



# An adaptive neuro-fuzzy logic based jamming detection system in WSN

K. P. Vijayakumar<sup>1</sup> · K. Pradeep Mohan Kumar<sup>1</sup> · K. Kottilingam<sup>1</sup> · T. Karthick<sup>1</sup> · P. Vijayakumar<sup>1</sup> · P. Ganeshkumar<sup>2</sup>

© Springer-Verlag GmbH Germany, part of Springer Nature 2018

## Abstract

Wireless sensor network (WSN) is employed in variety of applications ranging from agriculture to military. WSN is vulnerable to various security attacks, in which jamming attacks obstruct and disturb the exchange of information between sensor nodes in WSN by transmitting signals to jam legitimate transmission to cause a denial of service. Hence, it is essential to secure the sensor networks from jamming attacks. In this paper, two approaches: fuzzy inference system (FIS) and adaptive neuro-fuzzy inference system (ANFIS)-based jamming detection system are proposed for detecting the presence of jamming by computing two jamming detection metrics, namely, packet delivery ratio and received signal strength indicator. FIS approach is based on Takagi–Sugeno fuzzy logic which optimizes the jamming detection metrics. ANFIS approach combines fuzzy logic and learning ability of the neural network to optimize the metrics for detecting various types of jamming. The proposed approaches are compared with existing system and themselves. The simulation result shows that the proposed ANFIS approach detects the jamming attacks as high as true detection ratio.

**Keywords** Adaptive neuro-fuzzy inference system · Fuzzy logic · Jamming · Wireless sensor networks · Cluster

## 1 Introduction

Sensor nodes consist of sensing, computing, communicating components, and memory. These nodes are deployed in a region called sensor field to sense the environment. The

sensor networks are comprised of several tiny sensor nodes. The wireless sensor networks (WSNs) are becoming increasingly attractive for numerous application areas ranging from military to healthcare (Akyildiz et al. 2002; Liu 2012; Alrajeh et al. 2013). Sensor nodes have very limited memory space, energy, and computational power (Rani and Jayakumar 2012). These nodes work in an infrastructureless and dynamically changing environment (Shi and Perrig 2004) and route the collected data to the sink node for further interpretation. Sensor nodes are self-organized.

The sensor networks can be modelled either by using flat network or by cluster-based network. The issues associated with the flat network are increased collision, increased communication overhead, decreased throughput, and energy consumption. Clustering results in a two-layered hierarchy in which cluster heads (CHs) form the higher layer, whereas cluster members form lower layer. In cluster-based wireless sensor network (CWSN), nodes are partitioned into clusters. 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

Communicated by P. Pandian.

✉ K. P. Vijayakumar  
kalkivijay@rediffmail.com  
K. Pradeep Mohan Kumar  
kpradeep.kumar15@gmail.com  
K. Kottilingam  
kottilingam.k@ktr.srmuniv.ac.in  
T. Karthick  
karthick.course@gmail.com  
P. Vijayakumar  
vijaymean2win@gmail.com  
P. Ganeshkumar  
drpganeshkumar@gmail.com

<sup>1</sup> SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India

<sup>2</sup> PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India

reclustering, decreases collision, reduces the communication overhead, and improves throughput and network lifetime (Liu 2012; Abbasi and Younis 2007; Boyinbode et al. 2010; Kuila and Jana 2012; Liu and Shi 2012; Wang and Wong 2013; Sikander et al. 2013; Kumar 2014; Singh and Sharma 2015; Yadav et al. 2015).

The sensor networks are vulnerable to jamming attacks at physical layer and data link layers (Jo et al. 2015) because the sensor nodes use wireless medium for data communication (Mokammel Haque et al. 2008); the sensor nodes operate at very low radio power (Shon and Park 2009) and limited communication range between source and sink. 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 (Hong et al. 2011). Therefore, a mechanism is needed to detect various types of jamming attacks. However, to the best of our knowledge none of the existing literature had applied the adaptive neuro-fuzzy inference system (ANFIS) for detecting the presence of jamming in CWSN.

The motivations of this paper are as follows: (1) the jamming detection approach is employed for downstream data communication in which cluster head computes the jamming detection metrics to identify the jamming attack unlike existing system (in the existing systems Xu et al. 2005; Cakiroglu and Ozcerit 2008; Mario et al. 2010, individual sensor nodes compute the jamming detection metrics which lead to computational overhead). (2) Fuzzy logic-based approach optimizes the metrics for detecting jamming attacks unlike existing system. That is, in the existing system, the detection of jamming attack is determined by comparing the estimated metrics and jamming detection metric's threshold. Consider the scenario: when the measured jamming detection metric is compared against the threshold value, then it is determined that the measured metrics value is very close to threshold value. In this scenario, the existing system falsely determines that the node is jammed, but the node is actually not jammed or it determines that the node is not jammed, but the node is actually jammed. Therefore, the fuzzy logic approach is employed in WSN to optimize the jamming detection metrics for detecting the presence of jamming accurately. (3) Adaptive neuro-fuzzy inference system combines the fuzzy logic and learning ability of the neural network to optimize the metrics for identifying the jamming attack.

ANFIS is a class of adaptive networks that integrates both neural networks and fuzzy logic (Mathur et al. 2016). Neural network is supervised learning algorithms which employs past dataset for the prediction of future values. In fuzzy logic, the control signal is generated from firing the rule base. This

rule base is formed based on past data and is random in nature. This implies that the controller's output is also random which may prevent optimal results. The ANFIS can select the rule base more adaptive to the situation. In this technique, the rule base is selected by employing the neural network techniques via the back propagation algorithm. To enhance its applicability and performance, the properties of fuzzy logic, that is, approximating a nonlinear system by setting IF–THEN rules, are inherited in this modelling technique. This integrated approach makes ANFIS to be a universal estimator.

The main idea of this paper is to develop and apply fuzzy inference system (FIS) and adaptive neuro-fuzzy inference system (ANFIS) model for detecting the presence of jamming in CWSN. These two approaches use the jamming detection metrics such as packet delivery ratio (PDR) and received signal strength indicator (RSSI). The PDR and RSSI of every sensor node in the cluster are computed and evaluated by the cluster head (CH), and the CH identifies whether the sensor node in the respective cluster is jammed or not. FIS approach is based on Takagi–Sugeno fuzzy logic which optimizes the jamming detection metrics to identify various jamming. ANFIS approach combines fuzzy logic and learning ability of the neural network to optimize the metrics for detecting various types of jamming. The performance of the proposed systems FIS and ANFIS to identify the presence of jamming is assessed in terms of true detection ratio (TDR) and false detection ratio (FDR). In this paper, henceforth the proposed FIS-based jamming detection system and ANFIS-based jamming detection system are named as FIS-JDS and ANFIS-JDS, respectively.

The contributions of this paper are described as follows: (1) FIS-JDS (Sect. 4.1): initially, it determines the activities of newly entered node and existing node by computing the jamming detection metrics PDR and RSSI. Subsequently, it applies the Takagi–Sugeno fuzzy logic for optimizing the computed PDR and RSSI values for detecting various types of jamming. (2) ANFIS-JDS (Sect. 4.2): it combines fuzzy logic and learning ability of the neural network to optimize the computed PDR and RSSI metrics for detecting various types of jamming. (3) Statistical test (Sect. 5): first, the one-way analysis of variance (ANOVA) is used to determine whether there are any significant differences between the means of proposed system and existing systems. Next, Root Mean Square Error (RMSE), RMSE percentage (RP), and the precision are computed to compare the proposed approaches themselves.

The rest of the paper is organized as follows: related work is discussed in Sect. 2. Section 3 describes the system model. The proposed FIS-JDS and ANFIS-JDS are explained in Sect. 4. Result and discussions are presented in Sect. 5. Section 6 concludes this paper.

## 2 Related work

In this section, existing jamming detection approaches proposed for flat WSN and CWSN jamming detection techniques which applied fuzzy logic are discussed. Next, the issues associated with these approaches and the need of ANFIS are discussed.

In Xu et al. (2005), signal strength consistency check and location consistency check algorithms are proposed. First algorithm uses the corresponding node's PDR and signal strength in order to determine the presence of jamming. Second algorithm uses the corresponding node's PDR and the location of its neighbour. Based on the PDR of the corresponding and neighbour node's PDR, a decision can be taken about whether the node is jammed or not. Two jamming detection algorithms were proposed for detecting jamming attack in the network (Cakiroglu and Ozcerit 2008). The first algorithm uses three jamming detection metrics such as BPR, PDR, and ECA to detect the presence of jamming. The second algorithm is devised to enhance the former one. This algorithm collects the neighbour node's condition for making decision.

A novel jamming detection approach is proposed to detect the presence of reactive jamming attack (Mario et al. 2010). This approach used both BER and RSS to detect the individual packet bit errors. Each node in the network has to compute and update the BER of all communication links with its one-hop neighbours. The authors Manju and Kumar (2012) proposed a method for detecting physical layer denial of service (DoS) jamming attack. This method selects only some nodes available in the network as monitor nodes using residual energy. The monitor nodes verify the RSSI and the PDR of other nodes for detecting the presence of jamming. The jamming detection mechanism uses two metrics such as SNR and BPR (Misra et al. 2010). The detection of jamming in this approach is BS centric, where collecting data, processing it, and decision-making are carried out by BS to make decision about whether the node is jammed or not.

The authors proposed a method for detecting the presence of jamming attack in a faster manner (Siddhabathula et al. 2012). This method can detect only constant jammers, but cannot detect various types of jamming attacks. The proposed Jamming Detection Technique (JDT) (Vijayakumar et al. 2015) is to detect the presence of jamming in WSNs by using two jamming detection metrics, namely, PDR and RSSI. This technique uses PDR and RSSI threshold values for detecting the presence of jamming. A novel jammer detection framework for CWSN (Ganeshkumar et al. 2016) is proposed to detect the presence of jamming and jammer intrusion in a CWSN is proposed. In these methods, the presence or absence of jamming is identified by comparing the threshold value. If the measured metric's value is equal or

above the threshold, then it is declared as no jamming, else it is declared as jamming. The issue in these methods is even if the measured metric's value is very close to the threshold, then it is declared as presence of jamming (but actually not jammed).

In Misra et al. (2010), the jamming detection mechanism is based on fuzzy logic system that 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 performed by BS to make the decision whether the node is jammed or not. In Vijayakumar et al. (2018), proposed fuzzy logic-based jamming detection approach optimizes the jamming detection metrics such as packet delivery ratio and received signal strength indicator for detecting the presence of jamming in CWSN.

From the study of above literatures, the issues associated with the jamming detection approaches developed for flat WSN, CWSN, and fuzzy logic are discussed as follows: the limitations of existing approaches implemented in flat WSN are: (1) individual node is burdened since data collecting, processing, and decision-making are performed by individual nodes to make a decision about 'jammed situation' or 'non jammed situation', (2) increased time and space complexity and (3) presence of jamming is not detected precisely if the node has no neighbour, (4) communication overhead since BS periodically collects the data from nodes for decision-making. The limitation of existing approaches implemented in CWSN is the event of jamming which is determined by only using jamming detection metrics thresholds. The FIS formulates the IF-Then rules to optimize the range of jamming detection metrics by deploying membership functions. The fuzzy logic transforms the decision-making being crisp centric to fuzzy centric. However, the FIS does not have the learning ability. The benefit of using an ANFIS over the FIS is: ANFIS combines the advantages of fuzzy logic and learning ability of the neural network (NN) to devise a mechanism that solves the problem (Mathur et al. 2016), and it provides enhanced results as compared to their individual results (Devi et al. 2017). Hence, the main idea is to develop and apply the adaptive neuro-fuzzy inference system for detecting the presence of jamming in CWSN.

## 3 System model

In this section, various jamming attacks, the jamming detection metrics employed in existing systems, jamming detection metrics used in the proposed system to identify the presence or absence of jamming in CWS, and finally the system configuration are discussed.

### 3.1 Types of jamming attacks

The proposed system includes four types of jamming such as constant, deceptive, random, and reactive jamming (Xu et al. 2005). Constant jammers continually transmit packets on the medium to jam the communication completely between source and destination. The deceptive jammer continuously generates packets on the medium, which is a dangerous type of jammer since it follows the MAC layer procedure. The random jammer transmits the packets in a regular interval and switches between jamming and sleeping. This type of jammer sleeps for a period of  $RT_s$  time and jams for a period of  $RT_j$  time. The  $RT_s$  and  $RT_j$  values may either be fixed or be in random. Random jammer may operate either as a constant or deceptive jammer during jamming time. Reactive jammer pays attention on communication medium and generates fake packet during data transmission.

### 3.2 Jamming detection metrics

In this section, the jamming detection metrics employed in existing systems and the jamming detection metrics used in the proposed system to identify the presence or absence of jamming in CWSN are discussed.

The jamming detection metrics used in the existing literature are PSR (Xu et al. 2005), PDR (Xu et al. 2005), BPR (Cakiroglu and Ozcerit 2008; Misra et al. 2010), signal-to-noise ratio (SNR) (Misra et al. 2010), energy consumption amount (ECA) (Cakiroglu and Ozcerit 2008), and BER (Mario et al. 2010; Misra et al. 2010). The definition of these metrics is given as follows (Vijayakumar et al. 2015; Ganeshkumar et al. 2016): 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 by destination node, and it 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 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.

In the proposed system, the PDR and RSSI are used as jamming detection metrics for identifying the presence of jamming in CWSN. The rationality of using PDR and RSSI as jamming detection metrics in the proposed system is well described in Vijayakumar et al. (2015), and statistical tests are performed for the following: (1) the rationality of using

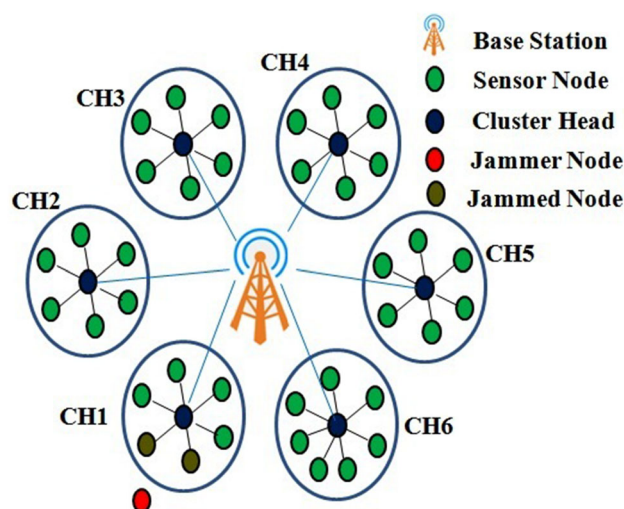


Fig. 1 Cluster-based WSN with a jammer node

PDR and RSSI, (2) to fix the threshold value of PDR, and (3) to classify various types of jamming.

### 3.3 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 (Park et al. 2008) and health-care applications (Fei et al. 2008; Egbogah and Fapojuwo 2011) use downstream data communication. Therefore, the proposed system is modelled by using cluster-based network for detecting the presence of jamming.

The system set-up consists of six clusters, a BS, and a jammer node as shown in Fig. 1. Each cluster consists of seven nodes (one CH and six CMs) except the cluster CH6 which consists of one CH and seven CMs. The system set-up includes totally 43 sensor nodes as per the specification given in Sect. 5.2. 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.

In the system configuration, the dark blue node, green node, red node, and dark green node represent CH, CM, jammer node, and jammed node, respectively. The black line denotes communication between CH and CM. The blue line denotes communication between CHs and BS. The CH1, CH2, CH3, CH4, CH5, and six members are formed into five clusters, respectively. The CH6 and seven members are formed as a cluster. The CH is one-hop distance with CMs and BS. The simulation is performed in fixed CHs (CH1, CH2, CH3, CH4, CH5, and CH6). 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. The proposed system can also be implemented in dynamic environment by deploying existing clustering algorithms (Liu and Shi 2012; Rajshekhar Chalak et al. 2010; Mo et al. 2011; Kang et al. 2012; Azad and Sharma 2013; Hussain et al. 2013; Chen et al. 2010) for selecting the cluster head. 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. In order to avoid the selection of jammer node as CH, the existing trust-based clustering election algorithm (Crosby et al. 2006; Ferdous et al. 2011; Paramasivan and Kaliappan 2014) can be applied along with the proposed system.

To illustrate the proposed system, a jammer is launched deliberately in the cluster CH1. The proposed system is installed in CH and BS. To understand the interactions of the jamming detection metrics (Sect. 3.2) and to measure the impact of various jammers (Sect. 3.1), we have performed simulations in Sect. 5. The simulation is carried out using various models as discussed in Sect. 3.1. In the simulation, a jammer is launched in the first cluster (CH1). This cluster consists of a cluster head (CH1) and six members. From the simulation result, it is observed that the CH1 identifies that the two members are jammed and rest of the members 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 (Sect. 3.1). Based on the simulation, it is justified that the CH has the ability to identify the jammed members. However, in the proposed system, base station can detect the presence of jamming at CH level since the proposed system is also installed in base station.

## 4 Proposed jamming detection system in CWSN

The main idea of this paper is to develop and apply fuzzy inference system (FIS) and adaptive neuro-fuzzy inference system (ANFIS) model for detecting the presence of jamming in CWSN. The proposed system consists of two approaches, namely, (i) fuzzy inference system-based jamming detection system (FIS-JDS) and adaptive neuro-fuzzy inference system-based jamming detection system (ANFIS-JDS), which are proposed for detecting the presence of jamming by computing two jamming detection metrics PDR and RSSI. FIS-JDS approach is based on Takagi–Sugeno fuzzy logic which optimizes the jamming detection metrics. ANFIS-JDS approach combines fuzzy logic and learning ability of the neural network to optimize the metrics for detecting various types of jamming. The constructions of these two approaches are given in next subsections.

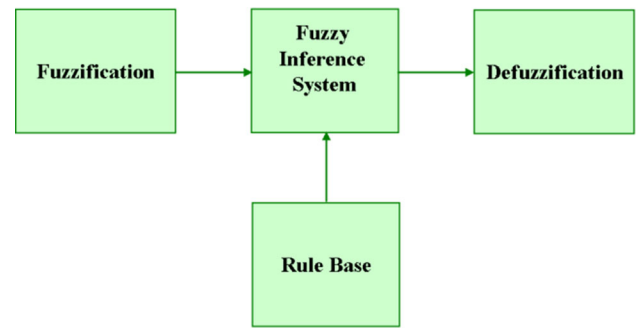


Fig. 2 Fuzzy inference systems

### 4.1 Fis-jds

Fuzzy logic is denoted as multiple-valued logic in which intermediary values are defined as true/false or one/zero. Fuzzy logic uses linguistic variables, fuzzy sets, and membership functions. Linguistic variables are variables, whose values are words or sentences in natural or artificial languages. The linguistic variables are described by fuzzy sets such as low, medium, or high. As an example, consider the word ‘Age’ in natural language; ‘Age’ is a linguistic variable can be defined by fuzzy sets like very young, young, middle age, old, very old. The membership function defines a curve that maps each element of the input space to a fuzzy set by a membership value ranging from 0 and 1. The fuzzy rules constitute the actual knowledge part, and it takes the form:

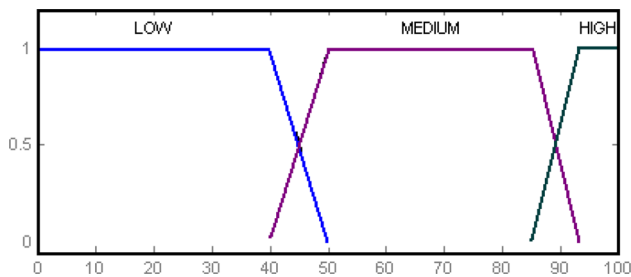
If  $x_1$  is  $A_1$  and If  $x_2$  is  $A_2$  then  $y_1$  is  $B_1$

where  $x_1$ ,  $x_2$ , and  $y_1$  are linguistic variables defined by fuzzy sets on the ranges  $A_1$ ,  $A_2$ , and  $B_1$ , respectively.

The fuzzy inference system (FIS) includes three main components, namely, fuzzification, rule base, and defuzzification, as shown in Fig. 2. (1) The fuzzification transforms the crisp value into degree of membership by using the corresponding membership functions. (The numerical inputs go through the fuzzification process in which the numeric values are mapped to one or more fuzzy values. The number of fuzzy values, beginning and ending parameters are arbitrary and depends on the application. These are generally set by an expert and are subject to modification by simulation and practical experiments.) Membership functions determine the confidence with which a crisp value is associated with a specific linguistic value. (2) Rule base includes set of linguistic statements, called rules. These rules are in the form of IF premise, THEN consequent where the premise consists of fuzzy input variables connected by logical functions (e.g. AND, OR, NOT), and the consequent is a fuzzy output variable. (3) The defuzzification transforms the fuzzy output into crisp value.

**Table 1** Input membership functions with ranges

Input variable	Fuzzy value	$A$	$B$	$c$	$d$
PDR	VERY LOW	− 5	0	30	40
	LOW	30	40	50	60
	MEDIUM	50	60	70	77
	HIGH	70	77	100	100
RSSI	LOW	− 5	0	40	50
	MEDIUM	40	50	85	93.14
	HIGH	85	93.14	100	120

**Fig. 3** PDR membership function

There are three types of FIS such as Takagi–Sugeno, Mamdani, and Tsukamoto. The Sugeno fuzzy model is applied in the proposed system. This model is also called first-order Sugeno model. The rule in Sugeno fuzzy model has the form as follows:

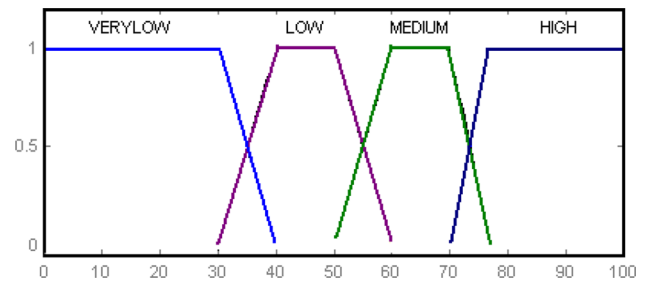
If  $x$  is  $A$  and If  $x$  is  $B$  then  $y$  is  $f = px + qy + m$

where  $x$  and  $y$  are inputs,  $A$  and  $B$  are fuzzy sets,  $p$ ,  $q$ , and  $m$  are parameters which are determined during the training process.

The proposed system uses two jamming detection metrics such as PDR and RSSI for determining the presence or absence of jamming. PDR and RSSI are considered as linguistic variables. In the first-order Sugeno model, the input membership functions, a rule base with fuzzy if–then rules, and output membership function are given as follows:

#### • Input membership functions

1. PDR—The PDR is measured by the cluster head, and measured PDR is represented by the fuzzy set with four linguistic variables VERY LOW, LOW, MEDIUM, and HIGH. The range of each linguistic variable is shown in Table 1. The graphical representation of the trapezoidal functions with respect to PDR is shown in Fig. 3.
2. RSSI—The observed RSSI is expressed with three linguistic variables LOW, MEDIUM, and HIGH. The

**Fig. 4** RSSI membership function

range of each linguistic variable is shown in Table 1. The graphical representation of the trapezoidal functions in respect of RSSI is shown in Fig. 4.

**Rule base** The relationship between the input (PDR, RSSI) and the output variable is performed through a collection of fuzzy rules. Every rule uses AND/OR connectors to associate various input factors with a specific output. The common form of the Sugeno linear output model of the proposed system is

If PDR is  $A_i$  and RSSI is  $B_i$  then  $f = p_i \text{ PDR} + q_i \text{ RSSI} + m_i$

where  $A_i$ ,  $B_i$  are fuzzy sets and  $p_i$ ,  $q_i$ ,  $m_i$  are parameters that are ascertained during the training process. For an example, the rule 1 denotes all the input factors that generate the JC as Extremely High. Initially, the weight of the rule is set to 1 and will be tuned after training the system. The fuzzy rules are given as follows:

1. If PDR is Very Low and RSSI is Low then JC is E-H
2. If PDR is Very Low and RSSI is Medium, then JC is S-H
3. If PDR is Very Low and RSSI is High, then JC is U-H
4. If PDR is Low and RSSI is Low, then JC is A-H
5. If PDR is Low and RSSI is Medium, then JC is High
6. If PDR is Low and RSSI is High, then JC is H-M
7. If PDR is Medium and RSSI is Low, then JC is A-M
8. If PDR is Medium and RSSI is Medium, then JC is L-M
9. If PDR is Medium and RSSI is High, then JC is A-L
10. If PDR is High and RSSI is Low, then JC is Low
11. If PDR is High and RSSI is Medium, then JC is B-L
12. If PDR is High and RSSI is High, then JC is NO

• **Output membership function** Jamming cut-off (JC) is the output function of FIS. The JC is represented with twelve linguistic variables: Extremely High (E-H), Superiorly High (S-H), Ultra High (U-H), Avg. High (A-H), High, High Medium (H-M), Avg. Medium (A-M), Low Medium (L-M), Avg. Low (A-L), Low, Below Low (B-L), and NO. The range of each linguistic variable is shown in Table 2.

**Table 2** Output membership function with range

Output variable	Fuzzy value	$A$	$b$	$c$	$d$
Jamming cut-off (JC)	EXTREMELY HIGH	-5	0	5	10
	SUPERIORLY HIGH	5	10	15	20
	ULTRA HIGH	15	20	25	30
	AVG HIGH	25	30	35	40
	HIGH	35	40	45	50
	HIGH MEDIUM	45	50	55	60
	AVG MEDIUM	55	60	65	70
	LOW MEDIUM	65	70	75	80
	AVG LOW	75	80	85	90
	LOW	85	90	92	94
	BELOW LOW	92	94	96	98
	NO	96	98	100	100

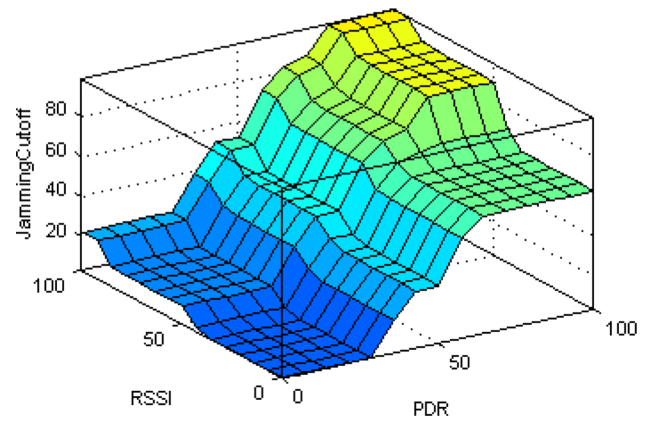
<b>HIGH</b>	<b>NO</b>
<b>A-H</b>	<b>B-L</b>
<b>A-M</b>	<b>L</b>
<b>U-H</b>	<b>A-L</b>
<b>S-H</b>	<b>L-M</b>
<b>E-H</b>	<b>H-M</b>

**Fig. 5** Sugeno model output function

The graphical representation of the trapezoidal functions in respect of PDR is shown in Fig. 5. Figure 6 illustrates the relationship among fuzzy input variables utilized in the fuzzy logic or input and output surface corresponding to the membership functions PDR and RSSI, output membership function Jamming cut-off.

## 4.2 ANFIS-JDS

In this section, the need of ANFIS and the proposed novel adaptive neuro-fuzzy logic-based jamming detection system is described. The fuzzy inference system (FIS) formulates the IF–Then rules to optimize the range of jamming detection metrics such as PDR and RSSI by deploying the trapezoidal function in Sugeno model. The fuzzy logic transforms the decision-making being crisp centric to fuzzy centric. How-

**Fig. 6** Surface plot corresponding to input and output

ever, the FIS does not have the learning ability. The benefit of using an ANFIS over the FIS is ANFIS combines the advantages of fuzzy logic and learning ability of the neural network (NN) to devise a mechanism that solves the problem (Mathur et al. 2016), and it also provides enhanced results as compared to their individual results (Devi et al. 2017). This mechanism utilizes the fuzzy logic to signify knowledge in an understandable way and the learning ability of the neural network to optimize the parameters.

ANFIS model is constructed based on only Sugeno model FIS. The variations between Sugeno and Mamdani models are (1) the Mamdani model uses defuzzification to provide fuzzy output, whereas in Sugeno model, defuzzification uses a weighted average to calculate crisp outputs, and (2) the number of fuzzy rules should be same as number of output functions in Sugeno model unlike Mamdani. The general rule set of first-order Sugeno fuzzy model is given as follows

Rule 1. If  $x$  is  $A_1$  and  $y$  is  $B_1$ , then  $f_1 = p_1x + q_1y + m_1$ .

Rule 2. If  $x$  is  $A_2$  and  $y$  is  $B_2$ , then  $f_2 = p_2x + q_2y + m_2$ .

where  $x$  and  $y$  are the inputs,  $A_i$  and  $B_i$  are the fuzzy sets,  $f_i$  are the outputs within the fuzzy region specified by the fuzzy rule, and  $p_i$ ,  $q_i$ , and  $m_i$  are the design parameters that are determined during the training process.

Figure 7 illustrates the reasoning mechanism for this Sugeno model, which is the basis of the ANFIS model. The ANFIS architecture used to implement these two rules is shown in Fig. 8. In this figure, a circle indicates a fixed node, whereas a square indicates an adaptive node. ANFIS has a five-layered architecture.

In the proposed ANFIS approach, a first-order Takagi–Sugeno fuzzy model with a two inputs and one output is considered. The functioning of ANFIS is a five-layered feed forward neural structure as shown in Fig. 8. The functionality of the nodes in these layers is given as follows;

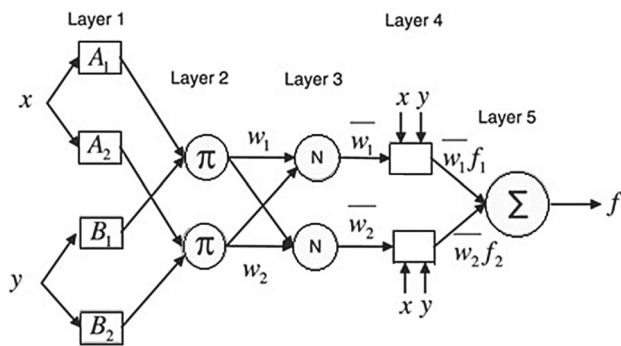


Fig. 7 ANFIS architecture [ANFIS IEEE]

- **Layer 1** The first layer is called as fuzzy layer, which consists of two inputs PDR and RSSI. The PDR and RSSI are the inputs of adaptive node labelled  $A_i$  and  $B_i$  respectively. The  $A_i$  and  $B_i$  are membership functions. The layer 1 outputs are the fuzzy membership degree of the inputs (PDR and RSSI) that are expressed as follows:

$$O_{1,i} = \mu_{A_i}(\text{PDR}) \quad \text{for } i = 1, 2, 3, \dots, n \quad (1)$$

$$O_{1,i} = \mu_{B_i}(\text{RSSI}) \quad \text{for } i = 1, 2, 3, \dots, n \quad (2)$$

where  $\mu_{A_i}$  and  $\mu_{B_i}$  are membership functions for PDR and RSSI, respectively.

- **Layer 2** This layer is called as product layer. Each node in this layer is fixed node labelled  $\Pi$ . The output of the second layer is the product of all incoming data. The output

$w_i$  is the weight function of the next layer and is expressed as follows:

$$O_{2,i} = w_i = \mu_{A_i}(\text{PDR})\mu_{B_i}(\text{RSSI}) \quad \text{for } i = 1, 2, 3, \dots, n \quad (3)$$

where  $O_{2,i}$  is the output of product layer.

- **Layer 3** In this layer, every node is fixed node labelled  $N$ . The  $i$ th node computes the ratio of the  $i$ th rules' firing strength to the sum of all rule firing strengths. The output of this layer is expressed as follows,

$$O_{3,i} = \bar{w}_i = w_i / \sum_{i=1}^n w_i \quad \text{for } i = 1, 2, 3, \dots, n \quad (4)$$

where  $O_{3,i}$  is the output of normalized layer.

- **Layer 4** In the defuzzification layer, the nodes are adaptive nodes with node functions. The defuzzification layer output is represented as follows:

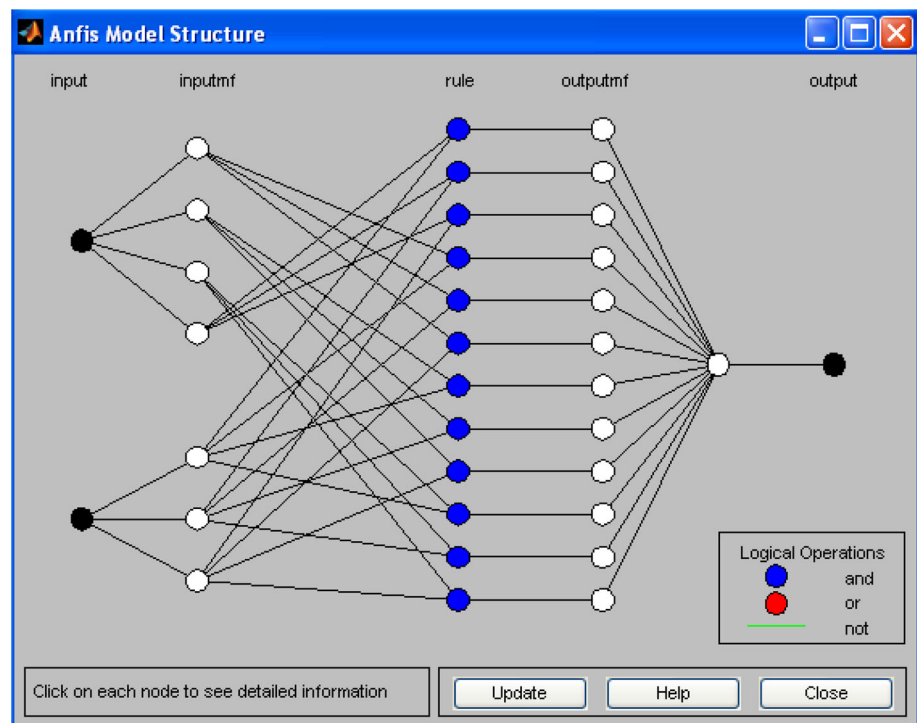
$$O_{4,i} = \bar{w}_i f_i = \bar{w}_i (p_i \text{PDR} + q_i \text{RSSI} + m_i) \quad \text{for } i = 1, 2, 3, \dots, n \quad (5)$$

where  $O_{4,i}$  is the output of defuzzification layer. The  $p_i$ ,  $q_i$  and  $m_i$  are constant parameters.

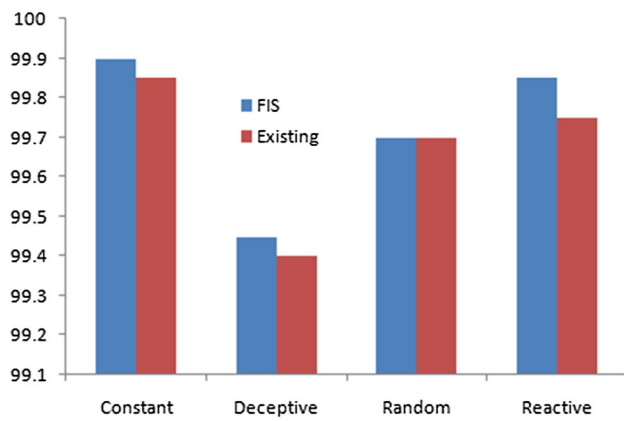
- **Layer 5** This layer is output layer, where single node is labelled  $S$ . The output layer carries out the summation of all incoming data. The overall output of the model is given as follows:

$$O_{5,i} = \sum_{i=1}^n \bar{w}_i f_i = \sum_{i=1}^n w_i f_i / \sum_{i=1}^n w_i \quad \text{for } i = 1, 2, 3, \dots, n \quad (6)$$

Fig. 8 The ANFIS structure for detection of jamming in WSN







**Fig. 9** Comparison of FIS-JDS and existing system with respect to TDR for various types of jammer

where  $O_{5,i}$  is the output of the system. The ANFIS structure for the proposed system to detect the presence of jamming is shown in Fig. 8.

## 5 Result and discussions

In this section, first, the individual performance of the proposed systems FIS and ANFIS approach is discussed. Next, the performance of FIS approach is compared with the existing system (Mathur et al. 2016) and then compared with ANFIS approach. Both FIS and ANFIS are modelled by using MATLAB. The performance of individual approaches FIS and ANFIS is described below.

### 5.1 Performance measure of FIS-JDS

The performance of the proposed FIS-JDS is assessed in terms of true detection ratio (TDR). 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. That is, TDR is estimated by dividing the true positive index (TPI) over summation of true positive index and false negative index (FNI). The TDR is expressed as follows:

$$\text{TDR} = \text{TPI} / (\text{TPI} + \text{FNI}) \quad (7)$$

where TPI represents number of correctly detected jammed nodes and FNI denotes the number of nodes that are not jammed, but these nodes are actually jammed.

Now the performance evaluation metric TDR of the proposed FIS-JDS is compared with the existing systems (Mathur et al. 2016) as shown in Fig. 9. From Fig. 9, it is evident that the proposed FIS-JDS system achieves TDR as high as 99.9% and negligible false detection ratio (FDR) (the comparison of FIS-JDS with existing system is not included since estimated FDR value is negligible).

The analysis of variance (ANOVA) test is applied for determining to determine whether there is any significant difference between the means of FIS-JDS and Jamming detection mechanism (JM) (Mathur et al. 2016). The one-way ANOVA is performed on the samples to state that there is difference between the three population means or not.

The ANOVA test analyses the null hypothesis  $H_0 : \mu(a) = \mu(b)$  against the alternative hypothesis,  $H_1 : \mu(a) \neq \mu(b)$  where  $\mu(a)$  and  $\mu(b)$  are means of two populations. The null hypothesis states that there is no difference between the three population means (i.e. there is no difference between the TDR of FIS-JDS and JM). The alternate hypothesis states that there is difference between the three population means (i.e. there is difference between the TDR of FIS-JDS and JM). The results of estimation of one-way ANOVA are shown in Table 3. The sum of squares and mean square for all sam-

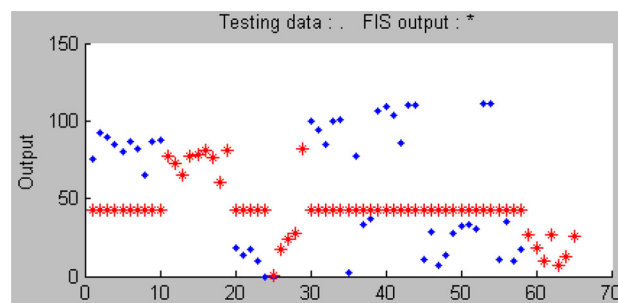
**Table 3** Results of ANOVA between TDR for various jamming of FIS-JDS and JM

Analysis of results of TDR for various jamming		Sum of square	Degree of freedom (df)	Mean square	F	Significance (P)
Constant	Between detection systems	2.8	1	2.8	10.88889	0.001542
	Within detection system	17.48571	68	0.257143		
	Total	20.28571	69			
Deceptive	Between detection systems	0.057143	1	0.057143	0.109677	0.74153
	Within detection system	35.42857	68	0.510008		
	Total	35.48571	69			
Random	Between detection systems	6.3	1	6.3	11.07386	0.001416
	Within detection system	36.68571	68	0.568908		
	Total	44.98571	69			
Reactive	Between detection systems	6.3	1	6.3	15.88347	0.000167
	Within detection system	26.97143	68	0.396639		
	Total	33.27143	69			

**Table 4** Specification of ANFIS

Specification	Value
Number of nodes	43
Number of linear parameters	36
Number of nonlinear parameters	28
Total no. of parameters	64
No. of training data pairs	100
Number of fuzzy rules	12

ples are estimated for between the class (FIS-JDS and JM) and within the class. The degree of freedom (df) denotes the number of independent sample. The Fisher or F statistic determines that if the value of F is greater than one, then it refers that there exists difference between class (FIS-JDS and JM); otherwise, the difference between the class does not exist. The F value of constant, random, and reactive jamming is 10.88889, 11.07386, and 15.88347, respectively. From Table 3, it is noted that the F value of constant, random, and reactive jamming is greater than '1' except deceptive jamming. This states that the difference between class (FIS-JDS and JM) means exists. Then, the statistical significance ( $P$  value) is established. The  $P$  value is used to indicate a probability that we compute on observed samples. If the  $P$  value is less than the significance level ( $\alpha$ ), then the null hypothesis is rejected and the alternate hypothesis is accepted. The significance level ( $\alpha$ ) is considered as 0.05. The  $P$  value of constant, random, and reactive jamming is 0.001542, 0.001416, and 0.000167, respectively. It is evident that the  $P$  value of constant, random, and reactive jamming

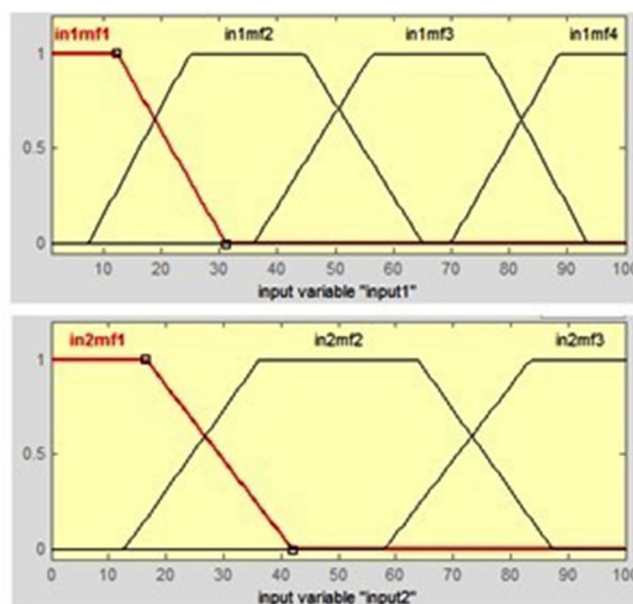
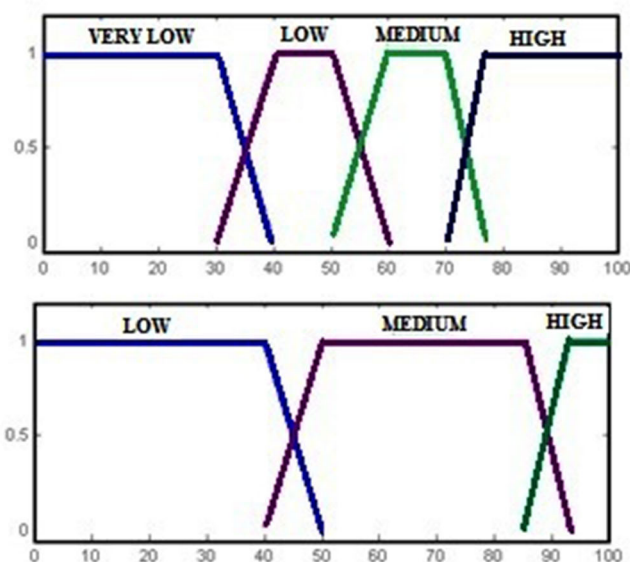
**Fig. 11** Testing error of ANFIS-JDS

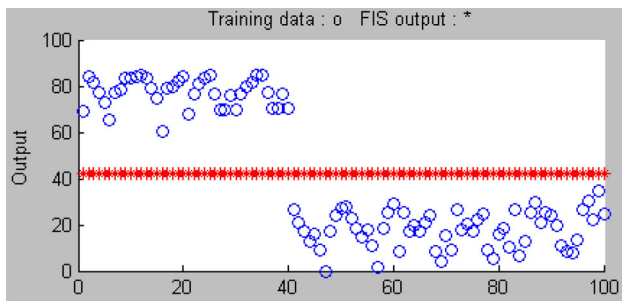
is less than the significance level 0.05 ( $\alpha$ ). Thus, it proves the significance of alternate hypothesis  $H_1$  for constant, random, and reactive jamming (i.e. there is statistically significance difference between the TDR of FIS-JDS and JM). But, the  $P$  value of deceptive jamming is 0.74153 and the  $P$  value is greater than significance level 0.05. Therefore, null hypothesis  $H_0$  is significance for deceptive jamming. Hence, it is concluded that the proposed FIS-JDS approach works well than the existing system (JM).

## 5.2 Performance measure of ANFIS-JDS

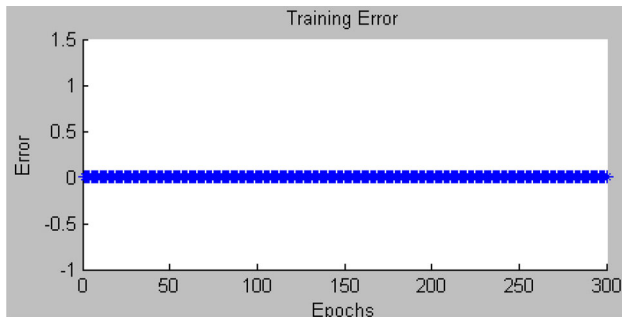
The ANFIS modelling is carried out using ANFIS editor in MATLAB. The ANFIS specification of the proposed system is shown in Table 4. The performance metrics of the ANFIS model include trainability, training time, and training error.

The objective of the training is to adjust the parameters, specifically the input membership function parameters and the corresponding output values. The training needs two

**Fig. 10** Membership functions of inputs (PDR, RSSI) before and after training



**Fig. 12** Training error of ANFIS-JDS



**Fig. 13** Training error mapping Sugeno to ANFIS-JDS

types of data, namely, training data and testing data. The training data are a set of records which consist of  $[r \times c]$ , where  $r$  denotes the number of rows that holds input values and  $c = f + 1$ , where  $f$  is the number of input factors in the proposed model,  $c = 3$ . Each row includes three columns: first two columns contain the values of the two input factors (PDR, RSSI) and the last column contains the value for the corresponding output. The testing data contain the data in the same way as the training data, but the testing data are accurate and smaller than the training data. In the ANFIS editor, three sets of training data are used to train the ANFIS. The training and testing data include 100 and 65 records, respectively. The input membership function parameters of the FIS before and after training are shown in Fig. 10.

The testing error and training error obtained from the ANFIS editor are shown in Fig. 11 and Fig. 12. This model is run for several times in order to minimize the error as shown in Fig. 13.

Now, the proposed jamming detection approaches FIS and ANFIS are compared by using statistical measurements. The measurements are Root Mean Square Error (RMSE), RMSE percentage (RP), and the precision. The RMSE, RP, and precision are expressed as

$$\text{RMSE} = \sqrt{\sum_{i=1}^n (\bar{a} - a)^2 / n - 1} \quad (8)$$

$$\text{RP} = \text{RMSE} / \mu(a) \quad (9)$$

where  $\bar{a}$  denotes the anticipated value,  $y$  indicates the actual value,  $n$  represents the number of data items, and  $\mu(a)$  signifies mean of the actual data.

The proposed jamming detection approaches FIS-JDS and ANFIS-JDS are assessed using RMSE, RMSE%, and precision as shown in Table 5. The precision denotes the number of nodes is correctly detected as jammed, also referred as TDR. The RMSE, RP, precision of FIS-JDS for various jamming such as constant jamming, deceptive jamming, random, and reactive jamming are (0.29, 0.0029, 99.9), (0.95, 0.0096, 99.45), (0.59, 0.0059, 99.7), and (0.38, 0.0038, 99.85), respectively. The RMSE, RP, precision of ANFIS-JDS for various jamming such as constant jamming, deceptive jamming, random, and reactive jamming are (0.24, 0.0024, 99.92), (0.72, 0.0073, 99.6), (0.45, 0.0045, 99.8), and (0.29, 0.0029, 99.91), respectively. From Table 5, it is evident that the value of RMSE for training data of all types of jamming of ANFIS-JDS is smaller than FIS-JDS. Furthermore, the precision value of ANFIS approach for various jamming (99.92, 99.6, 99.8, 99.91) is higher than the precision values of FIS approach for various jamming (99.9, 99.45, 99.7, 99.85). Thus, it is concluded that the ANFIS approach works excellently than the FIS approach to detect the presence of various types of jamming in the CWSN.

## 6 Conclusion

In this paper, an adaptive neuro-fuzzy inference system-based jamming detection approach is proposed for detecting various forms of jamming attacks. The proposed approach is employed in both CH and BS to identify attacks in clus-

**Table 5** Performance of jamming detection approaches (FIS-JDS and ANFIS-JDS)

Training data for various types of jamming	FIS			ANFIS		
	RMSE	RP	Precision	RMSE	RP	Precision
Constant	0.297044	0.002973	99.9	0.242536	0.002427	99.92286
Deceptive	0.954864	0.009601	99.45	0.727607	0.007305	99.6
Random	0.594089	0.005958	99.7	0.453743	0.004547	99.8
Reactive	0.383482	0.00384	99.85	0.297044	0.002973	99.91429

ter member and cluster head level, respectively, by using two jamming detection metrics PDR and RSSI. To exhibit the performance of the proposed approaches, FIS-JDS and ANFIS-JDS are simulated using MATLAB. The statistical tests are carried out to compare the performance of the proposed system with existing system. The result of the simulation and the ANOVA test proves that the ANFIS approach works better than FIS-JDS approach and the existing system. In future, it is planned to extend the achievement of our proposed approach and deploy in real-world environment.

## Compliance with ethical standards

**Conflict of interest** The authors declare that they have no conflict of interest.

**Human and animal rights** We have not performed any experiments which involve animals or humans.

## References

- Abbasi AA, Younis M (2007) A survey on clustering algorithms for wireless sensor networks. *Comput Commun* 30(14–15):2826–2841
- Akyildiz IF, Su W, Sankarasubramanian Y, Cayirci E (2002) Wireless sensor networks: a survey. *Comput Netw* 38(4):393–422
- Alrajeh NA, Khan S, Shams B (2013) Intrusion detection systems in wireless sensor networks: a review. *Int J Distrib Sens Netw* 2013:1–7
- Azad P, Sharma V (2013) Cluster head selection in wireless sensor networks under fuzzy environment. *ISRN Sens Netw* 2013:1–8
- Boyinbode O, Le H, Mbogho A, Takizawa M, Poliah R (2010) A survey on clustering algorithms for wireless sensor networks. In: *Proceedings of the 13th international conference on network-based information systems*, pp 358–364. <https://doi.org/10.1109/nbis.2010.59>
- Cakiroglu M, Ozcerit AT (2008) Jamming detection mechanisms for wireless sensor networks. In: *Proceedings of the 3rd international conference on scalable information systems*, pp 4–6, June 2008
- Chen J-S, Hong Z-W, Wang N-C, Jhuang S-H (2010) Efficient cluster head selection methods for wireless sensor networks. *J Netw* 5(8):964–970
- Crosby GV, Pissinou N, Gadze J (2006) A framework for trust-based cluster head election in wireless sensor networks. In: *Proceedings of 2nd IEEE workshop on dependability and security in sensor networks and systems*, Columbia, pp 13–22
- Devi R, Jha RK, Gupta A, Jain S, Kumar P (2017) Implementation of intrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network. *Int J Electron Commun* 74:94–106
- Egbogah EE, Fapojuwo AO (2011) A survey of system architecture requirements for health care-based wireless sensor networks. *Sensors* 11:4875–4898
- Fei H, Jiang M, Celentano L, Xiao Y (2008) Robust medical ad hoc sensor networks (MASN) with wavelet-based ECG data mining. *Ad Hoc Netw* 6(7):986–1012
- Ferdous R, Muthukkumarasamy V, Sithirasenan E (2011) Trust-based cluster head selection algorithm for mobile ad hoc networks. In: *IEEE 10th international conference on trust, security and privacy in computing and communications (TrustCom)*, Changsha, pp 589–596
- Ganeshkumar P, Vijayakumar KP, Anandaraj M (2016) A novel jammer detection framework for cluster based wireless sensor networks. *EURASIP J Wirel Commun Netw*. <https://doi.org/10.1186/s13638-016-0528-1>
- Hong S, Lim S, Song J (2011) Unified modeling language based analysis of security attacks in wireless sensor networks: a survey. *KSII Trans Internet Inf Syst*. <https://doi.org/10.3837/tiis.2011.04.010>
- Hussain K, Abdullah AH, Iqbal S, Awan KM, Ahsan F (2013) Efficient cluster head selection algorithm for MANET. *J Comput Netw Commun* 2013:7
- Jo M, Han L, Duy Tan N, Peter H (2015) A survey: energy exhausting attacks in MAC protocols in WBANs. *Telecommun Syst* 58(2):153–164. <https://doi.org/10.1007/s11235-014-9897-0>
- Kang S, Lee S, Ahn S, An S (2012) Energy efficient topology control based on sociological cluster in wireless sensor networks. *KSII Trans Internet Inf Syst* 6(1):339–358
- Kuila P, Jana PK (2012) Improved load balanced clustering algorithm for wireless sensor networks. *Adv Comput Netw Secur* 7135:399–404
- Kumar D (2014) Performance analysis of energy efficient clustering protocol for maximizing lifetime of wireless sensor networks. *IET Wirel Sens Syst* 4(1):9–16
- Liu X (2012) A survey on clustering routing protocols in wireless sensor networks. *Sensors* 12(8):11113–11153. <https://doi.org/10.3390/s120811113>
- Liu X, Shi J (2012) Clustering routing algorithms in wireless sensor networks: an overview. *KSII Trans Internet Inf Syst* 6(7):1735–1755
- Manju VC, Kumar MS (2012) Detection of jamming style DoS attack in wireless sensor network. In: *Proceedings of second IEEE international conference on parallel distributed and grid computing (PDGC)*, pp 563–567
- Mario S, Boris D, Srdjan C (2010) Detection of reactive jamming in sensor networks. *ACM Trans Sens Netw*. <https://doi.org/10.1145/1824766.1824772>
- Mathur N, Glesk I, Buis A (2016) Comparison of adaptive neuro-fuzzy inference system (ANFIS) and Gaussian processes for machine learning (GPML) algorithms for the prediction of skin temperature in lower limb prostheses. *Med Eng Phys* 38(10):1083–1089
- Misra S, Singh R, Rohith Mohan SV (2010) Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. *Sensors* 10(4):3444–3479
- Mo S, Chen H, Yinglong L (2011) Clustering-based routing for top-k querying in wireless sensor networks. *EURASIP J Wirel Commun Netw* 2011:73
- Mokammel Haque M, Pathan A-SK, Hong CS, Huh E-N (2008) An asymmetric key-based security architecture for wireless sensor networks. *KSII Trans Internet Inf Syst*. <https://doi.org/10.3837/tiis.2008.05.004>
- Paramasivan B, Kaliappan M (2014) Secure and fair cluster head selection protocol for enhancing security in mobile ad hoc networks. *Sci World J* 2014:1–6
- Park S-J, Vedantham R, Sivakumar R, Akyildiz IF (2008) GARUDA: achieving effective reliability for downstream communication in wireless sensor networks. *IEEE Trans Mob Comput* 7(2):214–230
- Rajshekhar Chalak A, Misra S, Obaidat MC (2010) A cluster-head selection algorithm for wireless sensor networks. In: *17th IEEE international conference on electronics, circuits, and systems ICECS*, pp 130–133
- Rani TP, Jayakumar C (2012) Survey on key pre distribution for security in wireless sensor networks. *Adv Comput Sci Inf Technol Netw Commun* 84:248–252. [https://doi.org/10.1007/978-3-642-27299-8\\_26](https://doi.org/10.1007/978-3-642-27299-8_26)

- Shi E, Perrig A (2004) Designing secure sensor networks. *IEEE Wirel Commun* 11(6):38–43
- Shon T, Park Y (2009) A hybrid adaptive security framework for IEEE 802.15.4-based wireless sensor networks. *KSII Trans Internet Inf Syst*. <https://doi.org/10.3837/tiis.2009.06.002>
- Siddhabathula K, Dong Q, Liu D, Wright M (2012) Fast jamming detection in sensor networks. In: *Proceedings of IEEE international conference on communications*, pp 934–938
- Sikander G, Zafar MH, Raza A, Babar MI, Mahmud SA, Khan GM (2013) A survey of cluster based routing schemes for wireless sensor network. *Smart Comput Rev* 13(4):261–275
- Singh SP, Sharma SC (2015) A survey on cluster based routing protocols in wireless sensor networks. *Procedia Comput Sci* 45:687–695
- Vijayakumar KP, Ganeshkumar P, Anandaraj M (2015) A novel jamming detection technique in wireless sensor networks. *KSII Trans Internet Inf Syst* 9(10):4223–4249
- Vijayakumar KP, Ganeshkumar P, Anandaraj M, Selvaraj K, Sivakumar P (2018) Fuzzy logic-based jamming detection algorithm for cluster based wireless sensor network. *Int J Commun Syst* 31:e3567. <https://doi.org/10.1002/dac.3567>
- Wang XY, Wong A (2013) Multi-parametric clustering for sensor node coordination in cognitive wireless sensor networks. *PLoS ONE*. <https://doi.org/10.1371/journal.pone.0053434>
- Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: *Proceedings of the sixth ACM international symposium on mobile ad hoc networking and computing*, pp 46–57, Nov 2005
- Yadav RK, Kumar V, Kumar R (2015) A discrete particle swarm optimization based clustering algorithm for wireless sensor networks. *Adv Intell Syst Comput* 338:137–144

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.