Intrusion detection based on fuzzy logic for wireless body area networks: review and proposition

Asmae Bengag, Amina Bengag, Omar Moussaoui
Mathematics, signal and image processing and computing research Laboratory, Higher School of Technology,
Mohammed First University, Oujda, Morocco

Article Info

Article history:

Received Nov 27, 2021
Revised Feb 21, 2022
Accepted Mar 10, 2022

Keywords:

Artificial intelligence
Attacks
Fuzzy logic
Intrusion detection system
Network security
Wireless body area network

ABSTRACT

Wireless body area networks (WBANs) are very helpful for monitoring the patient's case, due to the medical sensors. However, this technology faces several problems such as loss communication, security issues and energy consumption. Our work focused on the security and specifically the intrusion detection system (IDS), which is one of the most effective techniques used to identify the presence of intrusions in a network. To make the IDS more efficient, the fuzzy logic (FL) is one of the well-known techniques that is known for its powerful mechanism used to differentiate network traffic levels. In this paper, we start to present an overview of IDS and FL functionality. Moreover, we give a survey of recent works dealing IDS based on FL in wireless sensor and classify them on different measures. Hence, our comparative study is very helpful for the researchers, to understand the use of FL in IDS and have clear vision for developing their own security solution. In the second part, we develop a novel IDS based on Mamdani type fuzzy inference system for detecting jamming attacks in WBAN. Our IDS was built in Matlab, also we are used Castalia platform and OMNET++ simulator to simulate different scenarios of WBAN.

Corresponding Author:

Asmae Bengag
Mathematics, signal and image processing and computing research Laboratory
Higher School of Technology, Mohammed First University
BP 473 Complexe universitaire Al Qods, Oujda 60000, Morocco
Email: a1.bengag@ump.ac.ma

1. INTRODUCTION

In the recent time, wireless body area network (WBAN) network becomes one of the important parts of our daily life that improves the quality of the healthcare and studies, including emergency medical and remote medical surveillance. Indeed, the main component in WBAN system is the mini-medical sensors that are attached in the human body, in order to collect and transmit medical data such as temperature, cancer detection and heart rate. This data will be transmitted in three communication levels. The first one is called Intra-WBAN communication, in which the data is between the medical sensors and the coordinator node, using for example ZigBee (802.15.4) or Bluetooth (802.15.1) as communication protocols. After that, the coordinator node communicates with one or more point access using for instance WiFi; this part is named Inter-WBAN communication. Then, the third level is called beyond-WBAN communication in which the medical data is received to the medical center via mobile network [1], [2]. In the event that the sensor collects abnormal data, it will launch an alert to the medical team. Therefore, WBAN system helps to provide better care and to supervise the patients in real time via the wireless communication, in order to make the supervised person moves freely and easily.

Although the wireless communication is offering many benefits, it still facing various and serious problems, as low power, lost communication and secure data. In fact, security field is the most critical challenging in WBANs [3]. The communication mode used can be easily attacked by different anomalies and attacks, which threats sensitive data and reduces the quality-of-service (QoS), especially the quality of healthcare as shown on the Figure 1. More seriously, in the case of emergency, the sensors could be unavailable that are not be able to send or receive any information because of an intrusion as denial of service (DoS) attack. Besides, other attacks push the sensors to consume a lot of energy and involve the collision between nodes [4]. These problems may cause severe damage to the patient [5]. Therefore, it is very important to develop a controller on the system like the intrusion detection system, which is one of the most useful security solutions for monitoring the network traffic and detecting attacks. However, the mechanism used in the intrusion detection system (IDS) still suffers from different challenges such as binary decision, in which increase the false alarm rate.

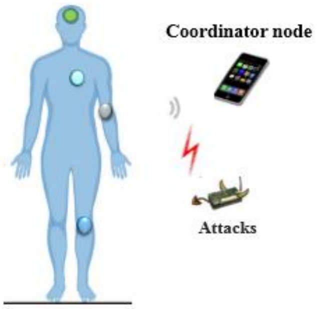


Figure 1. The scenario of WBAN with an attack [2]

Over the years, the artificial intelligence provides many benefits for implementing IDS, by taking care of the energy consumption rate [6]. There are several types of attack detection that apply the mechanisms of AI technologies, such as support vector machine (SVM), game theory, neural networks, decision tree and fuzzy inference systems (FIS), which allowed to improve the quality of IDS. Indeed, fuzzy logic system is very close to human reasoning and can predict uncertain operating problems. In the case of IDS, FLS will allow to make good decisions and help the system to estimate the results under ambiguous information, with low false alert and high detection rate. The objective of this paper is to present the benefits of applying and implementing the fuzzy logic in the intrusion detection system. Furthemore, we proposed a novel IDS based on Mamdani fuzzy inference system for jamming attacks in WBAN system. Our proposed IDS is based on three main network parameters: Packet delivery ratio (PDR), received strength signal indication (RSSI), and energy consumption amount (ECA).

The key contributions of our work discuss how fuzzy logic can be applied in the IDS to optimize the detection of an attack in wireless network. Besides, we study the advantages and disadvantages of each work in order to select the more efficient mechanism in terms of energy consumption and detection for WBAN system. The rest of paper is organized as follows: section 2 gives an overview of the IDS functionality, by presenting the metrics used for measuring the performance of an IDS and classifying detection approaches. Then, we present the main components of the fuzzy logic system. Section 3 describes the previous works that integrate FL into the IDS to detect an attack in the wireless sensor network (WSN). In section 4, we classify the previous proposed techniques and discuss the best method that will be used in a WBAN network. Finally, we conclude the paper by highlighting some future directions of research in WBAN security.

2. OVERVIEW OF IDS AND FUZZY LOGIC

2.1. Intrusion detection system

In the last few years, the intrusion detection system has become one of the major components in network security scheme, which based on specific parameters linked with the system. Furthermore, the main goal of the IDS is to supervise the network traffic by differentiating the legitimate scenarios from the abnormal one, in order to launch alerts and inform the concerned person in real time. Basically, the IDS could be implemented in different ways: on specific device as host intrusion detection system, or to control all network traffics as network intrusion detection system [7]. However, the IDS system has two biggest drawbacks that include false positives and negatives detection.

2.1.1. Detection performance metrics

The detection techniques are measured by different metrics in order to define the detection performance. In this section, we present the main metrics used.

- False negative (FN): is collected by the IDS as normal activity when the activity is actually an attack, and the system does not generate an alarm in emergency cases [8], [9]. In fact, the FN is the most serious and state, in which the detection does not generate an alert on the necessary malicious traffic.
- False positive (FP): is identified by the IDS as an intrusion or an attack on the network when the activity is normal behavior [10]. For example, the legitimate user has entered an incorrect password several times.
- True positive (TP): is a successful detection that is correctly identified by IDS as an attack and the activity is truly an attack.
- True negative (TN): is like the TP, which is correctly identified by IDS as legitimate activity and the activity is really normal.
- True detection rate (TDR): represents the successfully detection of the attack by calculating the ratio of the true positive index (TPI) by the sum of TPI and false negative index (FNI) [9]. This metric is expressed as (1).

$$\mathrm{TDR} = \frac{\mathrm{TPI}}{\mathrm{TPI+FNI}} \tag{1}$$

- False positive rate (FPR): indicates the ratio of the number of nodes misidentified by the IDS (there is no attack).
- False alarm rate (FAR): is a number of false positive or false negative. These cases make the intrusion detection not able to distinct anomaly signal with events that causes.
- Detection accuracy: is actually presented as an important metric that calculates the degree of a detection mechanism if it is consistent with the correct identification of malicious packets from DDoS traffic. This metric is based on the ratio of false negative and false positive rates to the detection of DDoS attacks [9]. Indeed, this metric is calculated according to four main criteria, which are FN, FP, TN and TP [11].

$$\mathrm{AC} = \frac{\mathrm{TN+TP}}{\mathrm{TN+FN+TP+FP}} \tag{2}$$

- Complexity: defines the complexity of the detection system basing on various metrics as memory storage and time [10].

2.1.2. Classification of detection approaches

Each research chooses a detection approach depending on the data type, working environment and type of attack. Indeed, basing on various researches [9], [12], [13] we can classify the detection approaches into misuse detection system, anomaly detection, hybrid detection, and specification based detection, as shown in Figure 2.

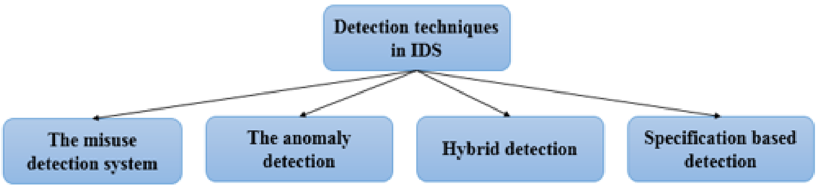

Detection techniques in IDS
The misuse detection system
The anomaly detection
Hybrid detection
Specification based detection

Figure 2. Detection techniques in IDS

- The misuse detection system: this detection is known also as signature detection and rule-based detection that detects an intruder on the system or network, based on the signature of the attack. With this method, important modules are used from an existing dataset in which produces a low false alarm that can cover a wide range of known attacks [13]. Nevertheless, the misuse detection cannot detect a novel attack that it must frequently update a signature to define a new attack [14].
- The anomaly detection: is also called detection-anomaly-based that is considered to identify an abnormal activity on a system. The anomaly detection tries to collect a set of data as a normal case, which helps to differentiate normal behavior from attacks and then launch an alert [15]. This technique based on different measures as statistical analysis, threshold detection and rule-based measures. Nevertheless, anomaly detection generates many false alerts because the data collected is not stable, which leads a weak detection.

- Hybrid detection: the objective of this method is to optimize the detection of an intrusion on a system by combining the detection by anomaly and the misuse detection system [13]. Although this approach offers higher detection accuracy, it involves a high complexity and implementation cost [9].
- Specification based detection: uses specifically to describe the correct operation of a protocol or system in order to monitor them. This action depends on the constraints of each area where the IDS is implemented [13]. The disadvantage of this method is that it is not efficient in term of detecting novel attacks as the anomaly detection.

2.2. Fuzzy logic system

Zadeh [16] built a fuzzy logic in 1965, which is a methodology for defining a good result based on ambiguous or inaccurate input information used on various fields like medical service, digital image processing, intelligent personal assistant and language processing. In general, fuzzy logic system is deployed for any kind of application related with uncertainty [17]. The FLS is done as human reasoning by determining the inputs parameters into outputs. Fundamentally, there are four main components of fuzzy logic system as shown in Figure 3 [18] namely, fuzzification, rule evaluation, aggregation of the rule, and defuzzification.

- The fuzzification: is based on the crisp inputs in order to transform them into fuzzy inputs [15], [19]. In general, the crisp inputs are extracted from the network traffic as real values, which are passed in the next component of fuzzy system "Fuzzification".
- The rule evaluation consists to compute the output basing on several logical rules in the form IF-THEN statements [20].
- The aggregation of the rule combines different rules in order to define all situations in the network and generate the final decision.
- Defuzzification: translates the output into a crisp values [21].

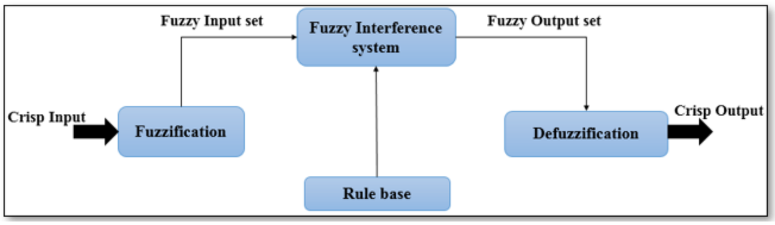


Figure 3. General fuzzy system architecture

In fuzzy logic, each input and output have the degree of truth that demonstrated by membership function (MF). The MF represents the degree between 0 and 1 over an interval of the crisp variable, which can have different forms as trapezoidal, Bell curves and triangular. Basically, there are two models of fuzzy logic system, namely, Mamdani and Takog-Sugeno model [22]. Mamdani model is developed by Ebrahim Mamdani [23] which is a set of linguistic control rules analyzed to create a control system, as well as the functions of output membership are the fuzzy sets [24], [21]. After that, Sugeno and Kang proposed a Sugeno model [25] which generates fuzzy rules from a specified input-output data set. The general rule set of first order Sugeno fuzzy model is given as (3) and (4).

Rule 1. If x is A1 and y is B1, then $f1=p1x + q1y + m1$. (3)

Rule 2. If x is A2 and y is B2, then $f2=p2x + q2y + m2$. (4)

The main differences between these two models of fuzzy logic that is Mamdani model uses defuzzification to offer fuzzy output, while in Sugeno model, defuzzification is done by using weighted average to calculate crisp outputs [18] and it is more efficient in terms of defuzzifcation. More specifically, in Sugeno model, the number of fuzzy rules should be the same as number of output functions and is not the case in Mamdani [18].

3. LITERATURE SURVEY

Recently, there are many works of intrusion detection systems based on several strategies as threshold, fuzzy logic and machine learning, to detect an attack in the network. Most previous studies are implemented on WSN, but they can be applied in WBAN network. In this section, we describe the functionalities of the previous works, in order to identify the most efficient techniques for the WBAN system.

Vijayakumaretal *et al.* [26] proposed a jamming detection technique called fuzzy logic-based jamming detection algorithm (FLJDA) for optimizing the jamming detection in cluster-based WSN (CWSN). In the proposed technique, the Mamdani's fuzzy model is applied FLJDA implementing in downstream data communication (from BS to sensors) using the PDR and RSSI as input parameters. In fact, the evaluation of these parameters values is calculated by the cluster head (CH), in order to determine if the members of cluster are under jamming or not. Vijayakumar *et al.* [18] developed two approaches for detecting the presence of jamming attack in CWSN, by calculating two parameters, namely, PDR and RSSI. The first one is fuzzy inference system based jamming detection system (FIS-JDS) that used for optimizing the detection by applying Takagi-Sugeno fuzzy logic. This proposed technique is implemented in CH and base station (BS), the CH detects the presence of jamming in CMs, while the BS can identify if the CH is jammed. The second approach called the adaptive neuro-fuzzy inference system (ANFIS-JDS) that uses learning ability with existing dataset for the prediction of future values to detect various types of jamming.

The work in Reyes and Kaabouch [27] focuses on detecting jamming attacks in wireless networks by verifying a link loss, which based on fuzzy logic technique using four parameters bad packet ratio (BPR), packet delivery ratio (PDR), received strength signal (RSS), and clear channel assessment (CCA) as inputs metrics. These parameters are used for calculating a jamming index (JI) to indicate the jamming level (high, medium or low). In the same way, Levonevskiy et al. have proposed a method that based on a vector of fuzzy values to detect DDoS attacks [28] by monitoring the network characteristics as packet size and ratio of received traffic to outgoing traffic. The theory of fuzzy logic is implemented also [29] to predict exhaustion attacks over the IEEE 802.15.4 MAC layer, using FCM clustering. The fuzzy based detection and prediction system (FBDPS) technique [19] is applied in IEEE 802.15.4 low rate wireless personal area networks (LR-WPAN), for detecting and predicting an attack that effects availability, which is a DoS. Furthermore, the authors selected BPR or packets dropped per terminal (PDPT) and signal to noise ratio (SNR) as crisp inputs to the system in order to make decision for attack detection by calculating the level of attack (LOA) as crisp output.

Differently, the authors suggested another model for detecting DDoS attack in the network, by calculating hurst parameters (H) as input parameters in the fuzzy logic system [30]. The H represents the degree of selfsimilarity that related with long-range dependence, which has value between 0 and 1. Nguyen *et al.* [31] proposed a novel technique to detect anomaly network traffic in wireless sensor network, using a fuzzy inference system. They are applied the Mamdani inference to identify features of sensory traffic, with two inputs parameters: mean and variance of sensory data. Chaudhary *et al.* [32] are implemented the sugeno type fuzzy inference system on the IDS for detecting the flooding attack in mobile ad hoc networks. The fuzzy inference is applied in each node to calculate the level of truth and check the behavior of the node. This method is based on two main input parameters, namely, number of request packet received and average no. of received route request packet as destination.

Furthermore, a novel IDS is proposed in Chaudhary *et al.* [33] for detecting packet dropping attack in MANETs using Mamdani fuzzy inference system, which simulated by QualNet simulator 6.1. The traffic listening is used to extracted the input parameters, namely, data packet forwarded ratio and data packet forwarded ratio. Hiremath *et al.* [24] implemented a novel technique for the detection and prediction of cooperator Black Hole attack in MANETs, basing on the adaptive fuzzy inference system. This last one contains four crisp inputs: trust, data rate, data loss and energy. However, this technique has a drawback in term consumption of energy because it makes the member of nodes send periodically data for checking the values of the four parameters. Differently, fuzzy logic is not only used to optimize the detection of an attack, but it can also be used to monitor the forest from the fire, as Bolourchi *et al.* [34] proposed an intelligent fire detection system implemented on the sensors that based on Mamdani model, for monitoring big forest. The mechanism uses five inputs parameters as temperature, smoke, light, humidity and distance. Besides, there are other techniques use fuzzy logic for having a low consumption energy in the sleep/idle case for the wireless body area networks. Gouda and Kabat [6] develop an energy efficient of MAC protocol called fuzzy_TADMAC protocol using the fuzzy logic that are implemented in OMNET++ simulator. They are based on three fuzzy input variables (data rate, Fuzzy Wakeup Acknowledgement at time e instant Ti and priority) and fuzzy Wakeup Acknowledgement at time instant Ti+1 as output variables.

4. FINDINGS

4.1. Comparaison criteria of proposed IDS

As shown in the previous section, each technique of IDS utilized its crisp inputs, membership function and fuzzy model. In, Table 1 we indicated a detailed comparison of the previous techniques. First, we start by illustrating the used comparaison measures:

- Type of fuzzy model presents the type of fuzzy model, which can be Mamdani or Sugeno model.
- Crisp inputs: are parameters used as indicators to detect an attack.
- Output parameter: is considered the result or degree of presence of the attack in the network.
- Simulator: the simulator used to simulate the normal and abnormal scenarios.
- Best performance results (accuracy): this measure used to study the performance of the proposed method such as TDR, TPR, and FPR.

Table 1. Summary of reviewed literature

Articles	The approaches used	Type of fuzzy model	Crisp Inputs	Output parameter	Simulator	Best performance results (Accuracy)
[26]	FLJDA: Fuzzy logic-based jamming detection algorithm	Mamdani	-PDR -RSSI	Jamming cutoff (JC) or center of gravity (COG)	Matlab 7.1, NS2 simulator	True detection ratio: 99.89%
[18]	FIS-JDS: Fuzzy inference system-based jamming detection system & ANFIS-JDS: Applying neuro-fuzzy inference jamming detection system	Takagi–Sugeno	-PDR -RSSI	Jamming cutoff (JC)	Matlab tool	FIS-JDS and ANFIS-JDS achieve TDR more than: 99.4%
[27]	Lost link detection using FIS	Mamdani	-BPR -PDR -RSS -CCA	Jamming index (JI)	Matlab, NS2 simulator	98.4 % and 95.25% efficiency in detecting constant and random jamming respectively
[19]	Fuzzy based detection and prediction system (FBDPS)	---	-BPR -SNR	Level of Attack (LOA) or center of gravity (COG)	NS2 simulator	Performance having average of 99.75%
[28]	Network Attacks Detection Using Fuzzy Logic	---	-Ratio of the incoming traffic to the outgoing -Packet size	---	---	---
[24]	Adaptive system of fuzzy inference to detect and prevent the black hole attack	Takagi–Sugeno	-Trust -Data loss -Data rate -Energy	Output		The PDR is increased by 98.63%
[22]	To detect anomaly traffic basing on Fuzzy Logic	Mamdani	-Expected value -Variance value of the sensor data.	---	Matlab tool	Higher accuracy
[32]	To detect flooding attack in mobile ad hoc networks.	Takagi–Sugeno	-Number of request packet received -Average no. of received route request packet as destination	Verity Level	Qualnet simulator 6.1, Matlab tool	High true positive rate under: Low mobility: 99.1% Medium mobility: 95.4% High mobility: 91.1%
[33]	IDS based on fuzzy logic used to detect packet-dropping attack in MANETs.	Mamdani	-Data Packet Forwarded Ratio -Data Packet Dropped Rate	Verity Level	Qualnet simulator 6.1	True positive rate: 98.3% False positive rate: 1.3%
[29]	Detection of Exhaustion Attacks over IEEE 802.15.4 MAC Layer Using Fuzzy Logic System.	---	-Energy decay rate (EDR) -Attack detection rate (ADR)	Multiobjective optimization	---	Higher accuracy
[31]	Anomaly Traffic Detection Based on Fuzzy Logic Approach in WSN.	Mamdani	-Mean of sensory data -Variance of sensory data	Probability of sensory data	Matlab tool	Higher accuracy

Most of these researchers prove their models using one or more performance metric that evaluate the detection approaches. The performance of the proposed system in [17], [24] are evaluated in terms of TDR and FDR, they are achieved at least “99.4%” of true detection ratio (TDR), whereas the FDR is negligible. In addition, the authors [26] are based on the efficiency that is “98.4%” in detecting jamming, which is calculated according to four main criteria: the total number of simultated situations (N), the number of misdetection (m), the number of false alarms (f), and the number of results with the wrong reason (r). This metric is mathematically defined as $Efficiency = (N - m - f - r)/N$. Howerver, the proposed method [23] is evaluated by calculating the PDR, throughput and end-to-end.

4.2. Pros and cons of proposed IDS for WBAN

Actually, each method presents advantages and disadvantages for WBAN system, in terms of energy consumption, detection rate, false positives and negatives alert rates. Regarding the detection**,** the attack detection solution is implemented on the cluster head that is able to compute the linguistic variables of each cluster member, in order to consume minimum energy of nodes. Papers such as [18], [19], [24], [26], [29] are used this solution that is more efficient in the case of WBAN system. In this case, we propose that is more efficient to implement the IDS based on FLS in a coordinator node or personal digital device (PDA). More specifically, the PDA will be used as a cluster head to collect, analyze and compute the parameters from the medical sensors (cluster member), and verify wheither the sensor is under jamming attack or not.

However, some method as [14], [19], [27], [28] require a complicated calculation on the nodes, which is costly in terms of energy. The technique [27] makes the member of nodes send periodically data for checking the values of the four inputs parameters (BPR, PDR, RSS, and CCA). Moreover, the fuzzy rules need to be modified every time according to the changes of topology, in order to optimize the detection. In this case, it is preferable to apply fuzzy logic system with other intelligent mechanism as neural networks learning.

5. PROPOSED METHOD

5.1. Description

In this section, we present our proposed IDS based on Mamdani type fuzzy inference system for detection jamming attacks in WBAN system. In fact, we are used three network parameters used as crisp inputs: PDR, RSSI, and ECA as illustrates in Figure 4. The parameters values were valued by the FIS to calculate and define the output, which represents the probability of jamming level called jamming detection index (JDI). The three parameters are used as jamming attack metrics that are changed depending to the normal and abnormal condition of the medical sensor.

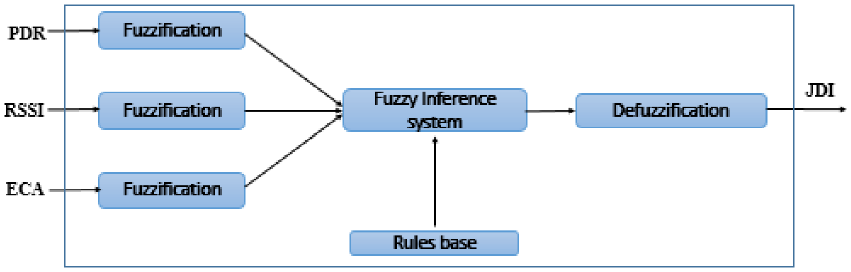


Figure 4. Fuzzy logic system of our proposed system

The PDR is presented as the ratio of the number of packages deliverd correctly sent by the node to the total number of packets sent [35]. Concerning RSSI is the power level received by a sensor. Whereas, the ECA presents the amount energy consumed by the node in a specified time for a node.

There are some cases resemble the jamming cases that called the false positive rate like imperfect connection, low energy and collision problem. Hence, the combination of these parameters allows our IDS to reduce the FPR and increase the TDR. The FIS system uses three trapezoidal membership functions for each input (PDR, RSSI, and ECA) and output JDI that define the membership to low, medium and high. For example, the Figure 5 illustrates the combined membership function for the PDR parameter.

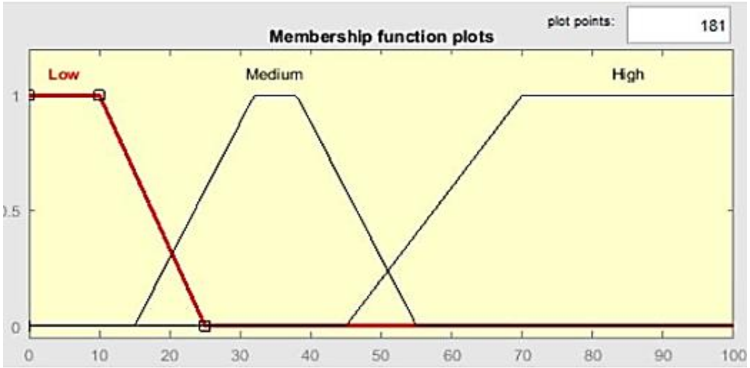


Figure 5. Combined MF for the PDR parameter

The Table 2 gives the values of MFs (A, B, C, and D) of that are defined according to our several scenarios in normal and abnormal cases (under jamming). The set of rules is one of the important elements of the FIS. We are based on the Comb method to define the set of rules in order to avoid combinatorial explosion [36]. As we are mentioned above, our system based on three linguistic variables with three possible levels (low, medium and high), if we apply a traditional fuzzy system, we have 27 rules (3^3). While, with the Comb method, we can reduce the number of rules on 9 rules (3*3). In fact, we eliminated some rules that are not necessary and they have no advantage in the system in order to reduce the complexity of the calculation. For instance, in case the RSSI is low, then we can conclude that medical node is not under a jamming attack. Besides, if the PDF value is higher, we can conclude that medical sensor is not subject to jamming attack, whatever the value of ECA and RSSI. The nine fuzzy rules are defined to identify the degree of JDI level. Some of these rules are given as:

- If PDR is High then JDI is low;
- If RSSI is low then JDI is low;
- If PDR is low and RSSI is medium and ECA is low then JDI is medium;
- If PDR is low and RSSI is high and ECA is high then JDI is high;

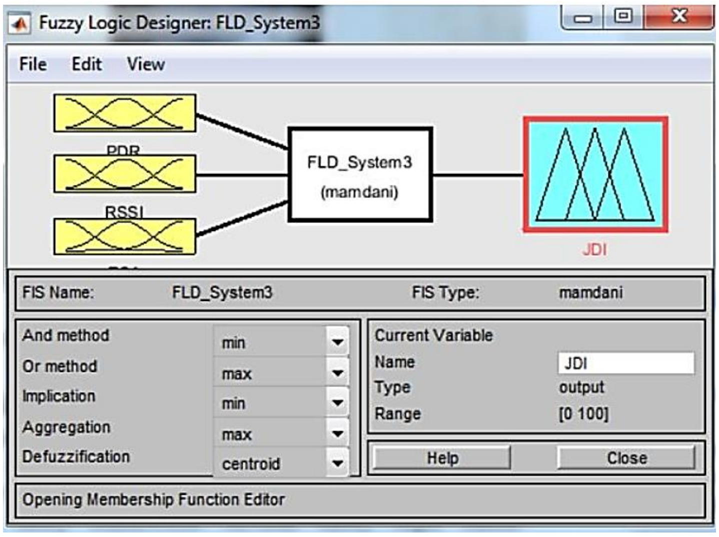
Table 2. Varibles values used in MFs

Input variable	Membership function	A	B	C	D
PDR	Low	-0.5	0	10	25
	medium	15	32	38	55
	high	45	70	100	102
ECA	Low	-0.5	0	5	10
	medium	5	10	25	30
	high	25	30	100	102
RSSI	Low	-0.5	0	5	10
	medium	5	10	15	20
	high	15	20	100	102

5.2. Tests and results

In this section, we present our methodology that we followed for evaluating our proposed IDS. Firstly, we are used Castalia platform under OMNET++ simulator to simulate a WBAN system in different scenarios, normal and abnormal cases. Indeed, according to the architecture of the WBAN network, our work is focused on the communication between the medical nodes and the coordinator node. More specifically, our normal scenario contains three medical sensors attached on the human body and a coordinator node communicated via ZigBee (802.15.4 MAC). Then, we studied the impacts of jamming attacks by simulating a WBAN system under a jammer node in diverse cases, basing on various positions of the the jammer node according to the medical nodes. We are used the BypassMac for the jammer node that does not respect the MAC protocol mechanism.

Secondly, the parameters values PDR, ECA and RSSI will be studied in our proposed techniques that was built in Matlab as shown in Figure 6. Indeed, the matlab fuzzy logic Toolbox aims us to identify crisp inputs, crisp output, MFs and rules base using the graphical interface. The fuzzy operators (AND or OR) are used to interpret the relationships obtained from the rules base. Indeed, the surface viewer is used to represent the output surface for our fuzzy system. The Figure 7 shows the surface view of the relationship between the Inputs parameters (PDR and RSSI) and the output JDI.



FIS Name: FLD_System3
FIS Type: mamdani

And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: JDI
Type: output
Range: [0 100]

Opening Membership Function Editor

Figure 6. Fuzzy inference system editor

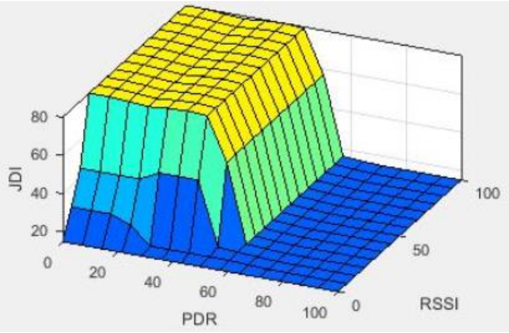


Figure 7. Surface view of the inputs PDR and RSSI

Our system is able to control the communication of the WBAN network and specify the level of jamming detection index (low, medium, or high), as presented in Table 3. In addition, our proposed system aims to differentiate two types of jamming attacks, which could be constant jamming and reactive jamming. These two types present in the network when the legitimate node has a high RSSI and low PDR. In fact, other cases increase the power transmission and decrease the PDR due to the propagation loss, for instance, the case where the coordinator node has exceeded the authorized distance with the medical node. Furthermore, the objective of adding the ECA parameter to reduce the false positive rate and increase the detection rate. This meteric aims also our proposed IDS to differentiate the constant and reactive jamming. The first one causes a higher consumption of energy by forcing the legitimate nodes to stay in listening mode. While, the ECA remains normal under reactive jamming, because this type disrupts the communication when the legitimate send the packet RTS [1]. The Table 3 shows some examples of simulations results.

Basing on the result, the proposed fuzzy based intrusion detection system is able to detect and identify the jamming attacks in WBAN network, with high true positive rate and low false positive rate. Indeed, our proposed technique was evaluated by four main metrics: Detection rate (DR), FPR, TPR, and efficiency as demonstrated in Table 4. The proposed system provides 100% of detection rate, with 98.04% of efficiency. We have also obtained 96.15% for TPR and 3.22% for FPR.

Table 3. Evaluting the traffic network using our proposed IDS

Inputs			Output		
PDR	RSSI	ECA	JDI value	JDI Level	Possible cause/Decision
16.48	88	20	78	High	Jammed: High power constant jamming
9	90	4.21	80.14	High	Jammed: High power reactive jamming
62.58	9	4.22	15.55	Low	Propagation loss (distance)
97.57	26	5	14.88	Low	Not jammed
96.98	15	3.07	14.88	Low	Not jammed
17.9	90	23	78.20	High	Jammed: High power constant jamming
61.84	10	4.63	15.61	Low	Propagation loss (distance)
52.88	55	8.5	37.624	Medium	Not jammed: Propagation loss
62.67	15	4	15.54	Low	Not jammed: Collision case
9.70	76	25.39	78	High	Jammed: High power constant jamming
0	83	30	80.14	High	Level is very high
99.24	14	5.13	14.88	Low	Not jammed
99.58	6	4.99	14.88	Low	Not jammed
99.58	10	5.10	14.88	Low	Not jammed
67	12	22	15.14	Low	Multi-path interference
43	55	4.56	45	Medium	Propagation loss (distance)

Table 4. Proposed jamming detection performance

Metrics	DR	TPR	FPR	Efficiency
Rules	$\frac{\text{Number of attacks detected}}{\text{Total number of existing attacks}}$	$\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}$	$\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}$	$\frac{\mathrm{N}-(\mathrm{m}+\mathrm{f}+\mathrm{r})}{\mathrm{N}}$
Jamming attacks	100%	96.15%	3,22%	98,04%

6. CONCLUSION

In this review paper, we presented a survey of several detection techniques based on fuzzy logic system to detect attacks in wireless sensor network. Our work provides new researchers to discover and understand the different detection approaches and the metrics used for measuring the proposed techniques as detection rate, false and negative rate. Furthermore, we are classified various proposed techniques for treating and defining the most efficient for WBAN system. According our classification, we have concluded that is very useful to implement the IDS based on FL in the coordinator node, which has no problem in term of energy consumption and computational capability. More specificaly, it is preferable to use the coordinator node as cluster head in order to calculate the input parameters for each medical sensors (cluster members) and identify if the sensor is under jamming attacks or not. In this paper, we are also proposed a novel robust IDS based on Mamdani type fuzzy inference system that detectes jamming attacks in WBAN system. According to the results, our proposed IDS ables to control WBAN network traffic, which we have obtained 98.04% efficiency in detecting jamming attacks in WBAN system.

ACKNOWLEDGEMENTS

This work is supported by the Hassan II Academy of Sciences and Technologies and Mohammed First University, Morocco.

REFERENCES

[1] A. Bengag, O. Moussaoui, and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," in *2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS)*, Oct. 2019, pp. 1–5, doi: 10.1109/ICDS47004.2019.8942268.

[2] A. Bengag, A. Bengag, and O. Moussaoui, "Attacks classification and a novel IDS for detecting jamming attack in WBAN," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 2, pp. 80–86, 2020, doi: 10.25046/aj050210.

[3] A. Bengag, A. Bengag, and O. Moussaoui, "Effective and robust detection of jamming attacks for WBAN-based healthcare monitoring systems," *Lect. Notes Electric Engenering*, vol. 681, pp. 169–174, 2021.

[4] A. Bengag, A. Bengag, and O. Moussaoui, "Classification of security attacks in WBAN for medical healthcare," in *The 4th International Conference on Networking, Information Systems amp Security.*, Apr. 2021, pp. 1–5, doi: 10.1145/3454127.3456605.

[5] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "Authentication techniques and methodologies used in wireless body area Networks," *Journal of Systems Architecture*, vol. 101, p. 101655, Dec. 2019, doi: 10.1016/j.sysarc.2019.101655.

[6] K. C. Gouda and M. R. Kabat, "Traffic aware dynamic MAC protocol using fuzzy logic controller for wireless body area networks," in *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, Jun. 2018, pp. 204–209, doi: 10.1109/ICCONS.2018.8663081.

[7] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, Sep. 2017, pp. 277–282, doi: 10.1109/SISY.2017.8080566.

[8] C.-Y. Ho, Y.-C. Lai, I.-W. Chen, F.-Y. Wang, and W.-H. Tai, "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 146–154, Mar. 2012, doi: 10.1109/MCOM.2012.6163595.

[9] P. Kaur, M. Kumar, and A. Bhandari, "A review of detection approaches for distributed denial of service attacks," *Systems Science & Control Engineering*, vol. 5, no. 1, pp. 301–320, Jan. 2017, doi: 10.1080/21642583.2017.1331768.

[10] G. C. Tjhai, M. Papadaki, S. Furnell, and N. L. Clarke, "Investigating the problem of IDS false alarms: An experimental study using Snort," *IFIP International Federation for Information Processing*, vol. 278, pp. 253–267, 2008.

[11] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 4, pp. 541–553, Oct. 2019, doi: 10.1016/j.jksuci.2018.03.011.

[12] R. S. Chaudhari and G. R. Talmale, "A review on detection approaches for distributed denial of service attacks," in *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, Feb. 2019, pp. 323–327, doi: 10.1109/ISS1.2019.8908125.

[13] S. Potteti and N. Parati, "Intrusion detection system using hybrid Fuzzy Genetic algorithm," in *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, May 2017, pp. 613–618, doi: 10.1109/ICOEI.2017.8300775.

[14] A. S. Subaira and P. Anitha, "Efficient classification mechanism for network intrusion detection system based on data mining techniques: A survey," in *2014 IEEE 8th International Conference on Intelligent Systems and Control (ISCO)*, Jan. 2014, pp. 274–280, doi: 10.1109/ISCO.2014.7103959.

[15] S. P. Thakare and M. Ali, "Introducing fuzzy logic in network intrusion detection system," *International Journal of Advanced Research in Computer Science*, vol. 3, no. 3, pp. 1–6, 2012.

[16] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965, doi: 10.1016/S0019-9958(65)90241-X.

[17] V. Rajaram, S. Srividhya, and N. Kumaratharan, "Impact of fuzzy inference system for improving the network lifetime in wireless sensor networks – a survey," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, Apr. 2018, pp. 0933–0937, doi: 10.1109/ICCSP.2018.8524341.

[18] K. P. Vijayakumar, K. P. M. Kumar, K. Kottilingam, T. Karthick, P. Vijayakumar, and P. Ganeshkumar, "An adaptive neuro-fuzzy logic based jamming detection system in WSN," *Soft Computing*, vol. 23, no. 8, pp. 2655–2667, Apr. 2019, doi: 10.1007/s00500-018-3636-5.

[19] C. Balarengadurai and S. Saraswathi, "Fuzzy based detection and prediction of DDoS attacks in IEEE 802. 15. 4 low rate wireless personal area network," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, no. 6, pp. 294–301, 2013.

[20] M. Blej and M. Azizi, "Comparison of Mamdani-type and Sugeno-type fuzzy inference systems for fuzzy real time scheduling," *International Journal of Applied Engineering Research*, vol. 11, no. 22, pp. 11071–11075, 2016.

[21] P. Kumari, M. P. Singh, and P. Kumar, "Survey of clustering algorithms using fuzzy logic in wireless sensor network," in *2013 International Conference on Energy Efficient Technologies for Sustainability*, Apr. 2013, pp. 924–928, doi: 10.1109/ICEETS.2013.6533511.

[22] M. Almseidin and K. Szilveszter, "Intrusion detection mechanism using fuzzy rule interpolation," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 16, pp. 5473–5488, 2018.

[23] E. H. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," *International Journal of Man-Machine Studies*, vol. 7, no. 1, pp. 1–13, Jan. 1975, doi: 10.1016/S0020-7373(75)80002-2.

[24] P. S. Hiremath, Anuradha T, and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," in *2016 International Conference on Information Science (ICIS)*, Aug. 2016, pp. 245–251, doi: 10.1109/INFOSCI.2016.7845335.

[25] M. Sugeno, *Industrial applications of fuzzy control*. New York: Elsevier Science Inc., 1985.

[26] K. P. Vijayakumar, P. Ganeshkumar, M. Anandaraj, K. Selvaraj, and P. Sivakumar, "Fuzzy logic-based jamming detection algorithm for cluster-based wireless sensor network," *International Journal of Communication Systems*, vol. 31, no. 10, p. e3567, Jul. 2018, doi: 10.1002/dac.3567.

[27] H. I. Reyes and N. Kaabouch, "Jamming and lost link detection in wireless networks with fuzzy logic," *International Journal of Scientific & Engineering Research*, vol. 4, no. 2, pp. 1–7, 2013.

[28] D. K. Levonevskiy, R. R. Fatkieva, and S. R. Ryzhkov, "Network attacks detection using fuzzy logic," in *2015 XVIII International Conference on Soft Computing and Measurements (SCM)*, May 2015, pp. 243–244, doi: 10.1109/SCM.2015.7190470.

[29] C. Balarengadurai and S. Saraswathi, "Detection of exhaustion attacks over IEEE 802.15.4 MAC layer using fuzzy logic system," in *2012 12th International Conference on Intelligent Systems Design and Applications (ISDA)*, Nov. 2012, pp. 527–532, doi: 10.1109/ISDA.2012.6416593.

[30] S. Pharande, P. Pawar, P. W. Wani, and A. B. Patki, "Application of Hurst parameter and fuzzy logic for denial of service attack detection," in *2015 IEEE International Advance Computing Conference (IACC)*, Jun. 2015, pp. 834–838, doi: 10.1109/IADCC.2015.7154823.

[31] V.-T. Nguyen, T.-X. Nguyen, T.-M. Hoang, and N.-L. Vu, "A new anomaly traffic detection based on fuzzy logic approach in wireless sensor networks," in *Proceedings of the Tenth International Symposium on Information and Communication Technology - SoICT 2019*, 2019, pp. 205–209, doi: 10.1145/3368926.3369714.

[32] A. Chaudhary, V. Tiwari, and A. Kumar, "A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks," in *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, May 2014, pp. 1–4, doi: 10.1109/ICRAIE.2014.6909148.

[33] A. Chaudhary, A. Kumar, and V. N. Tiwari, "A reliable solution against Packet dropping attack due to malicious nodes using fuzzy logic in MANETs," in *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, Feb. 2014, pp. 178–181, doi: 10.1109/ICROIT.2014.6798326.

[34] P. Bolourchi and S. Uysal, "Forest fire detection in wireless sensor network using fuzzy logic," in *2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks*, Jun. 2013, pp. 83–87, doi: 10.1109/CICSYN.2013.32.

[35] M. Çakıroğlu and A. T. Özcerit, "Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 19, no. 1, pp. 1–19, 2011, doi: 10.3906/elk-0912-334.

[36] W. E. Combs and J. E. Andrews, "Combinatorial rule explosion eliminated by a fuzzy rule configuration," *IEEE Transactions on Fuzzy Systems*, vol. 6, no. 1, pp. 1–11, 1998, doi: 10.1109/91.660804.

BIOGRAPHIES OF AUTHORS

Asmae Bengag is currently a Ph.D student Computer Engineering at Mathematics, signal and image processing and computing research Laboratory (MATSI), EST Oujda, Mohammed 1st University scince 2018 (Morocco). She has a M.Sc. degree in internet of things from ENSAF in Sidi Mohamed Ben Abdellah University in Fez, Morocco (2018). Her research focusses on Network technology, WBAN, Network Security, IDS, Artificial Intelligence, and routing protocols. She can be contacted at email: asmaebengag@gmail.com.

Amina Bengag was graduated from ENSAO with a degree of state engineer Telecommunication and Networks in 2016. She obtained her Ph.D in Computer Science in 2021 from Mohammed 1st University Oujda (Morocco). Her research focusses on VANET, Routing protocols, IT Security, Artificial Intelligence, Computer Networking, Virtualization, and WBAN. She can be contacted at email: bengag.amina@gmail.com.

Prof. Dr. Omar Moussaoui is an Associate Professor at the Higher School of Technology (ESTO) of Mohammed First University, Oujda, Morocco. He has been a member of the Computer Science Department of ESTO since 2013. He is currently director of the MATSI research laboratory. Omar completed his Ph. D. in computer science at the University of Cergy-Pontoise France in 2006. His research interests lie in the fields of IoT, AI, Wireless Networks and Security. He has actively collaborated with researchers in several other computer science disciplines. He participated in several scientific and organizing committees of international conferences. He served as reviewer for numerous international journals. He has more than 20 publications in international journals and conferences, and he has co-authored 2 book chapters. Omar is an instructor for CISCO Networking Academy on CCNA Routing, and Switching and CCNA Security. He can be contacted at email: o.moussaoui@ump.ac.ma.