A Fuzzy Logic-Based Intrusion Detection System for WBAN Against Jamming Attacks

Asmae Bengag, Amina Bengag, Omar Moussaoui, and Blej Mohamed

Abstract Wireless Body Area Network (WBAN) is a set of special nodes called medical sensors. These sensors are very useful and helpful for making the user able to connect everywhere and every time. However, they suffer from many problems like the low computing capacity, energy and memory space. In terms of security, WBAN systems are threatened by various types of attacks due to the wireless communication. This technology must have a robust mechanism to detect attacks for making medical applications more reliable and safety. In our work, we have focused on identifying jamming attacks from WBAN using the fuzzy logic system (FLS) that is one of the powerful mechanisms of artificial intelligence (AI) to determine different network cases. The proposed system used one of the fuzzy inference methods named Mamdani model and based on three network parameters Packet delivery ratio (PDR), received strength signal indicator (RSSI) and energy consumption amount (ECA). Our intrusion detection system is simulated by using MATLAB 9.0 and Castalia for analyzing the output result as jamming detection index (JDI).

Keywords WBAN · Security · Intrusion detection system · Jamming · Fuzzy logic · Mamdani model · False alert

1 Introduction

Currently, WBAN becomes one of the important parts of our daily life that improves the quality of the health care and studies, including emergency medical and remote medical surveillance [1]. This technology is based on mini medical sensors that are attached in the human body in order to communicate with the medical center using wireless. In fact, the medical nodes transmit a sensitive data via wireless medium to the coordinator node or the personnel device assistant (PDA) using ZigBee (802.15.4)

A. Bengag (✉) · A. Bengag · O. Moussaoui · B. Mohamed
MATSI Research Laboratory, ESTO, Mohammed First University, Oujda, Morocco
e-mail: asmaebengag@gmail.com

H. Bekkay et al. (eds.), *Proceedings of the 3rd International Conference on Electronic Engineering and Renewable Energy Systems*, Lecture Notes in Electrical Engineering 954, https://doi.org/10.1007/978-981-19-6223-3_1

or Bluetooth (802.15.1) [2]. After that, the data is transmitted to the medical center using mobile networks or internet. However, this communication is not reliable because it deployed in open radio frequencies and in various attacks [3, 4]. Jamming attack is one of the attacks that threats the availability of the network as a security aspect. This attack makes the legitimate nodes not able to send or receive any information by transmitting a high-range signal. More specifically, it disrupts the communication between the medical nodes and involves the collision between them, and it causes the energy consumption of the sensors.

The intrusion detection system (IDS) has become an essential solution security, for detecting an intrusion in a system. We can implement an IDS in two ways, the first one on specific device as host intrusion detection system and the second way as a controller for the network. Indeed, the IDS is one of the effective solutions to detect and monitor an intrusion in the network as jamming attacks. Nevertheless, there are various challenges used in detection techniques as the binary decision [5]. For instance, the IDS can classify normal activities as an intrusion that increases the false alerts. Therefore, the FLS is used to solve diverse kinds of problems and makes the IDS to take the good decisions with high detection attack and low false alert.

In this paper, we aim to develop a novel IDS based on the fuzzy logic using Mamdani inference mechanism, to detect jamming attacks in WBAN. The proposed solution uses three network parameters, namely PDR, RSSI and ECA that are implemented as crisp inputs in FLS, to identify the network state and detect jamming attacks. More specifically, the parameters values were valued by the fuzzy inference system (FIS) to calculate the level of jamming, which is called jamming detection index (JDI).

The rest of the paper is organized as follows: Sect. 2 gives an overview of the main components of the fuzzy logic system. In Sect. 3, we present briefly some previous mechanisms based on FLS that detect jamming attacks. After that, we describe the performance of our proposed technique by explaining why we used the three parameters and how we calculated the level of jamming attack via FLS. Finally, we conclude our paper and give some future works.

2 Related Work

There has been different mechanisms for studding the state of the network in the literature to ameliorate the security issues in wireless sensor network (WSN), in order to detect jamming attacks. In fact, various techniques have been proposed for WSN that could be implemented in WBAN. In this section, we give a set of previous techniques for jamming detection based on fuzzy logic.

In [6], fuzzy logic is applied for determining node's malicious level in WSN, by calculating two metrics packet delivery ratio (PDR) and packet loss ratio (PLR). The simulation results are evaluated in MATLAB 7 and NS2. The authors in [7] proposed a

system named fuzzy logic-based jamming detection algorithm (FLJDA) for detecting jamming. This mechanism applied the Mamdani model using two input parameters PDR and RSSI. Indeed, the cluster head is used to calculate these parameters to identify if the cluster member is jammed or not.

Vijayakumar et al. [8] developed two methods for detecting the presence of jamming attack in cluster-based WSN (CWSN), using two main parameters RSSI and PDR. The first technique is named fuzzy inference system-based jamming detection system, which consists to optimize the detection by applying Takagi–Sugeno fuzzy model. The second one uses learning ability named the adaptive neuro-fuzzy inference system, basing on existing dataset for the prediction of the future values to detect various types of jamming. Reyes et al. [9] proposed a mechanism to check a link loss based on fuzzy logic technique, using the following inputs: PDR, RSS, bad packet ratio (BPR) and clear channel assessment (CCA). This technique is used to identify the level of jamming index (low, medium or high) in WSN.

Angrishi et al. [10] suggested the fuzzy-based detection and prediction system mechanism that is implemented on IEEE 802.15.4 low-rate wireless personal area network (LR-WPAN). This technique used two crisp inputs signal to noise ratio (SNR) and packets dropped per terminal (PDPT), for predicting and detecting DoS that affects the availability of the network.

3 Overview of Fuzzy Logic System

In recent times, the FLS is used in different real-time applications such as intelligent personnel, medical service, temperature monitoring and digital image processing, in order to identify the superlative decision. This methodology is built by Lotfi A. Zadeh professor in 1965 [11], to handle the uncertainty and ambiguity made from human reasoning. Principally, the FLS involves four main elements as shown in Fig. 2, namely fuzzification, fuzzy rules, fuzzy inference system and defuzzification.

The crisp inputs are collected from network traffic as real values in the first part of the fuzzy system named "fuzzification", in order to transform them into fuzzy inputs set. Then, with help of fuzzy rules, the fuzzy inference consists to calculate the crisp output set from the fuzzified input via fuzzy logic [5]. Basically, the FIS involves several rules base in the form IF-THEN statement, to optimize the range by using membership function (MF) [11]. Finally, the defuzzification translates the output into crisp values. Indeed, the MF determines the membership value or the degree of truth of each input and output between 0 and 1. The most shapes used for the MF are as follow: bell curves, triangular and trapezoidal.

There are three models of FIS, namely Mamdani, Sugeno and Tsukamoto models. The fundamental difference among these three models is how fuzzy input generates the crisp output [11]. In general, Mamdani model is based on the Center of Gravity mechanism used in the defuzzfication process, to get the fuzzy output [12]. On other hand, the Sugeno and Tsukamto calculate the crisp output using the weighted average [11]. Therefore, our proposed IDS employs the Mamdani because it is the

most appropriate for our system in detecting jamming attacks in WBAN. The fuzzy inference rule of Mamdani model is written as in (*A*) [7], where *x*, *y* and *z* are fuzzy sets linguistic variables defined by fuzzy sets. The linguistic values are presented in *A* and *B*, whereas the output is defined in *C*.

$$\text{Rule} = \text{If } x \text{ is } A \text{ and } y \text{ is } B, \text{ then } z \text{ is } C(A)$$

4 Proposed Fuzzy Logic Detection Jamming

4.1 Description

The proposed intrusion detection system used the FIS with three main network parameters: PDR, RSSI and ECA as illustrated in Fig. 3. These parameters are used as the jamming attack metrics in order to evaluate the network state. The PDR is presented as the ratio of the number of packets successfully sent by the node to the total number of packets transmitted by the node [9]. The RSSI metric presents the power content of the received radio signal at the receptor [4]. Besides, the ECA is the amount energy consumed by the node in a specified time for a sensor node [13].

The main reason for choosing these parameters is they are changed depending to the normal and abnormal conditions of the medical sensor. Furthermore, these parameters are used to avoid as much as possible the cases resemble the jamming cases, called the false positive alerts. For instance, these last could be the problems related to the collision problem, low energy or imperfect connection. Therefore, The FIS uses these parameters as crisps inputs, defined with three fuzzy sets: low (L), medium (M) and high (H), whereas the MF for the output has four fuzzy sets as follows: very low (VL), low (L), medium (M) and high (H). The output is a Jamming Detection Index (JDI) that represents the probability of jamming level in the network. The JDI value varies from 0 to 100, indicating "low jamming" to "high jamming", respectively.

Actually, to fuzzify the inputs and identify the fuzzy MF, we used the trapezoidal membership functions with the Mamdani inference method for the rules base. Indeed, the trapezoid shape is chosen because it can be mathematically manipulated to be very close to the most natural function [11]. Figure 4 illustrates the combination of three trapezoidal functions for the PDR parameter.

The generation of fuzzy rules and the values of each MF are based various tests and on the instructions of expert knowledge [5]. Table 1 illustrates the values of each membership function.

Table 1 MFs of the input and output functions

Input variable	Fuzzy value/MF	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	20	30
	Medium	25	35	45	55
	High	50	60	100	102
RSSI	Low	− 0.5	0	5	10
	Medium	5	10	15	20
	High	15	20	100	102

4.2 Fuzzy Inference System

The fuzzy inference is the second step in the FL. To define the set of rules, we are using the Comb method to avoid combinatorial explosion [14]. In our case, there are three (3) linguistic variables with three (3) possible levels (high, medium and low), so to calculate the rules basing on the traditional fuzzy system, we have as a result 27 rules (3 to the power of 3), whereas, we can reduce this number to 9 rules (3 * 3) due to the Comb method. In our case, we selected the logical nine fuzzy rules logical, because there are some rules and results are unlikely to occur in a real situation.

Furthermore, it is not necessary to add all the possibilities, and we used 9 fuzzy rules as given below, in the fuzzy inference system basing on how jamming affects the network parameters in order to identify the degree of JDI. In fact, we eliminate some rules that do not have a value added to the system. For instance, in case the PDR is high (Rule 1), we can conclude that there is no jamming whatever the value of RSSI and ECA. In addition, if the RSSI is low (Rule 2), it means that the medical node is not jammed, whatever the value of PDR and ECA. The set of fuzzy rules is given as follows:

1. If PDR is high, then JDI is very low;
2. If RSSI is low, then JDI is low;
3. If PDR is low, RSSI is medium, and ECA is low, then JDI is medium;
4. If PDR is low, RSSI is high, and ECA is high, JDI is high;

The relationships obtained from the rule base are interpreted using the minimum operator “AND”. The surface plot corresponding to membership functions of PDR and RSSI variables is given in Fig. 5.

The node with linguistic values low PDR, high RSSI and high energy has the highest probability to be attacked by the jamming attack, and the node with high PDR, low RSSI and low energy has the lowest probability to be under jammer node.

4.3 Test and Simulation Results

According the communication architecture of the WBAN, our work is focused on the first-level "inter-BAN communication". The values of three crisp inputs PDR, RSSI and ECA are generated through OMNET++ as network simulator using Castalia platform, which is useful for the WBAN. Indeed, we have simulated the WBAN in normal and abnormal cases for collecting the parameters values. In the normal scenario, we have simulated the WBAN with three medical nodes and coordinator node using the ZigBee as MAC protocol. While for studding the impacts of jamming attack, we used also the BypassMac that does not respect the MAC protocol mechanism, in order to simulate a jammer node as shown in Fig. 1.

After the different simulation, the parameters values of each node are studied in our proposed mechanism that was built in MATLAB. Due to the Fuzzy Logic Toolbox

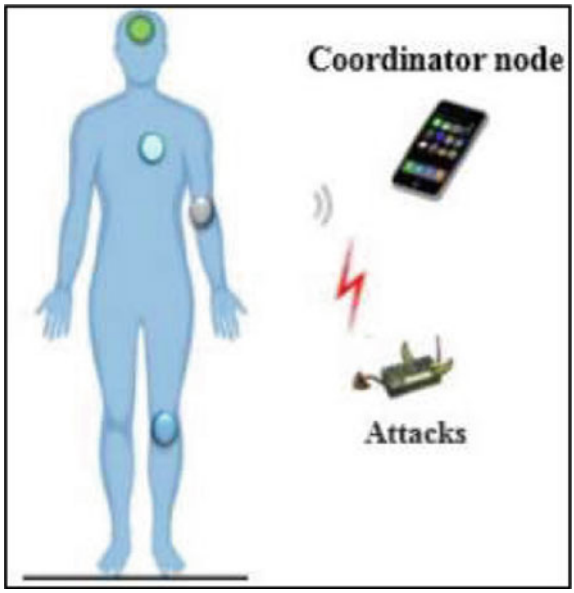

Fig. 1 Communication between medical nodes and PDA under jamming attack [2]

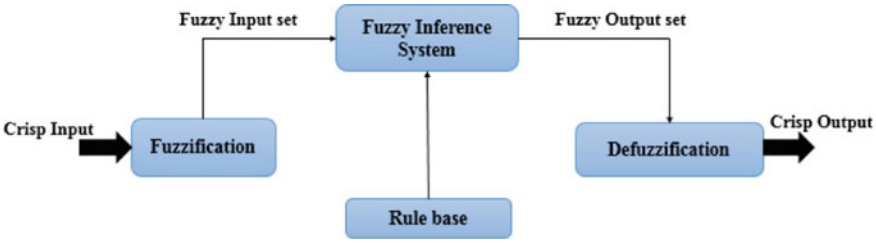

Fig. 2 General fuzzy system architecture

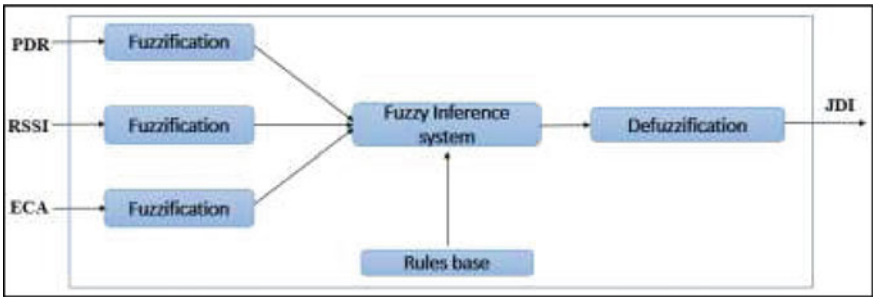

Fig. 3 FLS of our proposed system

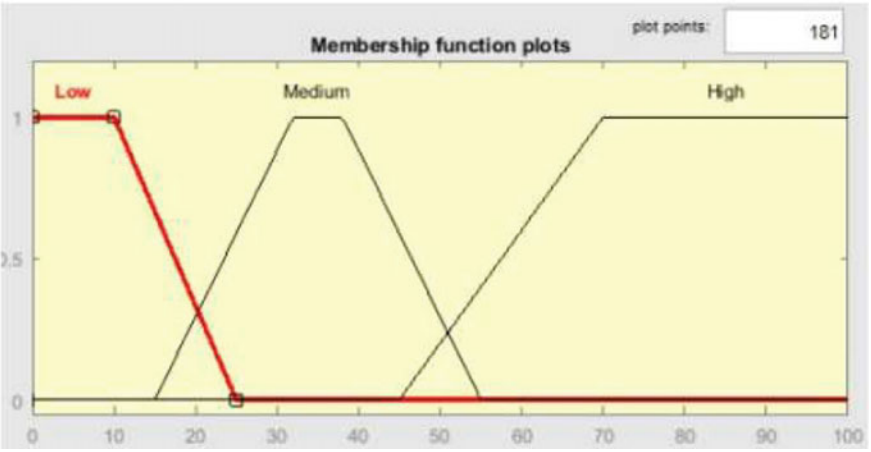

Fig. 4 Membership functions for the input PDR

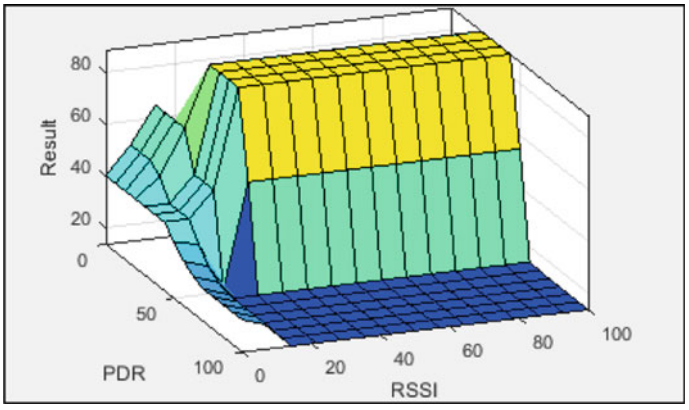

Fig. 5 Surface plots of PDR and RSSI

Table 2 Evaluated the traffic network using our proposed system

Inputs			Outputs		
PDR	RSSI	ECA	JDI value	JDI level	Decision
29.34	85	76	88.4763	High	Jammed: high-power jamming
11.438	65	57	65	High	Jammed
4.618	82	73	79.8829	High	Jammed
54.21	12.73	10	40	Low	Not jammed: possible collision case
90.033	22	5	40	Low	Not jammed
79.33	44.21	32	40	Low	Not jammed

of MATLAB, we defined the MF using the graphical interface. This Toolbox aims also to complete the fuzzification of the input variables and the fuzzy operator as AND or OR to define the rules base. According to the combination of the different input values RSSI, ECA and PDR, our system is able to control the communication system and indicates the level of Jamming Detection Index, as shown in Table 2. If the output has high as result, it means that the medical node is under jamming.

5 Conclusion

Jamming attacks are among attacks of DoS attacks. The goal of these attacks is to destroy the communication of the network by transmitting a successive signal. In this paper, we developed a new intrusion detection system that aims to control the network traffic, for detecting jamming attacks in WBAN system. Indeed, we have integrated the fuzzy logic approach into our IDS to take the good decisions with high detection attack and low false alert. The system is evaluated by using different scenarios simulated in Castalia. In our future research, we aim to implement our proposed system in coordinator node used as CH in order to calculate the parameters values of each medical sensors (cluster member).

References

1. Bengag A, Bengag A, Moussaoui O (2021) Effective and robust detection of jamming attacks for WBAN-based healthcare monitoring systems. In: Lecture notes in electrical engineering, vol 681, pp 169–174
2. Bengag A, Bengag A, Moussaoui O (2020) Attacks classification and a novel IDS for detecting jamming attack in WBAN. Adv Sci Technol Eng Syst 5(2):80–86
3. Bengag A, Bengag A, Moussaoui O (2021) Classification of security attacks in WBAN for medical healthcare. NISS 21:1–5
4. Bengag A, Moussaoui O, Moussaoui M (2019) A new IDS for detecting jamming attacks in WBAN. In: 2019 Third international conference on intelligent computing in data sciences (ICDS), pp 1–5

5. Almseidin M, Kovacs S (2018) Intrusion detection mechanism using fuzzy rule interpolation. J Theor Appl Inf Technol 96(16):5473–5488
6. Kanagasabapathy PMK (2019) Rapid jamming detection approach based on fuzzy in WSN. 1–14
7. 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(10):1–21
8. Vijayakumar KP, Pradeep Mohan Kumar K, Kottilingam K, Karthick T, Vijayakumar P, Ganeshkumar P (2019) An adaptive neuro-fuzzy logic based jamming detection system in WSN. Soft Comput 23(8):2655–2667
9. Reyes HI, Kaabouch N (2013) Jamming and lost link detection in wireless networks with fuzzy logic. Int J Sci Eng Res 4(2):1–7
10. Angrishi K et al (2013) Fuzzy based detection and prediction of DDoS attacks in IEEE 802.15.4 low rate wireless personal area network. IEEE Netw 24(2):943–983
11. Chaudhary A, Tiwari VN, Kumar A (2014) Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks. In: Souvenir of the 2014 IEEE international advance computing conference (IACC), pp 256–261
12. Hiremath PS, Anuradha T, Pattan P (2017) Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs. In: Proceedings—2016 international conference on information science (ICIS), pp 245–251
13. Çakiroğlu M, Öozcerit AT (2011) Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks. Turk J Electr Eng Comput Sci 19(1):1–19
14. Combs WE, Andrews JE (1998) Combinatorial rule explosion eliminated by a fuzzy rule configuration. IEEE Trans Fuzzy Syst 6(1):1–11