ACM Trans. Netw. **9**, 1 (2011)
22. Y Zhu, Y Jiang, On optimal antijamming strategies in sensor networks. Int. J. Distributed Sensor Netw. **2012**(2012), 1–9 (2012)
23. N Sufyan, NA Saqib, M Zia, Detection of jamming attacks in 802.11b wireless networks. EURASIP J. Wireless Commun. Netw. **2013**, 208 (2013)
24. O Punal, I Aktas, C-J Schnelke, G Abidin, K Wehrle, J Gross, in *IEEE 15th International symposium on a World of Wireless, Mobile and Multimedia Networks*. Machine learning-based jamming detection for IEEE 802.11: design and experimental evaluation (IEEE, USA, 2014), pp. 1–10
25. GV Eduard, SA Muhammad, LA Elena, A novel cheater and jammer detection scheme for IEEE802.11-based wireless LANs. Comput. Netw. **86**, 40–56 (2015)
26. C-S Jorge, V-R Andres, L-B Andres, R-A EMario, S-R AVictor, On the use of electromagnetic waves as means of power supply in wireless sensor networks. EURASIP J. Wireless Commun. Netw. **2014**, 36 (2014)
27. M Patel, A Aggarwal, in *IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)*. Security attacks in wireless sensor networks: a survey (IEEE, India, 2013), pp. 329–333
28. D Martins, H Guyennet, in *13th International Conference on Network-Based Information Systems (NBiS)*. Wireless sensor network attacks and security mechanisms—a short survey (IEEE, Takayama, Japan, 2010), pp. 313–320