A Novel Jamming Detection Technique for Wireless Sensor Networks

K.P.Vijayakumar[1], P.Ganeshkumar[2] and M.Anandaraj[3]
[1,2,3] PSNA College of Engineering and Technology, Dindigul
Tamil Nadu, India
[1][e-mail: kalkivijay@rediffmail.com]
[2][e-mail: drpganeshkumar@gmail.com]
[3][e-mail: ananddgl@yahoo.com]
*Corresponding author: K.P.Vijayakumar

Received March 2, 2015; revised May 20, 2015; revised July 9, 2015; accepted August 17, 2015; published October 31, 2015

Abstract

A novel jamming detection technique to detect the presence of jamming in the downstream direction for cluster based wireless sensor networks is proposed in this paper. The proposed technique is deployed in base station and in cluster heads. The proposed technique is novel in two aspects: Firstly, whenever a cluster head receives a packet it verifies whether the source node is legitimate node or new node. Secondly if a source node is declared as new node in the first step, then this technique observes the behavior of the new node to find whether the new node is legitimate node or jammed node. In order to monitor the behavior of the existing node and new node, the second step uses two metrics namely packet delivery ratio (PDR) and received signal strength indicator (RSSI). The rationality of using PDR and RSSI is presented by performing statistical test. PDR and RSSI of every member in the cluster is measured and assessed by the cluster head. And finally the cluster head determines whether the members of the cluster are jammed or not. The CH can detect the presence of jamming in the cluster at member level. The base station can detect the presence of jamming in the wireless sensor network at CH level. The simulation result shows that the proposed technique performs extremely well and achieves jamming detection rate as high as 99.85%.

Keywords: wireless sensor networks**,** threats, jammers, packet delivery ratio, received signal strength indicator

http://dx.doi.org/10.3837/tiis.2015.10.026 **ISSN : 1976-7277**

1. Introduction

Sensor networks are usually composed of tiny sensor nodes. Sensor nodes consist of sensing, computing, communicating components and memory. These nodes are deployed in a region called sensor field to sense the environment. Wireless sensor networks (WSNs) are becoming increasingly attractive for numerous application areas ranging from military to healthcare [1-3]. Sensor nodes have very limited memory space, energy, and computational power [4]. These nodes work in an infrastructureless and dynamically changing environment [5] and route the collected data to the sink node for further interpretation. Sensor nodes are self-organized and can be clustered. Clustering results in a two layer hierarchy in which cluster heads (CHs) form the higher layer whereas cluster members form lower layer. Every cluster has cluster head and cluster members. CM communicates with other CMs in a cluster through CH and CHs communicate with other CHs through base station (BS). CM may move from one cluster to another and new node may join in a cluster. Clustering achieves energy efficiency by reclustering, decreases collision, reduces the communication overhead, improves throughput and network lifetime.

In data link layer, the sensor network is vulnerable to jamming attacks [5] and Energy-exhausting attacks [6], because the sensor nodes use wireless medium for data communication [7], the sensor nodes operate at very low radio power [8]. However, this paper mainly focuses on jamming attacks in data link layer for down stream communication in cluster based sensor network. The jamming attacks are launched by the jammers. The jammers aim is to disturb the communication between sensor nodes or corrupt legitimate transmissions of sensor nodes by causing intentional packet collisions at medium. Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks [9]. Hence a mechanism is needed, to detect various type of jamming attacks and to detect the jammer (a node which performs jamming activity).

In the existing literature [10-13] several jamming detection approaches were proposed to detect the presence of jamming in the sensor networks for upstream data communication. However, to the best of our knowledge none of the existing literature had considered the issue of jamming detection during downstream data communication (from base station to sensors) in the wireless sensor networks. Therefore, in this paper, the main idea is to detect the presence of jamming in downstream data communication in the cluster based wireless sensor networks. The need for jamming detection in WSN depends on the type of application. Consider a security application, where sensors are required to detect and identify the presence of a target object. For this application, the sink must send the following information to the sensor nodes: (i) control code (program to reconfigure/retask the sensors to suit the current task of object detection), (ii) database of the target image to help the sensors in finding the target, and (iii) queries containing information about the object detection. Finally the sensors detect the target image and replies to the sink. Therefore in this kind of application, lot of message has to be sent from sink to sensor as opposed to the normal data collection application, in which the data are transferred from sensor to sink.

There are several jamming detection approaches in the existing literature [10-13]. However, the communication and computation overhead in existing approaches is found to be high and these schemes cannot be directly applied to the environment discussed in the above target object detection application due to the following reasons:

1) In this paper, jamming detection in cluster based sensor network for downstream data communication is focused. The downstream communication refers to the communication between the sink node and sensor nodes. In downstream communication, the message is transmitted from sink to sensors. Here the data transmission is broadcasting, whereas in upstream data communication the message is transmitted from the sensor node to sink node and this is referred as unicast communication. Therefore the characteristics of upstream and downstream communication is completely different and thus jamming detection technique designed for upstream communication cannot be applied as such for downstream communication.

2) The jamming detection approach is node-centric or BS centric, where the collection of data, processing and decision making are done by individual nodes or BS deliberately, to make the decision about 'jammed situation' or 'non jammed situation'. Each and every node in the network explicitly involves in this procedure. Thus, the overhead in the existing approaches are, i) the complete processing and decision making is done at the node level (that is, individual node is burdened for computation), ii) communication overhead since BS periodically collects the data from nodes for decision making.

3) The existing approach collects respective node's metric and also the neighbor nodes' metric to make the decision whether the node is jammed or not. The overhead in this approach are, i). increased time and space complexity (because as it is mentioned, all the neighbor node's data have to be collected, stored and processed to make decision), and ii).Presence of jamming is not detected precisely if the node has no neighbor.

The primary motivation of the proposed novel jamming detection technique is to identify the jamming attack within the cluster and outside the cluster. The key ideas of this technique are listed below: 1) In the proposed technique, instead of using flat network as such the cluster based sensor network is considered for down stream communication (from BS to sensors). For this the sensor nodes are grouped into several clusters. Each cluster has a CH and CMs. The message from BS is transferred to all the CHs in the network. In turn the CH transmits the received message to all the CMs under its control. The CH computes the PDR without much computational overhead when the CMs reply to CH by sending acknowledgement. The CH easily measures the RSSI, when the CH receives the acknowledgement and reply for queries sent from BS via CH. This setup has several advantages such as increased scalability, low energy consumption, small size of routing table, limited communication bandwidth, decreased collision and communication overhead, 2) The proposed technique uses CH centric (network centric) approach for detection of jamming in the cluster based sensor network [14]. In this approach, the CH estimates the metrics (PDR, RSSI) and makes decision about 'jammed situation' or 'non jammed situation'. The metrics PDR and RSSI of 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 CH itself without needing the help from the members. Therefore it can be claimed that the CM is not burdened (is not heavily loaded) in the proposed approach, 3) In the proposed approach, CH estimates the data for processing and decision making. CH does not depend on neighbour's data. Therefore the communication overhead is reduced.

The main objective of this paper is to detect the presence of jamming in wireless sensor networks using two jamming detection metrics namely packet delivery ratio (PDR) and received signal strength indicator (RSSI). It is well known fact that jamming deliberately decreases the PDR of jammed node. By roughly examining the PDR of a node, it is not possible to judge whether that node is jammed or not. Therefore proper reference or appropriate experimental results is needed to find the range of PDR for determining the

presence of jamming. Setting up of jamming detection metrics threshold in the existing literature was done based on the reference value published in [10]. In this paper, the statistical tests are performed in order to fix the threshold value of PDR for detecting the presence of jamming and to classify various types of jamming. PDR and RSSI of every member in the cluster is measured and assessed by the cluster head. And finally the cluster head determines whether the members of the cluster are jammed or not. For this the cluster head employs jamming detection technique (JDT). In this paper, JDT works in two steps such as Cluster updation and Jamming Detection. The cluster updation step verifies whether the source node is CM, BS, or new node. The jamming detection step constantly determines the behaviour of the nodes in every cluster. If jamming detection step identifies a node's behaviour is unusual then this step declares that the corresponding node is jammed node. In order to determine the behaviour of CMs, it observes the PDR and RSSI of the CMs periodically. The performance of the proposed system for detecting the presence of jamming is evaluated in terms of true detection ratio (TDR), false detection ratio (FDR) and undetection ratio (UDR).

The main contributions of this paper are summarized as follows: 1) A novel jamming detection technique (section 4.1): This technique consists of two steps. First, it performs verification whenever a packet is received. Finally it observes the behavior of newly joined node and existing node, 2) Jamming detection metrics (section 3.4.3): The proposed technique uses PDR and RSSI of CMs in the network. Jammer detection level is bounded by threshold values of PDR and RSSI, 3) Statistical Proof (section 3.4): Stastical tests are performed for the following, i). The rationality of using PDR and RSSI, ii). To fix the threshold value of PDR, iii). To classify various types of jamming, and iv). To compare the performance of the results obtained from the simulation and the anticipated results (shown in **Table 8**), and 4) Decision Level, jamming circumstance of member is based on the parameters that are estimated, maintained and governed by cluster head unlike existing methods. That is, the estimation of jamming detection metrics and decision making process are done at network centric (cluster head centric), instead of node centric. Therefore, the CMs are not burdened.

The rest of the paper is organized as follows: Related work is presented in Section 2. In Section 3 the system model is presented. Section 4 presents the proposed technique in two aspects: Cluster updation and Jamming Detection. Simulation and discussions on the results are presented in Section 5. Finally, Section 6 concludes this paper.

2. Related Work

In [10] four types of jamming models proposed such as constant jammer, deceptive jammer, random jammer and reactive jammer. The jamming attack detection mechanisms are studied and the experiments are performed using the MICA2 Mote platform. This mechanism used two metrics namely packet send ratio (PSR) and PDR. From the results, it observed that the PSR and PDR were hard to decide about jamming and its types. Then, they devised signal strength consistency check and location consistency check. The signal strength consistency check algorithm uses the corresponding node's PDR and signal strength in order to determine the presence of jamming. The location consistency check algorithm uses the corresponding node's PDR and location of its neighbor. Each node collects and stores its neighbour's location. Based on the corresponding node's PDR and neighbor node's PDR, it can make decision whether the node is jammed or not. In these approaches, each node involves in collection of respective node's metric and neighbor nodes' metric to make the decision about 'jammed situation' or 'non jammed situation'. The overheads in this approaches are: i) the

complete processing and decision making is done at the node level (nodes are burdened for computation), ii) increased time and space complexity since as it is mentioned, all the neighbor node's metric have to be collected, stored and processed to make decision, iii) communication overhead due to collection of neighbor node's metric for making decision, iv) The presence of jamming is not detected precisely if the node has no neighbor, and v) This method requires some additional GPS hardware or localization techniques to locate neighbor nodes location.

In [11] they proposed two jamming detection algorithms for detection of jamming attack in the network. The first algorithm uses three metrics such as bad packet ratio (BPR), PDR and energy consumption amount (ECA) to detect the presence of jamming. If all three metrics are lower than their thresholds then it is declared as there is no jamming, else if only the PDR is above its threshold then it is declared as no jamming. Otherwise, it is announced that there is jamming. The second algorithm is devised to enhance the former one. This algorithm collects the neighbor node's condition for making decision. The overheads in this approaches are: i) the complete processing and decision making is done at the node level, ii) communication overhead, increased time and space complexity since as it is mentioned, all the neighbor node's metric have to be collected, stored and processed to make decision. In [12] two jamming attack detection metircs such as bit error rate (BER) and received signal strength (RSS) used. Each node in the network has to compute and update the BER of all communication links with its one-hop neighbors. But it is hard to compute the BER by a sensor node, since it entails collection of huge data. They proposed a method to detect various type of jammer. This method includes three steps; i) error sample acquisition, ii) interference detection, and iii) sequential jamming test to deduce presence or absence of reactive jamming. This method has a strong statistical foundation and can detect the presence of jamming attacks. But, its limitations are; i) This method cannot classify various types of jamming attacks, and ii) increased computational and space complexity.

In [13] the jamming detection mechanism uses two metrics such as signal to noise ratio (SNR) and BPR. The detection of jamming in this approach is BS centric, where the collection of data, processing and decision making are done by BS to make the decision whether the node is jammed or not. Every node in the network has to report the data (the number of total packets received during particular time period, number of packets dropped during particular period and received signal strength) periodically to the BS for making decision. Its limitations are; i) communication overhead since every node in the network has to report the data periodically to the BS, and ii) the nodes are fixed in the network, so it may not support mobility. In [14] the jammer detection approach used PDR for detection of jamming attack. The overhead in this approach is, the PDR alone is not sufficient to detect the presence of jamming since the factors other than jamming can also influence the data transmission and cause the PDR value to become low.

In [15] they proposed a method for detection of physical layer denial of service (DoS) jamming attack. This method selects only some of the nodes available in the network as monitor node using residual energy. The monitor nodes verify the RSSI and PDR of other nodes for detection of presence of jamming. But its limitation is, it is needed to deploy several monitor nodes in order to cover the entire network. In [16] authors proposed a method for detection of jamming attack in a faster way. This method uses collaborative detection approach, in which only PDR is evaluated in an given area instead of a pair of nodes. They performed jamming attack detection using TelosB motes. The overheads in this method are; i) more energy consumption and exhaust batteries of the nodes shortly since regularly transmitting beacon messages for detection of jamming quickly, and ii) This method can detect only constant jammer, but cannot detect various types of jamming attacks.

Sensor networks need various techniques to preserve them from threats. In [17] the different jamming attacks employed against a sensor network. Two jamming detection approaches proposed. In the first approach, channel surfing or spatial retreat is employed to move away from interferer. In the second approach, Power Control and Code Throttling is used to compete with interferer by adjusting resources. In [18] the security schemes against jamming reviewed and categorized into Detection techniques, Proactive countermeasures, Reactive countermeasures and Mobile agent-based countermeasures. Also presented security mechanism against jamming in wireless sensor networks. In [19] a minimax robust detection framework proposed to detect the node misbehavior at the MAC layer. The work in [20] considered, passing attack notification messages out of a jammed region by creation of wormhole links between sensor nodes, one of which resides out of the jammed area. The links are made through frequency hopping over a channel set either in a predetermined or in an ad hoc manner. In [21] monitor nodes deployed to detect the jammer node. Monitor nodes transfer a notification message out of the jamming region, after detection of the jammer node. In [22] a method presented that allows a receiver to detect jamming attack, if this method observes that a secondary message is received without the primary message. In addition authors proposed code tree method that mitigates jamming when jamming is detected. In [23] Pareto-dominated optimal strategies and risk-dominated strategies proposed for detection of jamming attack and to safeguard from attack. In [24] a lightweight intrusion detection framework integrated for clustered sensor networks is proposed that prevent most routing attacks on sensor networks. In [25] the proposed routing protocols multi-parent hierarchical (MPH), ad hoc on demand distance vector (AODV) and dynamic source routing (DSR) are compared. In order to compare, the metrics such as number of packet retransmissions, carrier sense multiple access (CSMA) inner loop retries, the number of nodes answering the queries from the coordinator (sink) node and the energy consumption are considered. Among these, the MPH greatly tolerates the jamming attacks. In [26] a new method developed to detect the malicious entity for IEEE 802.11 network using a novel metric called Beacon Access Time (BAT). In [27] a novel selfish attack type in cognitive radio ad-hoc networks is identified and proposed simple and efficient technique called COOPON that detect the selfish cognitive radio attack with multichannel resources by cooperative neighboring cognitive radio nodes.

3. System Model

In this section, we first discuss four types of jamming attack models, and then specify the system configuration in which various types of jammers are launched in order to determine the effect of each jammer. Next, the metrics used in the existing and in the proposed work for detection of jamming are described. The proposed work metrics are used to measure the jamming attack effectiveness.

3.1 Jamming Attack Models

In the proposed work, four types of jamming models are used such as constant jammer, deceptive jammer, random jammer and reactive jammer [10]. Constant jammer continuously injects packets (random bits) on the medium in order to jam the entire communication on the channel. The constant jammer does not follow any MAC layer procedure during injection of packets. The deceptive jammer frequently propels usual packets (not random bits) on the medium. It is a hazardous type of attack in which the attackers do not show their presence, because the procedure of MAC layer is followed by deceptive jammer. The random jammer does not inject the packets continuously; instead it switches between jamming and sleeping.

This type of jammer sleeps for T_S random amount of time and jams for T_J random amount of time. The value of T_S and T_J may be either fixed value or random value. So, the power consumption may be reduced by the jammer by changing between sleep mode and jam mode. It can also act as constant jammer or deceptive jammer during jam mode. Reactive jammer observes the channel activity and transmits fake data whenever transmission takes place.

3.2 System Configuration

In downstream data communication, BS transmits data (control code, database and queries) to sensors reliably. Accordingly the sensors reply to sink. The security applications such as target image detection [28], health care applications [29-30] uses downstream data communication and can be modeled either by using flat network or cluster based network. The issues associated with the flat network are, increased collision, increased communication overhead, decreased throughput and energy consumption. Therefore cluster based network is used in the proposed system in order to address the above mentioned issues.

In the system configuration, the black nodes denote CHs, the white nodes denote CMs, the yellow nodes denote jammed CMs and the red node denotes jammer node. The lines denote communication between CH and CM. The arrows denote communication between CHs and BS. The CH21 and members 1 to 5, CH22 and members 6-10, CH23 and members 11-15, CH24 and members 16-20 are formed into four clusters, respectively. The CH is one hop distance with CMs and BS. The simulation is performed in fixed CHs (CH21, CH22, CH23 and CH24). The proposed system is implemented in the topology with fixed CH as depicted in Fig. 1. Therefore the election of CH in the sensor network is not focused in this paper. But in order to elect the CH dynamically, existing clustering algorithms [31-37] can be applied in the proposed JDT. JDT is very flexible to support the deployment of existing clustering algorithm in it and this is considered as future work. The communication range of each node in the network is 5m.

The proposed system can also be implemented in dynamic environment by deploying existing clustering algorithms [31-37] for selecting the cluster head. In this case, the proposed system does not prevent the election of jammer node as CH during the re-election of CH and there is a probability for the CH election algorithm, to elect a jammer node as CH. However in the proposed system, base station can detect the presence of jamming at CH level (because the proposed system is also installed in base station). Therefore in JDT prevention of electing jammer node as CH is absent but detecting the presence of jamming at CH level is present. This may be considered as limitation in the proposed work. In order to avoid the selection of jammer node as CH, the existing trust based clustering election algorithm [38-40] can be applied along with the JDT.

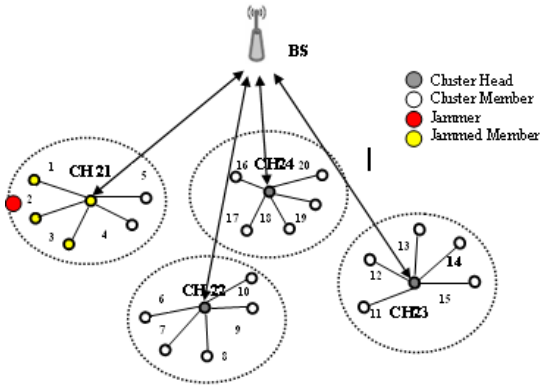

Fig. 1. Wireless Sensor Network with a jammer node

To illustrate the proposed system, a jammer is launched deliberately in the cluster CH21. The proposed system is installed in CH and BS. To understand the interactions of the jamming detection metrics (section 3.4.3) and to measure the impact of a jammer in various scenarios (section 5.2), we have performed simulations in section 5. The simulation is done using various models as discussed in section 3.1. In the simulation, a jammer is launched in the first cluster (CH 21). This cluster consist of a cluster head (CH21) and five members such as M1, M2, M3, M4 and M5. From the simulation result, it is observed that the CH21 identifies that the members M1, M2 and M3 are jammed and the members M4 and M5 are not jammed. It is also evident from the simulation result that the CH has the ability to make distinction between various types of jamming (section 3.4.6). Based on the simulation it is justified that the CH has the ability to identify the jammed members.

3.3 Jamming Detection Metrics in existing literature

The jamming detection metrics used in the existing literature are PSR [10], PDR [10-11] [15-16], Signal Strength and location of neighbors (using GPS) [10], BPR [11] [13], ECA [11], BER [12], received signal strength (RSS) [12], SNR [13] and RSSI [15].

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 defined in the section 3.4.4. The BPR is computed at destination node and it is defined as the ratio of the number of bad packets received by a node to the total number of packets arrived at receiver 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 SNR is defined as the ratio of the received signal power in a node to the received noise power in a node. The RSSI is the ratio of received signal strength to the reference power.

The metrics PSR and PDR were used in [10] to identify the jamming attack. From the results, it was observed that the PSR and PDR were hard to decide about jamming and its types. Then, they devised two algorithms. The first algorithm used the PDR and signal strength in order to determine the presence of jamming. The second algorithm used the PDR and location of its neighbors to determine the presence of jamming. The estimation of PSR is complex task. Additionally, this approach needs localization technique or hardware such as GPS to identify neighbor's location. The metrics PDR, BPR and ECA were used in [11] to detect the presence of jamming. The BPR and ECA are estimated by nodes, accordingly the nodes are burdened. The metric BER and RSS were used in [12] for detection of jamming attacks. But it is hard to compute the BER by a sensor node, since senor node needs to collect huge amount of data. This method cannot classify various types of jamming attacks. The BPR and SNR metrics were used in [13] to detect various jamming attacks. The approach used in [13] causes communication overhead since every node in the network has to report the data periodically to the BS. The SNR is an effective metric to detect the presence of jamming at the physical layer. It is clear from the existing jamming detection metrics that there is no metric or combination of metric 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 in need to be explored.

3.4 Statistical Proof

In this section, we first determine whether various types of jamming influences PDR or not by performing the statistical test (T-Test). The T-Test proves that there is significant difference between the two population means (i.e., observed PDR during jamming free scenario and

observed PDR after launching of jamming). Similarly, the statistical test is performed for PSR, RSSI to determine whether various types of jamming influence PSR, RSSI or not (The statistical test to study the influence of jamming on the metrics PSR and RSSI is not included in the paper due to space constraint). From the T-Tests, it is noticed that the metrics PDR and RSSI passes the T-Test and PSR does not pass the test. Hence it is proved that the jamming influences the metrics PDR, RSSI. Next, the rationality of using PDR and RSSI is discussed and the reason behind choosing these metrics in cluster based WSNs is discussed. After that, PDR and RSSI are described. Then, T-Test is used to fix the PDR threshold. 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 specific type of jamming. The T-Test proves that there is significant difference between the two population means. Therefore by using the mean PDR of jammed member as reference value, the classification of jamming is performed (All the T-Tests have been performed by using samples obtained from our simulation).

3.4.1 Jamming and PDR

In order to justify whether the jamming influences PDR, the T-Test is carried out by considering some sample scenarios. We have performed simulations in section 5. Initially, the constant jamming is launched then two set of samples are considered with respect to without jamming and after launching of jamming in the network. The T-Test is performed on these samples to states that there is difference between the two population means (i.e., PDR is not affected during jamming free scenario and after launching of jamming) or not. Similarly the simulation is repeated for other types of jamming.

The T-Test tests the null hypothesis H_0: $\mu(x) = \mu(y)$ against the alternative hypothesis, H_1: $\mu(x) \neq \mu(y)$ where $\mu(x)$ and $\mu(y)$ are means of two populations. The null hypothesis states that there is no difference between the two population means (i.e., PDR is not affected during jamming free scenario and after launching of jamming).The alternate hypothesis states that there is difference between the two population means (i.e., PDR is not affected without jamming and PDR is affected after launching of jamming).

T-Test is performed on 40(20 for without jamming and 20 for after launching jamming) samples of PDR obtained from the CMs M1, M2, M3, M4 and M5. The degree of freedom (df) is calculated as 38 (n1+n2-2) and the level of significance (p) is 0.01 with the corresponding t value 62.5, 68.2, 72.4, 0.8 and 2.2 for 99 percent of confidence interval. The n1 represents total number of samples measured without jamming and n2 represents total number of samples measured during constant jamming. The result passes the T-Test. The t value of members M1, M2, M3, M4 and M5 is 62.5, 68.2, 72.4, 0.8 and 2.2 respectively. The t table value of T- Test is 2.75. From the observation, it is noted that the t value of the CMs M1, M2 and M3 exceeds the table value. This states that the PDR of M1, M2 and M3 are degraded due to jamming, whereas the members M4 and M5 are not affected by constant jamming. Thus T-Test result proves the significance of alternate hypothesis H_1 for constant jamming. The level of significance is 0.01. This states that the reliability of the result is 99 percent. That is, the obtained result is considered to be correct by 99 percent and the chance of obtained result to be wrong is 1 percent. Similarly the T-Test is performed for other types of jamming and the result proves the significance of alternate hypothesis.

3.4.2 The rationality of using PDR and RSSI

In order to explain the rationality of using PDR and RSSI for jamming detection in the proposed system, first the characteristics and the background of the existing jamming detection metrics such as PSR, PDR, BPR, ECA, BER, SNR, RSSI is explored. Then from the pros and cons of the existing metrics and from statistical proof, the suitable metric for jamming detection in cluster based downstream WSN is identified.

The jamming detection metrics used in the existing literature are PSR [10], PDR [10-11] [15-16], BPR [11] [13], ECA [11], BER [12], SNR [13] and RSSI [12] [15] (Section 3.3). Among these metrics, the proposed system uses the PDR and RSSI as the indicators for jamming detection. The rationality of using PDR and RSSI is described below,

- The PSR is measured by the source node and 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 [10]. The metric PSR is not suitable for cluster based WSN due to the following reasons, (i) PSR is affected by other network condition such as congestion [10], device failure [17]. So that, it is difficult to differentiate normal scenario with jamming scenario, (ii) PSR does not detect the reactive jamming [17] and does not distinguish between various types of jamming, and (iii) the value of PSR stays high (unchanged) even if the data packets are dropped at the destination node (because the destination node is jammed).
- The BPR is defined as the ratio of the number of bad packets received by a node to the total number of packets arrived at receiver node [11] [13]. The ECA is defined as the amount of energy consumed in a particular time for a wireless sensor network [11]. The BER is 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 [12]. The SNR is defined as the ratio of the received signal power in a node to the received noise power in a node [13]. BER is hard to compute by sensor nodes, since senor nodes need to collect huge amount of data regarding every bit of a valid and invalid packet. However, the metrics BPR, ECA and BER are estimated by sensor nodes (computed at destination node) and the metric SNR is computed by source node by collecting the information from destination and are not suitable for the proposed system (in proposed system the metrics are estimated at cluster head (source node)). The main idea of the proposed system is to detect the presence of jamming in downstream data communication in the cluster based WSNs.
- The metric RSSI is the ratio of received signal strength to the reference power [12][15]. The lower signal strength denotes the presence of jamming. But the signal strength becomes low due to dead node (energy consumption or node faults) or because of jamming. Upon using RSSI, it is also difficult to differentiate the normal scenario from reactive jamming [17]. Therefore RSSI alone can not be used to detect the presence of jamming. However, the RSSI can be combined with other metric to detect the presence of all types of jamming attacks at the physical layer and data link layer.
- The PDR is estimated by source node. The PDR is defined as the ratio of the total number of packets successfully (the packets for which acknowledgement received) sent by the node to the total number of packets sent by the node [10-11] [15-16] (section 3.4.4). It is identified that PDR is an excellent metric for jamming detection, since the cluster head can measure it by itself accurately without much computational overhead, PDR can identify the presence of all types of jamming attacks at the physical layer and data link layer, PDR is easily computable and PDR is suitable for cluster based WSN (section 3.4.3). The factors other than jamming such as collision, congestion, can also influence the data transmission and cause the PDR value to become low. Therefore, we

use PDR in conjunction with RSSI in order to detect the presence of all types of jamming (section 3.4.5).

From the above discussion, it is noticed that the metrics BPR, ECA and BER are estimated by destination node, the metric SNR is estimated at source node by collecting the information from destination and the metrics PSR, RSSI and PDR are estimated by source node. The main objective of this paper is to detect the presence of jamming in cluster based WSNs for downstream data communication. In down stream data communication, the cluster head acts as the source node for members. Therefore in the proposed system it is mandatory for the source node (cluster head) to compute the jamming detection metric to detect jamming attacks. In the proposed system, the source node (cluster head) estimates the jamming detection metrics to detect jamming attacks. Therefore the metrics BPR, ECA, BER and SNR are not suitable for the proposed system because these metrics are estimated at destination. The metrics PSR, RSSI and PDR can be used to detect the presence of jamming in the proposed system because these metrics are estimated at source. Among these three metrics (PSR, RSSI and PDR), it is necessary to find the most affected metric due to jamming. The idea is, if a metric is identified as most affected one due to jamming, then by using that metric jamming can be detected. That is, if PDR is affected by jamming then jamming can be determined by examining the PDR. Therefore it is important to determine which metric (PSR, RSSI and PDR) is mostly affected by jamming.

Roughly, it is not possible to judge whether the jamming influences the metrics PSR, RSSI and PDR or not. Therefore an appropriate experimental result is needed to find whether the jamming influences these metrics. To address this need, statistical test (T-Test) is performed in order to find the metric (PSR, RSSI and PDR) that is mostly affected by jamming. The T test is performed in order to examine the role of PSR, RSSI and PDR in jamming detection. The result of T-Test, to examine the role of PDR in jamming detection is discussed in section 3.4.1. The result passes the T-Test and proves the significance of alternate hypothesis H1 (i.e., PDR is not affected without jamming and PDR is affected after launching of jamming) for all types of jamming. The T-Tests, to examine the role of PSR in jamming detection and the T test to examine the role of RSSI in jamming detection is carried out but due to space constraints it is not included in the paper.

From the T-Tests, it is noticed that the metrics PDR and RSSI passes the T-Test and PSR does not pass the T-Test. Hence it is proved that the jamming influences the metrics PDR, RSSI. That is, the metrics PDR, RSSI is mostly affected due to jamming whereas the metric PSR is only lightly affected due to jamming (PSR does not pass the T test). The PDR is an excellent metric that can detect all types of jamming at the physical layer and data link layer. But the factors other than jamming such as congestion, collision, node failure can also influence the data transmission and cause the PDR value to become low [10]. Therefore, the metric PDR alone cannot be used to detect the presence of jamming. The metric RSSI alone cannot differentiate normal scenario from reactive jamming [17]. Therefore, the metric RSSI alone cannot be used to detect the presence of jamming. Though it is proved that, by examining the metrics PDR, RSSI the presence of jamming can be determined, due to the inherent drawback of these metrics, a single metric (either PDR alone or RSSI) alone cannot be used to determine the presence of jamming. Hence the idea is to use both the metrics PDR and RSSI for jamming detection. In this paper both the metrics (PDR and RSSI) is combinely used to detect the presence of all types of jamming even in the presence of other network conditions.

3.4.3 Jamming detection metrics in proposed system

We select PDR and RSSI as the jamming detection metrics for the proposed system. The reason behind choosing these metrics in cluster based WSNs are discussed as follows; i) The PDR is an excellent metric since the cluster head can measure it by itself accurately without much computational overhead, and PDR can identify the presence of all types of jamming attacks at the physical layer and data link layer, ii) The CH can easily measure the RSSI either by using formulae as per the chosen propagation model (in this paper, free space propagation model is chosen) or by the node's RF power meter, iii) In the proposed system (section 4), 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 CH itself without needing the help from the nodes. Therefore it can be claimed that the CM is not burdened (is not loaded heavily), and iv) In the proposed system, the metrics PDR and RSSI is used in detecting the presence of jamming and its types to an extend of 99 percent. The metrics PDR and RSSI is defined in the next section. The suitability of considering these metrics in WSN environment is illustrated in the section 3.4.2.

3.4.4 Definition of PDR and RSSI

In this section, we define the metrics that are used in this paper to detect the jamming attack. The proposed system uses two metrics namely PDR and RSSI. The PDR is estimated either by source node or destination node. The PDR is defined as the ratio of the total number of packets successfully (the packets for which acknowledgement received) sent by the node to the total number of packets sent by the node. The PDR is expressed as follows,

$$PDR = Pst / Pt \tag{1}$$

Where Pst is number of packets successfully transmitted by the source, Pt is total number of packets transmitted by the source. The RSSI is the ratio of received signal strength to the reference power. The received signal strength value can be converted into RSSI [41] as given below,

$$R\Pr = TPs \cdot Gt \cdot Gr\left[\frac{\beta}{4\pi d}\right] \tag{2}$$

$$RSSI = 10 \log \frac{R\Pr}{\Pr ef} \tag{3}$$

Where $R\Pr$ is Remaining Power at receiver, TPs is Transmitted Power at sender, Gt is Gain of the transmitter, Gr is Gain of the receiver, β is Wave length, d is Distance between sender and receiver and $\Pr ef$ is the reference power and it is experimentally equivalent to 1mW.

3.4.5 PDR and RSSI Threshold

PDR is used to infer the occurrence of jamming. Hence it is essential to find the relationship between the PDR and jamming. In general the well known fact is that jamming is inversely proportional to PDR. In order to determine the breaking point at which the jammer influences the reduction in PDR, the following analysis is carried out. The breaking point at which the jammer influences the PDR to reduce is fixed as the threshold value in the proposed system (in simulation) to detect the presence of jamming.

CH periodically monitors the PDR. If the observed PDR is lower than the PDR threshold then CH will declare that jamming is occurred. In order to fix the threshold, T-Test is performed with 4 samples of PDR observed from CMs M1, M2, M3, M4 and M5. The degree of freedom is computed as 3 and the level of significance (p) is 0.01 with the corresponding t value 5.9 for 99 percent of confidence interval. The result passes the T-Test. The t table value of T-Test 5.84. From the observation, it is noted that the t value (5.9) exceeds the table value (5.84). This proves that there is significance and the PDR threshold (PDR_Threshold) is fixed as 77 %. The factors other than jamming such as collision, congestion, can also influence the data transmission and cause the PDR value to become low. Therefore, we use PDR 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. It can be ascertained that the node is jammed, if observed PDR value is lower than its threshold and estimated RSSI value is higher than its threshold is encountered. The average RSSI (db) threshold (RSSI_Threshold) value is fixed as -69.6 for 5m [42].

3.4.6 Classification 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 M1, M2 and M3 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 3.4.1. 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 discussed in section 3.4.1. Similarly the experiment is repeated for other types of jamming. The RSSI is fixed as discussed above (section 3.4.5).

Table 1. Classification of jamming

Type of Jammer	Average PDR (%)	PDR Range (%)	RSSI (db)
Constant	9.46	0 – 10	-69.6
Deceptive	27.88	24.75 – 52.25	-69.6
Random	57.85	52.25 – 77	-69.6
Reactive	21.3	11 – 24.75	-69.6

4. Jamming Detection Mechanism

In this section, first, the modules (steps) in the jamming detection technique are discussed. Next the databank used in the detection of jamming is defined and finally Cluster updation step and Jamming Detection step of the jamming detection technique is described.

4.1 Jamming Detection Technique

The jamming detection technique (JDT) is proposed for WSNs. The JDT is implemented in all CH/BS. When a node sends a packet, the JDT determines whether the source node is a legitimate node or new node and observes the behavior of the members in a cluster periodically. JDT consists of two steps namely: 1. Cluster updation and 2. Jamming Detection.

Every CH has to maintain look up tables for verification and detection. The look up tables employed in JDT are cluster member and cluster head (CMCH) table, cluster member status

(CM_ Status) table, cluster member PDR (CM_PDR) table, cluster member maximum PDR (CM_MaxPDR) table and CM_Malicious table. These look up table are kept inside a data bank. The cluster updation step (first step) in JDT uses CMCH table. The main intention to maintain the CMCH table is to determine the type of the source node and to identify whether the source node is legitimate node or new node. In order to determine the behavior of members in the cluster, the Jamming Detection step (second step) in JDT maintains four tables such as CM_Status table, CM_PDR table, CM_MaxPDR table and CM_Malicious table. The description and use of each table is explained as follows,

1. The CMCH table contains two fields: Node ID and Node Type as shown in **Table 2.** The Node ID represents 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 CM_Status table contains two fields namely MID and Flag as shown in the **Table 3**. The MID field represents address of the members in the cluster and Flag represents the value either S or U, where S denotes successful delivery of a packet of the corresponding CM and U denotes unsuccessful (U is determined if there is no acknowledgement within the specified time interval) delivery of a packet. The JDT updates the flag entry with the value either S or U in this table.
3. The CM_PDR table consists of two fields such as MID and PDR as shown in **Table 4**. The MID field denotes address of the CM and the PDR field represents the PDR of each member in the cluster. The JDT computes this PDR value periodically (every 100msec) by observing the entries from **Table 3**.

Table 2. CMCH Table

Node ID	Node Type (Member, Head or BS)
1	M
2	M
3	M
--	---
21	H
22	H
--	---
50	B

Table 3. CM_StatusTable

MID	Flag (S or U)
1	U
2	U
3	U
4	S
5	S

Table 4. CM_PDR

MID	PDR
1	P1
2	P2
3	P3
4	P4
5	P5

Table 5. CM_MaxPDR

MID	MaxPDR
1	mp1
2	mp2
3	mp3
4	mp4
5	mp5

Table 6. CM_Malicious

E.No	MID	MLevel
1	1	H
2	2	H
3	3	H
4	4	L
5	5	N
6	1	H
-	-	-
-	-	-
15	5	N

4. The CM_MaxPDR table is formed by two fields such as MID and MaxPDR as shown in **Table 5**. The MID field represents address of the CM and MaxPDR represents the

maximum PDR of each member in the cluster. The JDT calculates this MaxPDR value periodically (every 1000msec) by observing the entries from **Table 4**.

5. The CM_Malicious table contains three fields such as E.No, MID and MLevel as shown in **Table 6**. The E.No field denotes the entry number in the table. The MID field represents address of the CM and MLevel denotes the malicious level of each member in the cluster. The JDT computes the value of MLevel periodically (every 3000msec) by observing the entries from **Table 5** and expresses the value as High (H), Normal (N) and Low (L). In order to do this, the following three rules are followed,
    1. If CM_MaxPDR**.**MaxPDR is less than PDR_Threshold and RSSI is greater than RSSI_Threshold, then its malicious level is assigned as H.
    2. If CM_MaxPDR**.**MaxPDR is equal to PDR_Threshold then its malicious level is assigned as N.
    3. If CM_MaxPDR**.**MaxPDR is greater than PDR_Threshold, then its malicious level is assigned as L.

Where CM_MaxPDR**.**MaxPDR represents the maximum value of PDR from the corresponding entries of each member in the cluster (every 1000msec).

If the CH receives a packet, then the cluster updation step in JDT has to determine whether the source node of the received packet is legitimate node (CM or BS) or new node. In order to determine this, the JDT refers CMCH table. If the address of the source node is found in the CMCH table, it indicates that the source node either exists in the cluster or exists in the network (BS or other CH).If the source node is not found in the CMCH table then JDT declares the source node as new node.

The Jamming Detection step determines the behavior of the members in a cluster. In order to determine the behavior of CMs, it observes the PDR of the CMs periodically (100msec). Next it measures the MaxPDR (every 1000msec) from the observed PDR values. If the MaxPDR is less than the PDR threshold then the CH measures the RSSI. The observed RSSI is compared against the RSSI threshold. If the observed RSSI is greater than the RSSI threshold then the behavior of the corresponding member is ascertained as unusual and the JDT declares that the corresponding member is jammed by the jammer.

4.1.1 Cluster Updation

Cluster updation Algorithm:

1. Sleep until a packet is received
2. If(received packet is destined to this CH)
    1. Extract the address of the source node
    2. Check the CMCH table to find an entry corresponding to source node address
    3. If (found)
        1. The source node is declared as existing CM in the cluster or BS
        2. Return
    4. Else
        1. Declare the source node as new node
        2. create an entry with source node’s identifier
        3. Add this entry into CMCH table
        4. Return
3. Else
    1. Discard the packet
    2. Return

Cluster updation step is responsible for making decision whether the source node is legitimate node or new node. For updation purpose, Cluster updation step refers the CMCH table as shown in **Table 2**. If address of the source node is found in **Table 2** then this step declares that the source node is existing CM in the cluster or BS. If this step determines that the source node is new node then the source node is added into **Table 2.** The cluster updation algorithm explains the working principle of the cluster updation step as given above.

4.1.2 Jamming Detection

Cluster updation step is responsible to declare whether the source node is legitimate node or new node in the cluster. The Jamming Detection step is responsible for monitoring the behaviour of existing nodes and newly joined node. This step determines whether the newly joined node or existing nodes are in normal condition or abnormal condition based on their behavior. In order to determine the behaviour of nodes, the PDR and RSSI is used.

Each CH computes PDR and maximum PDR of its each CM as shown in **Table 4** and **Table 5** respectively. The PDR is measured periodically (every 100msec) by referring the **Table 3** and the measured PDR is stored in the **Table 4.** The MaxPDR is estimated (every 1000msec) by observing the PDR entries from the **Table 4.** If the MaxPDR is greater than or equal to the PDR threshold then JDT ascertains the member's behavior as L or N and declares that the member is not jammed (normal). If the MaxPDR is less than the PDR threshold then JDT directly cannot justify that the corresponding CM is jammed. Because the PDR may be affected by other factors. Therefore PDR alone is not sufficient to determine the presence of jamming. In order to determine the presence of jamming accurately, it is important to consider an additional metric RSSI (RSSI threshold is fixed as discussed in the section 3.4.5). When the MaxPDR is less than the PDR threshold then JDT measures the RSSI of the corresponding CM. The measured RSSI is compared against the RSSI threshold. If the observed RSSI is greater than the RSSI threshold then JDT assigns the malicious level (MLevel) as H. If the Malicious level of the corresponding CM is determined as H for thrice then the corresponding CM is declared as jammed. The Jamming Detection Algorithm used in the Jamming Detection step to detect the presence of jamming is given as follows,

Jamming Detection Algorithm :

PDR Estimation (CM_PDR):

1. Sleep until the periodic timer matures (for every 100msec)
2. For each CM_i (i=1 to N, where N is the total number of members in a cluster)
    1. Fetch the records corresponding to MID_i from CM_Status table (**Table 3)**
    2. Compute the PDR of each CM_i from the fetched records
    3. Update the computed PDR in CM_PDR table (**Table 4**)
3. Return

Max_PDR Estimation (CM_MaxPDR):

1. Sleep until the periodic timer matures (for every 1000msec)
2. For each CM_i (i=1 to N)
    1. Fetch the records corresponding to MID_i from CM_PDR table (**Table 4)**
    2. Compute the MaxPDR of each CM_i from the fetched records
    3. Update the computed MaxPDR in CM_MaxPDR table (**Table 5**)
3. Return

CM_Malicious Level Estimation (CM_MLevel):

1. Sleep until the periodic timer matures (every 3000msec)
2. Set E = 1 (E denotes the records entry number in **Table 6**)
3. For j = 1 to 3

1. For every CM_i (i=1 to N)
    1. Fetch the record corresponding to MIDi from CM_MaxPDR table (**Table 5**)
    2. If (CM_MaxPDR**.**MaxPDR < PDR_Threshold)
        1. CH estimates the RSSI of corresponding CM
        2. If (RSSI > RSSI_Threshold)
            1. CM_Malilcious**.**MLevel = H

        (CM_Malicious**.**MLevel represents the malicious level of CM in **Table 6**)
    3. If (CM_MaxPDR**.**MaxPDR = = PDR_Threshold)
        1. CM_Malicious**.**MLevel = N
    4. If (CM_MaxPDR**.**MaxPDR > PDR_Threshold)
        1. CM_Malicious**.**MLevel = L
    5. Update the CM_Malicious**.**MLevel in the entry (E) of **Table 6**
    6. Increment : E = E + 1
2. End For
3. Sleep until periodic timer matures (for every 1000msec)

4. End For
5. Return

Detection:

1. Sleep until the periodic timer matures (every 3000msec to detect jammed node)
2. For every CM_i (i=1 to N)
    1. For every entry in the CM_Malicious Table (**Table 6)**
        1. Fetch the records corresponding to MIDi from CM_Malicious table
        2. If (CM_Malicious.MLevel is H)
            1. Declare CM_i is jammed
3. Return

In the jamming detection algorithm, the PDR Estimation, Max_PDR Estimation, CM_Malicious Level Estimation and Detection are run simultaneously. From the observation, it is noted that the CMs are not burdened for computation of metrics (PDR, RSSI), processing and decision making. Because the CH alone estimates the metrics and process and makes decision about ‘jammed situation’ or ‘non jammed situation’.

5. Experiments and Discussion

5.1 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. It is identified from the Fig. 1 that three members (M1, M2 and M3) are jammed. The two members (M4 and M5) and cluster head (CH21) are not affected by a jammer. 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 jammers are integrated to analyze the traffic in normal scenario and jamming scenario (section 5.2). The input parameters details are used for the simulation in respect of the sensor networks are shown in the **Table 7.**

Table 7. 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/sec	Variable
Transmission range	5m	5m
Propagation Model	Free Space	Free Space
Simulation Time	600 sec.	
MAC Protocol	None	
Jammer Type	Constant, Deceptive, Random and Reactive	

5.2 Discussions

The simulation is performed for 600 seconds as shown in the **Table 7**. Initially the simulation is done without jammer. Then the simulation is continued with various type of jammer. (Initially, the constant jammer is launched then set of samples are considered with respect to without jamming and after launching of jamming in the network. Similarly the simulation is repeated for other types of jamming). We have considered five set of 20 samples of PDR from the simulation to represent the normal scenario and jamming scenario with various types of jammers.

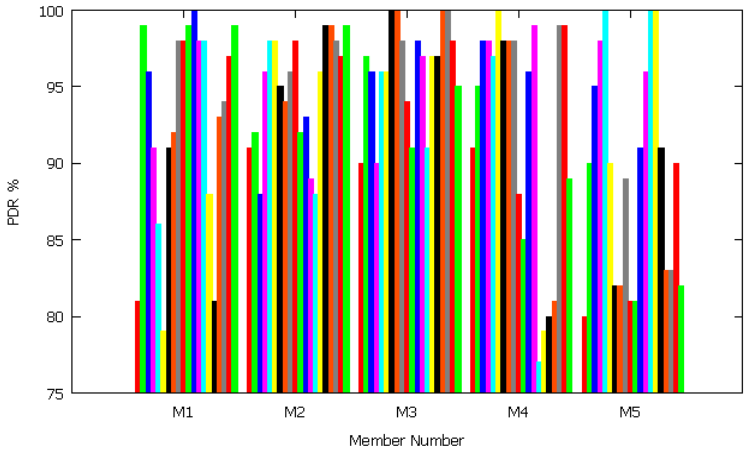

Fig. 2. Member wise traffic in Normal Scenario

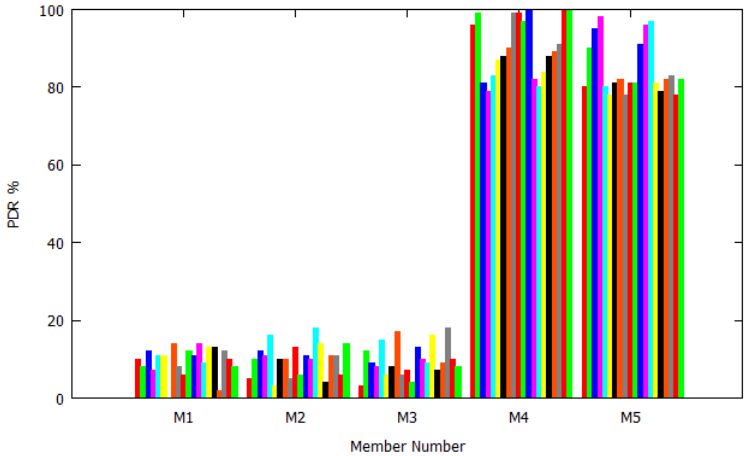

Fig. 3. Member wise traffic in presence of constant Jamming

The Fig. 2 represents the distribution of PDR of each member in normal scenario, in which PDR of all the members are above the PDR_threshold. The various histogram colors in the **Fig. 2** represent different samples of PDR. Next, constant jamming is launched in the network. **Fig. 3** shows the data transmission in a member wise manner, i.e. how many data packets are delivered to each member by CH. The X axis represents the member number and Y axis represents the achieved throughput in terms of PDR. It is observed from **Fig. 3** that the PDR of M1, M2 and M3 is lower than the PDR threshold due to constant jammer, whereas the PDR of M4 and M5 are above the PDR threshold. Theoretically, Constant jammer jams the entire communication on the channel since it continuously injects packets on the medium. But in practice, negligible communication takes place. The effect of jamming by a constant jammer is found to be more than 90%.

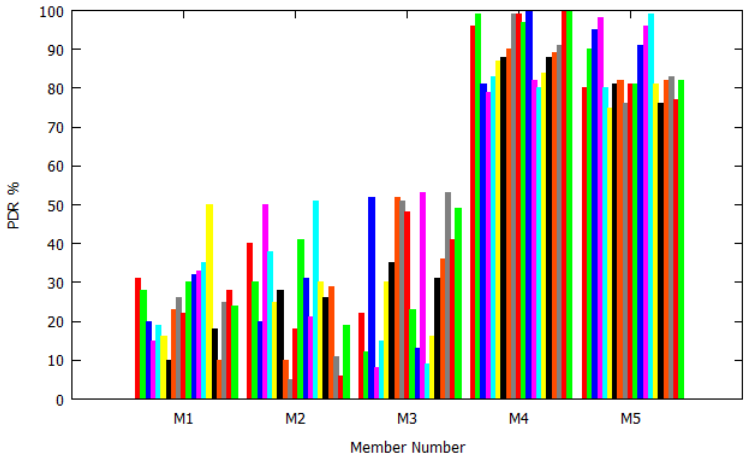

Fig. 4. Member wise traffic in presence of deceptive jamming

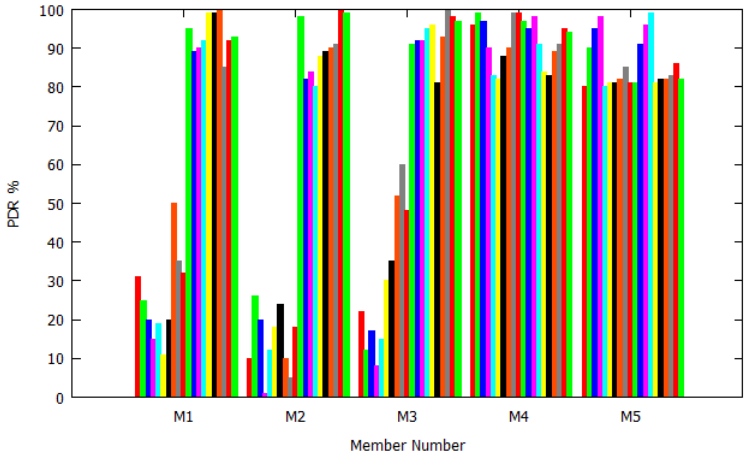

Fig. 5. Member wise traffic in presence of random jamming

In **Fig. 4**, Deceptive jammer jams the data transmission like constant jammer, but it is aware of the existing protocol in the network. The effect of deceptive jamming is found to be more than 81%. The random jammer randomly jams the data transmission on the medium as shown in **Fig. 5**. This type of jammer sleeps and jams for random amount of time. It is observed from the simulation that the average effect of random jamming is about 42%. Reactive jammer is also

aware of the communication protocol in the network. It continuously listens in the medium and begins to jam the medium when data transmission takes place. The average effect of this jamming is about 80% as shown in **Fig. 6**. The **Fig. 7** represents the average PDR with sampling duration of 200 sec for various jammers.

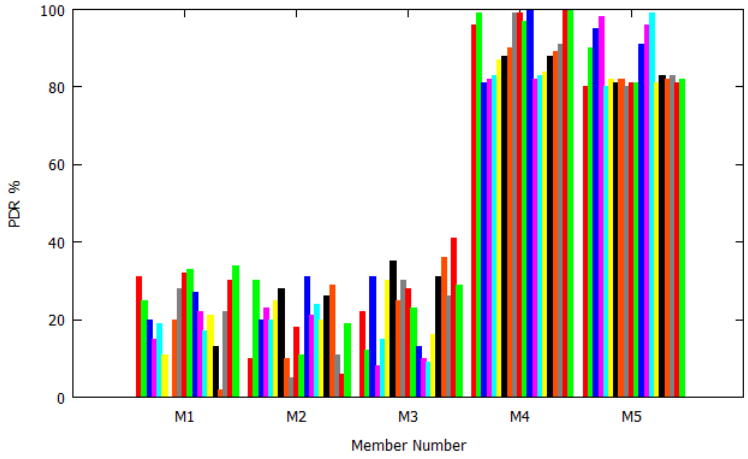

Fig. 6. Member wise traffic in presence of reactive jamming

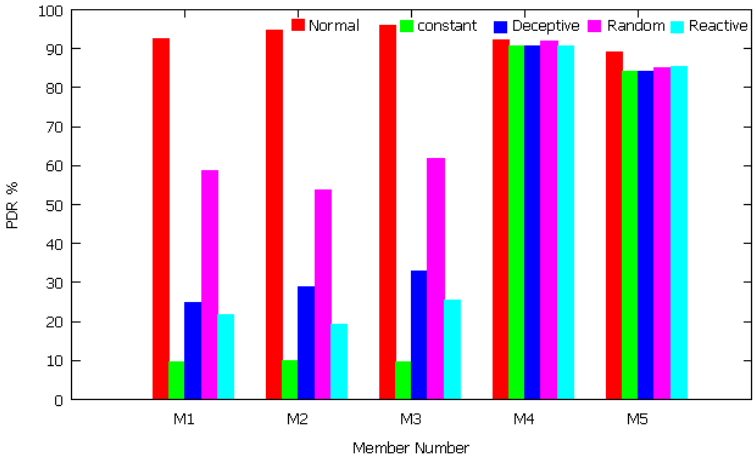

Fig. 7. Average PDR of various jamming

5.3 Performance Evaluation Metrics

In general, the CH detects the member as normal or abnormal. In some situation CH may not detects the abnormal node or CH may incorrectly detects the node as normal. The detection of nodes may be classified into i) True detection, ii) False detection, and iii) Undetection. The True detection means, CH detects a node as abnormal during that node is jammed. The False detection represents that CH faultily detects a node as abnormal though that node is normal. The Undetection, explains that CH incorrectly detects a node as normal, but the node is really jammed.

The metrics used for estimation of Detection Ratio, False alarm and Undetection ratio are given as follows: True Positive Index (TPI) represents number of correctly detected jammed nodes. True Negative Index (TNI) represents number of correctly detected normal nodes, but the nodes are really not jammed. False Positive Index (FPI) represents that the nodes are jammed but it is actually not jammed. False Negative Index (FNI) represents that the nodes are

not jammed but it is actually jammed. True Positive ratio (TPR) is the number of correctly detected jammed nodes to the total number of nodes actually jammed. True Negative ratio (TNR) is the number of correctly detected normal nodes (nodes that are not jammed) to the total number of normal nodes. False Positive ratio (FPR) is the number of nodes is incorrectly detected as jammed to the sum of nodes that are detected as jammed and number of nodes that are actually not jammed. False Negative ratio (FNR) is the number of nodes is incorrectly detected as normal to the sum of nodes that are detected as not jammed and number of nodes that are actually jammed.

In this paper, we have considered the performance metrics TPR as True detection ratio, FNR as False detection ratio and Undetection ratio. The terms which we have used in our performance evaluation is defined as follows,

True Detection Ratio (TDR) is defined as the ratio of the number of members that are correctly detected by the CH to the number of members that are exactly affected by the jammer. The TDR is estimated as follows,

$$TDR = TPI / \left(TPI + FNI \right) \tag{4}$$

False Detection ratio (FDR) is defined as the ratio of the number of members that are incorrectly detected by the CH to the number of members that are not actually affected by the jammer. That is, a member is in normal condition but it has been wrongly detected as abnormal. The FDR is estimated as follows,

$$FDR = FPI / \left(FPI + TNI \right) \tag{5}$$

Undetection ratio (UDR) is defined as the ratio of the number of members are not detected by the CH to the number of members are actually affected by the jammer. The UDR is estimated as follows,

$$UDR = FNI / \left(TPI + FNI \right) \tag{6}$$

The jammed member ratio (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 estimated as follows,

$$Jmr = nsj / nfj \tag{7}$$

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

It is essential to have a mechanism for measuring the performance difference between observed and anticipated values. In order to achieve this we use the chi square test to decide whether the effects are present or not. The Chi square test is performed after simulations (A cluster of six members (M1, M2, M3, M4, M5 and CH21) are considered as shown in the **Fig. 1**. The simulation setup for this scenario is made in such a way that 3 members (M1, M2 and M3) are affected by a jammer and two members (M4 and M5) 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 0.05 with the corresponding table value 5.991 for 95 percent of confidence interval.

Table 8. Chi Square test result for one of the simulations

Group of Malicious level	Members in the cluster (O)	Members by anticipation (A)	$(O-A)^2/A$	J	F	U	TDR = 100.J/A (%)	FDR = 100.F/A (%)	UDR = 100.U/A (%)
Normal	1	1	0	1	0	0	100	0	0
Low	1	1	0	1	0	0	100	0	0
High	3	3	0	3	0	0	100	0	0
Total	5	5	0	5	0	0	100	0	0

The results are shown in **Table 8**(result of single simulation is considered).The result passes the chi-square test as the total under $(O-A)^2/A$ is 0, which is less than the chi square table value (5.991). Hence there is no difference between observed (O)and anticipated (A) values. The level of significance is 0.05. This states that the reliability of the result is 95 percent. That is, the obtained result is considered to be correct by 95 percent and the chance of obtained result to be wrong is 5 percent. Therefore the result of the proposed system is extremely encouraging. In **Table 8**, J denotes Members correctly detected by JDT while node is jammed, F denotes Members incorrectly detected as abnormal by JDT while node is in normal and U denotes Members incorrectly detected as normal by JDT while node is in abnormal.

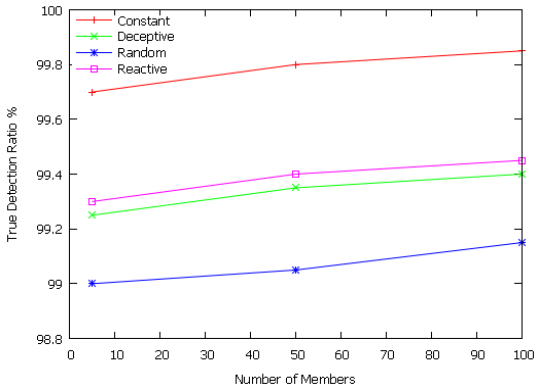

Fig. 8. TDR for different jamming of various Configurations

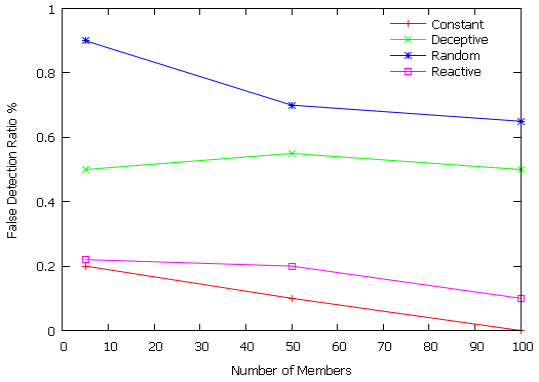

Fig. 9. FDR for different jamming of various Configurations

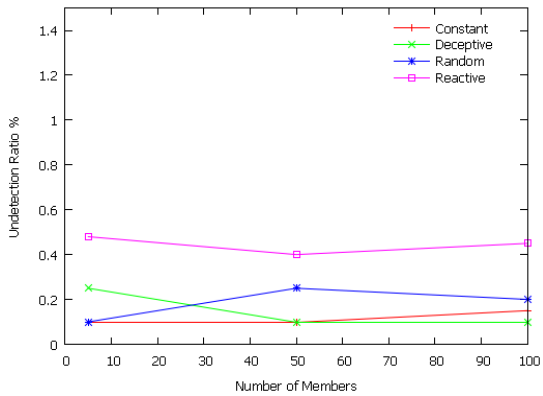

Fig. 10. UDR for different jamming of various configurations

As discussed before, the PDR threshold is fixed as 77 % from the result of T-Test with the probability of 0.99. Then various types of jamming have been launched. The TDR, FDR and UDR are determined based on the PDR threshold (77%). The mean TDR, FDR and UDR from these simulations are collected for different jammed members under various configurations (total number of members in a cluster in the simulation, n) for different types of jammers.

Table 9. TDR, FDR and UDR for 100 nodes configuration for various type of jammer and jmr

Jammer type	TDR for 100 nodes configuration			FDR for 100 nodes configuration			UDR for 100 nodes configuration		
	Jmr 25%	Jmr 50%	Jmr 100%	Jmr 25%	Jmr 50%	Jmr 100%	Jmr 25%	Jmr 50%	Jmr 100%
Constant	99.4	99.55	99.85	0.35	0.25	0	0.2	0.1	0
Deceptive	99.3	99.35	99.4	0.2	0.3	0	0.35	0.2	0
Random	99.15	99.45	99.7	0.5	0.2	0	0.3	0.15	0
Reactive	99.45	99.5	99.75	0.2	0.1	0	0.15	0.05	0

The **Fig. 8, Fig. 9, and Fig. 10** show the values of TDR, FDR and UDR for various member configuration (5, 50 and 100) for different types of jammers with probability p=0.01. The values of TDR, FDR and UDR for 100 nodes configuration for various type of jammer for various percent of jammed member ratio (25%, 50% and 100%) are shown in the **Table 9**.

Now we compare our performance evaluation metrics TDR, FDR and UDR with the existing system [13]. From the **Table 10**, it is noted that the proposed system works well in the probability 0.99. This states that the reliability of the result is 99 percent. That is, the obtained result is considered to be correct by 99 percent and the chance of obtained result to be wrong is 1 percent. It is concluded that the proposed system provides TDR as high as 99.85 percent and negligible FDR and UDR. The CH centric approach (centralized approach) is more accurate than the node centric (decentralized approach). Because the existing works involve in collection of respective node's metric (local condition) and neighbor nodes' metric (neighbor's condition) to make the decision whether the node is jammed or not. But in the proposed work, the CH alone estimates the metrics (PDR, RSSI) and makes decision about 'jammed situation' or 'non jammed situation' (CM is not burdened, since CM does not involves to collect metrics and to make the decision whether the node is jammed or not).

Table 10. TDR, FDR and UDR for 100 nodes configuration for various type of jammer and jmr

Jammer type	TDR, FDR and UDR for 100 nodes configuration														
	jmr 25%					jmr 50%					jmr 100%				
	Proposed			Existing *		Proposed			Existing *		Proposed			Existing *	
	TDR	FDR	UDR	TDR	FDR	TDR	FDR	UDR	TDR	FDR	TDR	FDR	UDR	TDR	FDR
Constant	99.4	0.35	0.2	99.15	0.01	99.55	0.25	0.1	99.45	0.01	99.85	0	0	99.5	0
Deceptive	99.3	0.2	0.35	99.35	0.02	99.35	0.3	0.2	99.4	0.01	99.4	0	0	99.5	0
Random	99.15	0.5	0.3	98.9	0.6	99.45	0.2	0.15	99	0.3	99.7	0	0	99.1	0
Reactive	99.45	0.2	0.15	99	0.02	99.5	0.1	0.05	99.1	0.02	99.75	0	0	99.25	0

* The UDR in the existing approach was not defined clearly

6. Conclusion

A novel jamming detection technique is proposed to detect the presence of jamming during downstream data communication in cluster based wireless sensor network. The proposed jamming detection technique uses the following three key elements to perform better than the existing jamming detection approaches. (i) The metric PDR is combined with the metric RSSI for jamming detection; (ii) Statistical tests are deployed to determine the detection metrics threshold and types of jamming (iii) A two step technique namely cluster updation and jamming detection is employed. The proposed jamming detection technique is simulated using MATLAB 7 and NS2 simulator. The simulation is done to determine the true detection ratio, false detection ratio and undetection ratio. The proposed system performs appreciably better (achieves higher true detection ratio (99.85) and negligible false detection ratio and undetection ratio) than the existing system. The idea behind this novel jamming detection technique can be applied in sensor networks to detect the presence of jammer. The future work directions include extending the coverage limit of nodes in the proposed JDT (every sensor node's coverage limit is considered as 5 meter) and to find the impact of the coverage limit on the performance metrics.Yet another possibility of future work is, dynamic election of CH in the sensor network. In order to elect the CH dynamically, it is planned to design a new cluster head selection algorithm that suits well for the proposed JDT. In future, it is also proposed to examine the performance of the JDT by deploying various existing trust based cluster head selection algorithm [38-40].

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002. Article (CrossRef Link)

[2] Xuxun Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks," *Sensors*, vol.12, no.8, pp. 11113-11153, 2012. Article (CrossRef Link)

[3] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," *International Journal of Distributed Sensor Networks*, vol.2013. pp. 1-7, 2013. Article (CrossRef Link)

[4] T. P. Rani, C.Jayakumar, "Survey on Key Pre Distribution for Security in Wireless Sensor Networks," *Advances in Computer Science and Information Technology, Networks and Communications*, vol. 84, 2012, pp: 248-252. Article (CrossRef Link)

[5] E.Shi and A.Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol.11, no. 6, pp.38-43, 2004. Article (CrossRef Link)

[6] Minho Jo, Longzhe Han, Nguyen Duy Tan and Hoh Peter In, "A Survey: Energy Exhausting Attacks in MAC Protocols in WBANs," *Telecommunication Systems*, vol. 58, no. 2, pp. 153-164, Feb 2015. Article (CrossRef Link)

[7] Md. Mokammel Haque, Al-Sakib Khan Pathan, Choong Seon Hong and Eui-Nam Huh, "An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks," *KSII Transactions on Internet an Information Systems*, vol. 2, no. 5, October 2008. Article (CrossRef Link)

[8] Taeshik Shon and Yongsuk Park, "A Hybrid Adaptive Security Framework for IEEE 802.15.4-based Wireless Sensor Networks," *KSII Transactions on Internet an Information Systems*, vol. 3, no. 6, December 2009. Article (CrossRef Link)

[9] Sunghyuck Hong, Sunho Lim and Jaeki Song, "Unified Modeling Language based Analysis of Security Attacks in Wireless Sensor Networks: A Survey," *KSII Transactions on Internet an Information Systems*, vol. 5, no. 4, April 2011. Article (CrossRef Link)

[10] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. of the Sixth ACM International Symposium on Mobile ad hoc Networking and Computing*,, pp. 46-57, November 2005.

Article (CrossRef Link)
[11] M. Cakiroglu and A. T. Ozcerit, "Jamming detection mechanisms for wireless sensor networks," in *Proc. of the 3rd International Conference on Scalable Information Systems*, pp. 4-6, June 2008. Article (CrossRef Link)
[12] S. Mario, D. Boris and C. Srdjan, C, "Detection of reactive jamming in sensor networks," *ACM Transactions on Sensor Networks*, vol. 7, no. 2, 2010. Article (CrossRef Link)
[13] Sudip Misra, Ranjit Singh and S. V. Rohith Mohan, "Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System," *sensors*, pp. 3444-3479, 2010. Article (CrossRef Link)
[14] J. Thangapoo Nancy, K. P. Vijayakumar and P. Ganeshkumar, "Detection of jammer in Wireless Sensor Network," in *Proc. of IEEE International Conference on Communications and Signal Processing (ICCSP)*, pp: 1435 – 1439, 2014. Article (CrossRef Link)
[15] V. C. Manju and M. S. Kumar, "Detection of jamming style DoS attack in Wireless Sensor Network," in *Proc. of 2nd IEEE International conference on Parallel Distributed and Grid Computing (PDGC)*, pp: 563-567, 2012. Article (CrossRef Link)
[16] K. Siddhabathula, Qi Dong, Donggang Liu and M. Wright "Fast jamming detection in sensor networks," in *Proc. of IEEE International Conference on Communications*, pp: 934 – 938, 2012. Article (CrossRef Link)
[17] Wenyuan Xu, Wade Trappe and Yanyong Zhang, "Jamming Sensor Networks: Attack and Defense Strategies," *IEEE Network*, vol. 20, no.3, pp. 41-47, 2006. Article (CrossRef Link)
[18] A. Mpitziopoulos, Damianos Gavels, Charalampos Konstantopoulos and Grammati Pantziou, "A Survey on Jamming Attacks and Countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no.4, pp.42-56, 2009. Article (CrossRef Link)
[19] Svetlana Radosavac and John S. Baras, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," in *Proc. of ACM WiSe '05*, pp.33-42, 2005. Article (CrossRef Link)
[20] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 1-15, Jan. 2007. Article (CrossRef Link)
[21] Mingyan Li, Iordanis Koutsopoulos and Radha Pooverndran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp.1119-1133, August 2010. Article (CrossRef Link)
[22] Jerry T. Chiang and Yih-Chun Hu, "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks," *IEEE/ACM Transactions on Networking*, vol.19, no.1, February 2011. Article (CrossRef Link)
[23] Yanmin Zhu and Yuan Jiang, "On Optimal Antijamming Strategies in Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 793194, pp.1-9, 2012. Article (CrossRef Link)
[24] T. H. Hai, Eui-Nam Huh and Minho Jo, "A lightweight intrusion detection framework for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 10, no. 4, pp. 559-572, 2010. Article (CrossRef Link)
[25] C. Del-Valle-Soto, C. Mex-Perera, Raul Monroy and Juan Arturo Nolazco-Flores, "On the Routing Protocol Influence on the Resilience of Wireless Sensor Networks to Jamming Attacks," *Sensors*, vol. 15, no. 4, pp. 7619-7649; 2015. Article (CrossRef Link)
[26] EduardGarcia-Villegas, M. S. Afaqui and Elena Lopez-Aguilera, "A novel cheater and jammer detection scheme for IEEE802.11-based wireless LANs," *Computer Networks*, vol. 86, pp.40-46, 2015. Article (CrossRef Link)
[27] Minho Jo, Longzhe Han, Dohoon Kim and Hoh Peter In, "Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks," *IEEE Network*, Vol. 27. No. 3, pp. 46-50, 2013. Article (CrossRef Link)
[28] Seung-Jong Park, Ramanuja Vedantham, Raghupathy Sivakumar and Ian F. Akyildiz, "GARUDA: Achieving Effective Reliability for Downstream Communication in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 2,pp. 214-230, February 2008. Article (CrossRef Link)

[29] Fei Hu, Meng Jiang, Laura Celentano and Yang Xiao, "Robust medical ad hoc sensor networks (MASN) with wavelet-based ECG data mining," *Ad Hoc Networks*, vol. 6, no. 7, pp. 986–1012, 2008. Article (CrossRef Link)
[30] Emeka E. Egbogah and Abraham O. Fapojuwo, "A Survey of System Architecture Requirements for Health Care-Based Wireless Sensor Networks", *Sensors*, vol. 11, pp. 4875-4898. 2011. Article (CrossRef Link)
[31] A. Rajshekhar Chalak, S. Misra and M. C. Obaidat, "A cluster-head selection algorithm for Wireless Sensor Networks," *17th IEEE International Conference on Electronics, Circuits, and Systems* ICECS, pp. 130-133, 2010. Article (CrossRef Link)
[32] Shangfeng Mo, Hong Chen and Li Yinglong, "Clustering-based routing for top-k querying in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking* 2011, 2011:73. Article (CrossRef Link)
[33] Sangwook Kang, Sangbin Lee, Saeyoung Ahn and Sunshin An, "Energy Efficient Topology Control based on Sociological Cluster in Wireless Sensor Networks," *KSII Transactions on Internet and Information Systems*, vol.6, no. 1, Jan 2012. Article (CrossRef Link)
[34] Xuxun Liu and Jinglun Shi, "Clustering Routing Algorithms In Wireless Sensor Networks: An Overview," *KSII Transactions On Internet and Information Systems*, vol. 6, no. 7, July 2012. Article (CrossRef Link)
[35] Puneet Azad and Vidushi Sharma, "Cluster Head Selection in Wireless Sensor Networks under Fuzzy Environment," *ISRN Sensor Networks*, vol. 2013, Article ID 909086, 8 pages, 2013. Article (CrossRef Link)
[36] Khalid Hussain, Abdul Hanan Abdullah, Saleem Iqbal, Khalid M. Awan and Faraz Ahsan, "Efficient Cluster Head Selection Algorithm for MANET," *Journal of Computer Networks and Communications*, vol. 2013, Article ID 723913, 7 pages, 2013. Article (CrossRef Link)
[37] Jong-Shin Chen, Zeng-Wei Hong, Neng-Chung Wang and San-Heui Jhuang, "Efficient Cluster Head Selection Methods for Wireless Sensor Networks," Journal of Networks, vol. 5, no. 8, pp.964-970, August 2010. Article (CrossRef Link)
[38] G. V. Crosby, N. Pissinou and J. Gadze, "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks," in *Proc. of 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Columbia, pp.13-22, 2006. Article (CrossRef Link)
[39] R. Ferdous, V. Muthukkumarasamy and E. Sithirasenan, "Trust-Based Cluster Head Selection Algorithm for Mobile Ad Hoc Networks," *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Changsha, pp: 589-596, 2011. Article (CrossRef Link)
[40] B. Paramasivan and M. Kaliappan, "Secure and Fair Cluster Head Selection Protocol for Enhancing Security in Mobile Ad Hoc Networks," *The Scientific World Journal*, vol. 2014 , Article ID 608984, 6 pages, 2014. Article (CrossRef Link)
[41] Bojan Mrazovac, Milan Z. Bjelica, Dragan Kukolj, Branislav M. Todorovic, and Dragan Samardzija, B. Mrazovac et al., "A Human Detection Method for Residential Smart Energy Systems Based on Zigbee RSSI Changes," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 3, pp.819-824, August 2012. Article (CrossRef Link)
[42] K. Benkic, M. Malajner, P. Planinsic and Z. Cucej, "Using RSSI value for distance estimation in Wireless sensor networks based on ZigBee," in *Proc. of 15th International Conference on Systems, Signals and Image Processing*, IWSSIP 2008, pp. 303-306, 2008. Article (CrossRef Link)

K.P.Vijayakumar received the degree of Bachelor of Engineering in Information Technology from Madurai Kamaraj University (India) in 2003, ME degree in Computer Science and Engineering from Anna University Chennai (India) in 2007, and doing PhD degree in Information and Communication Engineering at Anna University, Chennai. He is as an Associate Professor in the Department of Information Technology at PSNA College of Engineering and Technology, India. His research interests are in the area of Computer networks, Network Security, Wireless sensor network and Vehicular Ad hoc Networks.

P. Ganeshkumar is a Professor in the Department of Information Technology at PSNA College of Engineering and Technology, India. He received BE degree in Electrical and Electronic Engineering from Madurai Kamaraj University , India in 2001, ME degree in Computer Science and Engineering from the Bharathiyar University (India), and PhD degree in Information and Communication Engineering at Anna University, Chennai. He has received fund from AICTE for carrying out research project under RPS sceme. He is reviewer in many reputed journals and also acted as chair in many conferences. His research interests are in the area of AdHoc Network, Wireless Networks, Distributed Systems,Performance analysis and Cloud computing.

M.Anandaraj received BE degree in Computer Science and Engineering from Madurai Kamaraj University (India) in 2003, ME degree in Computer and Communication from Anna University Chennai (India) in 2007, and doing PhD degree in Information and Communication Engineering at Anna University, Chennai. He is an Associate Professor in the Department of Information Technology at PSNA College of Engineering and Technology, India. His research interests include computer networks, multicast algorithm design and network coding.