Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 2, 80-86 (2020)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Attacks Classification and a Novel IDS for Detecting Jamming Attack in WBAN

Asmae Bengag*, Amina Bengag, Omar Moussaoui

Applied Mathematics, Signal Processing and Computer Science Laboratory, ESTO, University Mohamed 1er Oujda, Morocco

ARTICLE INFO

Article history:
Received: 01 January, 2020
Accepted: 16 February, 2020
Online: 09 March, 2020

Keywords:
WBAN
Medical Sensors
Jamming attack
IDS
Parameters Network
ZigBee
OMNET++
Castalia 3

ABSTRACT

Wireless Body Area Network (WBAN) aims to monitor patient's health remotely, by using mini medical sensors that are attached on the human body to collect important data via the wireless network. However, this type of communication is very vulnerable to various types of attacks, poses serious problems to the individual's life who wears the nodes. In this paper, we present a new classification of the most dangerous attacks based on different criteria, which gives us a clear vision of how attacks affect a WBAN system. Moreover, this classification will help us to specify the strength and the weakness of each attack in order to facilitate the development of a new intrusion detection system (IDS). In the second part of this work, we develop a novel IDS for detecting three types of jamming attacks in WBAN. The proposed methodology is based on the network parameters as an indicator to differentiate the normal case from the abnormal case like false alert or attack state. Through simulation analysis that was applied on Castalia platform by using OMNET++ as a simulator, proves that the proposed IDS have a great effect for detecting the presence of jamming attack in the network.

1. Introduction

In the last two decades, wireless body area network (WBAN) has attracted huge number of researchers. WBAN is a network consisted of several types of medical sensors; each one has its own debit and functionality. These sensors facilitate the supervision of the patient's health and intervene as quickly as possible in emergencies.

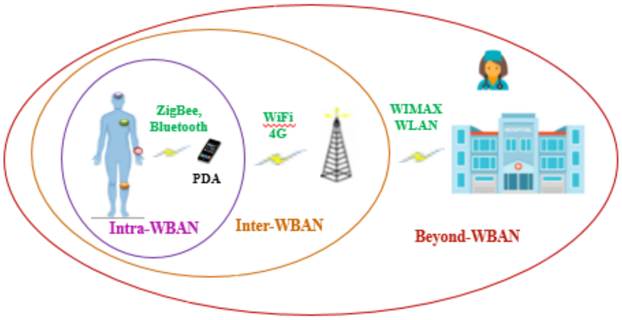


Figure 1 : Communication architecture of WBAN

The medical sensors are attached on the human body for collecting the biomedical parameters as the activity of muscles, brain or heart rate. Then, this information will be transmitted to the personal device assistant (PDA). Finally, the data will be received by the medical team via a wireless mode, as shown in Figure 1.

Actually, the communication is done by three levels [1]:

- Level 1: 'Intra-WBAN communication' that contains different devices especially medical sensors and the coordinator node or PDA. The communication between these nodes could be based on Bluetooth (802.15.1) or ZigBee (802.15.4). In fact, the main goal of PDA is to ensure a communication between sensors, and informs the final user as doctor or patient via an external gateway [2].

- Level 2: is named an 'Inter WBAN communication' that concerns a communication between the PDA and one or more access points (APs) via WiFi, to interconnect WBAN network with several networks [3].

- Level 3: called a 'Beyond-WBAN communication' in which the communication is between a various access points and medical server (hospital, nurse etc.) using for instance Internet or mobile networks.

However, the communication used in WBAN system is not reliable one hundred percent, because the wireless communication deployed on open radio frequencies with various attacks and different cases of anomalies. Furthermore, several attacks threat

[*] Asmae Bengag, asmaebengag@gmail.com

https://dx.doi.org/10.25046/aj050210

the security aspects like availability, which makes the medical nodes not able to send or transmit any information especially in the case of emergency. Besides, other attacks affect the integrity that can modify the data transmitted during the transmission and other ones threat the confidentiality aspect that could access sensitive data [4].

One of the most important challenges to secure the WBAN system is by using a robust mechanism to detect an attack in this kind of networks. Hence, we started our work by studying the impact of the most dangerous attacks in WBAN, by classifying them according to various criteria. Then, we focused on the Denial of Service (DoS) jamming attack that disturbs wireless communication by affecting the physical and MAC layers. In fact, we are developed a new IDS technique to detect jamming attacks that based on four important network parameters: packet delivery ratio (PDR), energy consumption amount (ECA), received signal strength indication (RSSI) and bad packet ratio (BPR).

The rest of this paper is organized as follows: in section II, we describe the previous different classification attacks works, and the various IDS mechanisms for detecting jamming on the network. Then in section III, we present our attacks classification in WBAN according to various measures. The steps of our IDS algorithm, the simulations scenarios and the results are discussed in section IV. Finally, our work is concluded in section V.

2. Related Work

In order to propose a new classification of attacks in WBAN, we are based on several previous works. In fact, each work is based on different measures and applied on specific technology such as MANET, WSN or WBAN.

In [5] authors proposed a classification attacks that applied in MANETs and based on six attributes: legitimacy of attacking node(external or internal node), the number of nodes participating as an attacker (singleton or collision attack), MANETs vulnerabilities utilized by the attack, the network resources exploited by the attacking node/s, the targeted victim and compromised security service of attack.

Another taxonomy proposed by Wu et al. in [6] that is applied in network and computer, which based on three dimensions: (i) the source of attack (local or remote); (ii) the techniques dimension that mean the all-possible techniques adopted by the attackers; and (iii) the results of attack. However, the weakness of this work is the less information about the type of target.

In [7], the authors present various attacks get into IEEE 802.15.4 and classifying them into three categories: (i) the radio jamming that is an attack created the problems of denial of service in the physical layer; (ii) the message manipulation attacks for injecting false information into the node network; and (iii) the last one is the steganography attacks. However, the weakness of this classification is the lack of other important measures as security aspects and position of attack in the network that will be presented in our classification.

In [8] authors classified attacks according MAC Layer basing on the functionality of the mac layer. They are presented two classification, the first one concerns the MAC layer as Guaranteed Time Slot (GTS) attack, and the second one based on MAC layer protocol rules.

The OSI model is important measure to identify problems of security in each layer; this work is proposed by Pooja et al. [9] and applied in MANET. Nonetheless, this classification is based on just one criterion and it is not enough to have a robust security solution.

All the above-mentioned classification has some limits that make them inappropriate to specify all types of attacks because they not consider some important metrics. Basically, in our classification, we are based on the important and clear metrics especially in WBAN as attack position basing on the communication architecture of WBAN and the attack functionality.

In this second part, we give an overview about the detection mechanisms that have been studied to detect jamming attack in a wireless network.

Fuzzy Inference System (FIS) is a technique proposed by Reyes et al. [4] that built in Matlab tool using the following metrics as input values: CCA, BPR, RSS and PDR. In order, detecting the link loss in wireless networks, these parameters will be used to calculate the values of the Jamming index (JI). The idea of this method is good, but it has a complicated calculation that makes sensor nodes consume more energy. In addition, it does not differentiate the types of jamming present in the network.

In [10] proposed a technique for identifying the following jamming types: constant, random, reactive and deceiving. The methodology is based on SS (Signal Strength) and PDR (Packet Delivery Ratio), to determine the normal cases from the jamming attack cases. However, the method could consider that the sensor is under a jamming attack but there is no attack in the network. For instance, in the case where the receptor sensor has a problem to respond with an ACK packet to the transmitter, we found that the transmitter node has a high SS level, and the PDR value is low. Hence, there is confusion between jamming scenario and affected node.

In [11], the author improved an IDS that includes Signal Strength (SS) and Packet Delivery Rate (PDR) to define the presence of jamming attack. On the other hand, they are used also Packet Send Rate (PSR), to distinguish different types of jamming attacks in WSN.

In [12] proposed jamming detection technique for WSN that called physical layer jamming identification using PDR and RSSI parameter. This method used only some nodes as monitor in the network that have residual energy. Nevertheless, for monitoring the entire network, the method needs to implement various monitor nodes.

By comparing our proposed methodology with the previous works, we are focused on four important network parameters PDR, ECA, RSSI and ECA that will be presented in the section 4. By using these parameters based on a simple technique that consume a less energy compared to the above-mentioned techniques. Moreover, these parameters have a good effect to differentiate the normal case and false alerts for the jamming attacks. Our intrusion detection system allows also us to identify three types of jamming attacks (constant jamming, reactive jamming and deceptive jamming) that are applied in the WBAN system.

3. Classification of attacks in WBAN

In this section, we describe our classification that based on previous attack taxonomies and other metrics, which adopt in wireless body area networks. Our taxonomy is based on six important criteria as follow:

- Attack impacts: are the results or the effects of attack action in the network.

- Security aspects: for having a robust system, we must take into consideration the fundamental security requirements in the medical application [13], such as data integrity, availability, data confidentiality, data freshness and authentication.

- OSI model: we can also classify attacks by the layers of the OSI model.

- Communication architecture of the WBAN: attack could place in different levels of the architecture of WBAN, either in the first level that directly threatens the medical sensors, level 2 or level 3 as exposed in the Table 1.

- Attack position in the network: we can distinguish two types of attack position, as internal attack that is a part of the network action, or as an external attack that is not a part of the system [5], like sniffing and man in the middle.

- Interruption act: the attack could be active by modifying or damaging the transmitted message to the receiver, and disrupting the communication [9]. Further, the passive attack threats the confidentiality aspect by collecting the data in the network without perturbing the communication [5].

Thus, the Table 1 presents the different attacks classified according to our taxonomy that are cited above.

This attack classification facilitates us to understand and identify the operation or strategy of each attack in the network. Furthermore, it helps us to find a robust mechanism to detect jamming attack in WBAN that will present in the next section.

4. A novel detecting jamming attack

Jamming attack is among one of the attacks that blocks and disrupts the communication between nodes, by sending illegitimate signals, in order to make the system unavailable. In other words, this attack generates interference, which makes the medical sensors consume a lot of energy, and involves the collision between them [14].

As we present in the previous section, jamming attack threats the physical layer that transmit a signal to create interference. Besides, data link layer could be under jammer node that does not respect the mechanism of its MAC protocol.

Table 1 Attacks classification in WBAN system

Attacks	Attack impacts	Security aspects	OSI model	Communication architecture of the WBAN	Attack position in the network	Interruption act
Tampering	Extracting cryptographic keys from the captured node [15]	Confidentiality Integrity data	Physical	Intra-WBAN	External	Active
Jamming	Disruption of communication by sending radio waves at a same frequency in the wireless network.	Availability	Physical Data Link	Intra and Inter WBAN	External	Active
Sybil	Obstruct the operation of routing protocols by operating multiple fake identities.	Confidentiality Integrity data	Network Data link	Intra, Inter and Beyond WBAN	Internal / External	Active
Hello floods	Blocking communication by sending broadcasts HELLO packets with high transmission.	Availability Confidentiality	Network	Inter and Beyond WBAN	External	Active
Selective forwarding	Delete some packets and refuse the transmission of data.	Availability, Confidentiality	Network	Inter and Beyond WBAN	External	Active
Flooding	Exhaust the energy of sensor and saturate the network.	Availability	Network Transport	Inter and Beyond WBAN	External	Active

4.1. Proposed methodology

In this section, we present our proposed methodology for identifying and detecting the presence of jamming attacks in WBAN system.

Our proposed algorithm has the ability to detect the presence of a jamming attack, and then identify which type it is. In fact, there are many types of jamming attack, but in our work, we mainly focus on three of them, constant jamming, deceptive jamming and reactive jamming.

Indeed, there are a lot of cases that resemble as jamming attack in the network namely false alerts, for example problems caused by a low energy or collision in the nodes, which reduce the quality of the IDS. In order, to have good IDS defending a malicious activities jamming in WBAN system, we are based on four important network parameters as a performance metrics that are mentioned in Table *2*.

Table 2 : The network settings used

Parameters	Definition
PDR (Packet Delivery Ratio)	The authors of [10][16] defined the PDR as the ratio of the packets successfully sent by the node, to the total sent packets.
ECA (Energy Consumption Amount)	Amount of energy consumed in a specified time [4].
BPR (Bad Packet Ratio)	BPR is a ratio of the failed packets received by a node [16].
RSSI (Received Signal Strength Indication)	RSSI is defined as a power content of the received radio signal at the receiver [4].

The diagram in Figure 3 shows the essential algorithm steps of the proposed IDS, which describes how our mechanism defend the remaining or not of jamming, and differentiate which types are on WBAN. As first step, we assume that the WBAN system is operating normally, without jamming attack or any problems. Then, each receiver sensors medical are calculated the thresholds of the network parameters PDRth, ECAth, BPRth and RSSIth. After that, for observing if there are any problems on the WBAN, the initial parameters (PDRth, ECAth, BPRth and RSSIth) are compared with the current values.

For mentioning the presence of jammer node and specify its type, one of the conditions will be launched an alert, and we can conclude that the node is under jamming attack. For the constant jamming, could be generated interferences between nodes sensors, by sending continually a random bits or signals in the wireless network [4], and forces the legitimate nodes to stay in listening mode, which cause a higher energy consumption. That is why the PDR and BPR values are lower than the normal case, and the ECA and RSSI parameters are higher.

In the case where the legitimate node is under the deceptive jamming, the latter sends data regularly to the channel that resembles legal, in order to deceive each node. Hence, we could be found that the PDR value is lower than the PDRth, and for the BPR, RSSI and ECA values are higher than their thresholds.

Furthermore, to identify a reactive radio jammer when the legitimate node sends the packet RTS, then the attack starts to transmit data and makes the communication medium busy. Thence, the legitimate node will consume a modest rate of energy. However, the value of the PDR input parameter very lower, whereas the BPR and RSSI values are higher than the normal values and the packet delivery ratio is very lower.

4.2. Simulation and results

4.2.1. Simulation parameters

We have made two main scenarios, in the first one we are simulated a WBAN system in normal case without malicious node, the studied scenario covers three types of medical sensors (EMG, ECG and EEG) are attached on human body. More specifically, the wireless communication protocol used between legitimate sensors and PDA is ZigBee (802.15.4 MAC), and CC2420 Radio used as a radio model as shown in Figure 2.

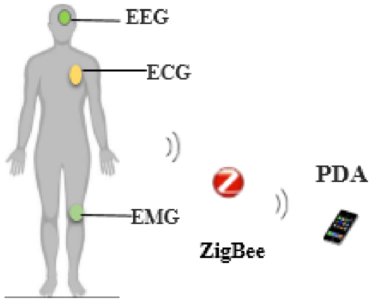


Figure 2: Simulation of WBAN in normal case

Simulation parameters, used in this case, are listed in Table 3.

Table 3 : Simulation parameters for WBAN without jamming

Used parameters	Values
Nodes	4 (3 medical sensors and 1 PDA)
Simulation time	300s (second)
MAC protocol type	ZigBee (Basic802154)
End simulation	End of the simulation

After that, we are simulated a WBAN system under a jammer node, as shown in Figure 4, in order to understand the impacts of jamming attack in the WBAN system and specially the MAC layer and the network parameters to compare with the normal case.

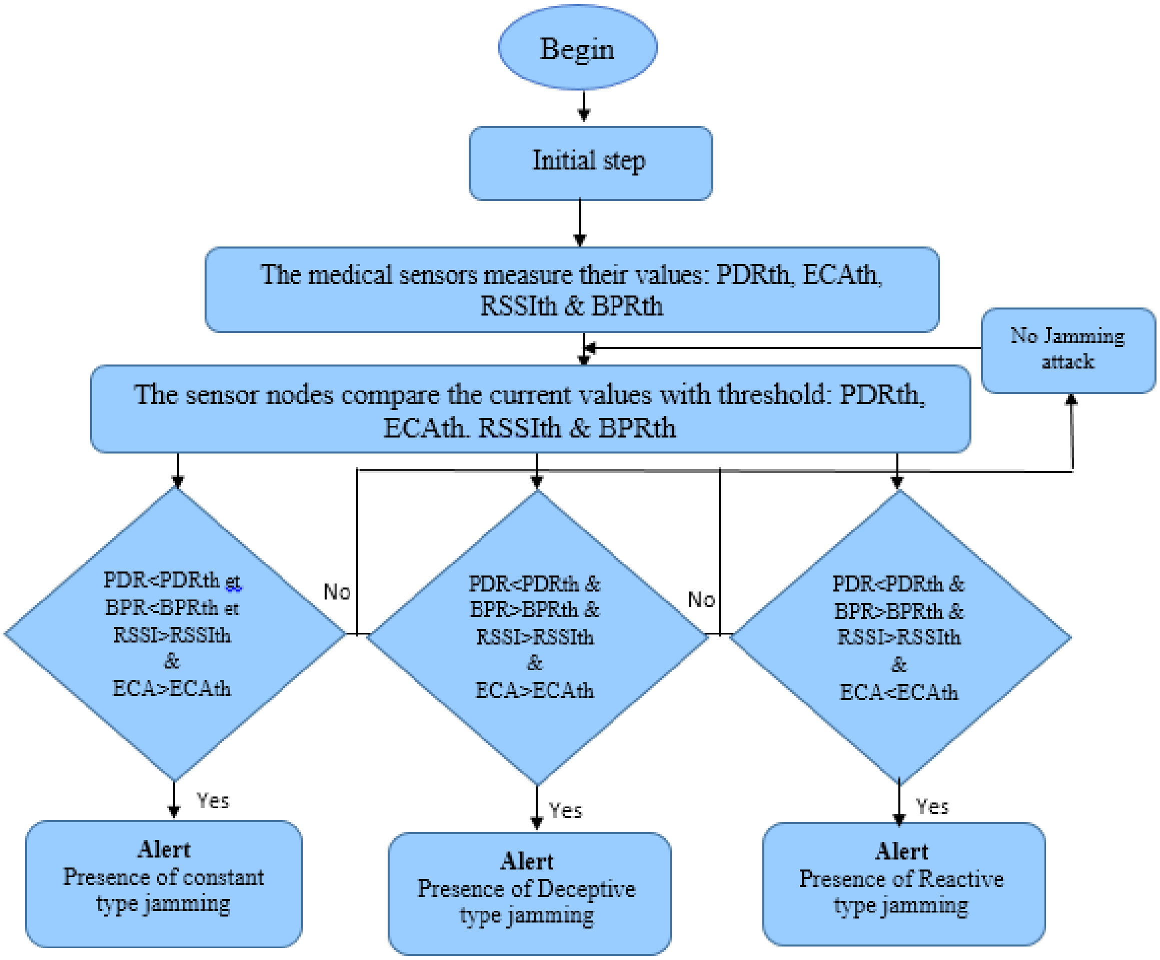

Begin
Initial step
The medical sensors measure their values: PDRth, ECAth, RSSIth & BPRth
No Jamming attack
The sensor nodes compare the current values with threshold: PDRth, ECAth. RSSIth & BPRth
PDR<PDRth et BPR<BPRth et RSSI>RSSIth & ECA>ECAth
No
PDR<PDRth & BPR>BPRth & RSSI>RSSIth & ECA>ECAth
No
PDR<PDRth & BPR>BPRth & RSSI>RSSIth & ECA<ECAth
Yes
Yes
Yes
Alert Presence of constant type jamming
Alert Presence of Deceptive type jamming
Alert Presence of Reactive type jamming

Figure 3 : Proposed mechanism for detecting different types of jamming attacks

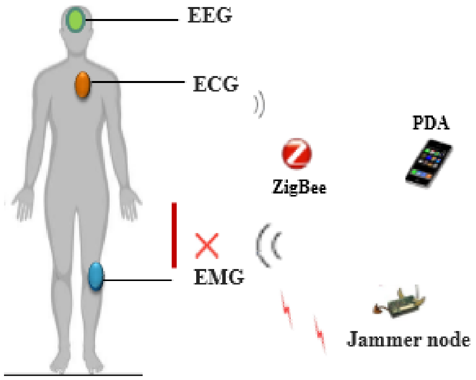


Figure 4: The scenario of WBAN with jamming attack

As mentioned in Table 4, we are chosen the BypassMAC as MAC protocol for the jammer node, because as we explained before the jamming attack interrupts the communication between the nodes, and makes them not able to access the channel, by perturbing the MAC protocol mechanism.

4.2.1. *Simulation results and discussion*

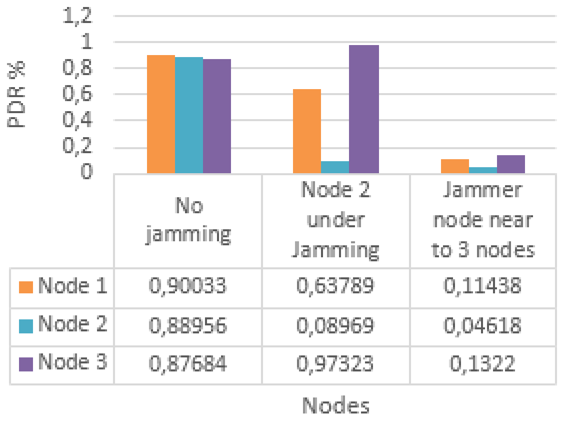
In this section, we measure the performance of our proposed approach jamming detection in WBAN, by calculating the network parameters in both cases without and with jammer node.

Table 4: Simulation parameters for jammer node

Used parameters	Values
Number of jammer nodes	1
Simulation time	300s (second)
MAC protocol	BypassMAC
Constant Data Payload	2000
End simulation	End of the simulation

As shown in Figure 5 and Figure 6, when the legitimate node is under Jamming, the PDR value is very lower than the normal case, and the signal indicator is higher (-63,43 dBm). Moreover, in the normal case, the PDR parameter is higher and the RSSI is lower (-90 dBm). When the node (1) is near to the node (2) who is under jamming, we found that the node (1) could be also affected by the attack.

When the medical sensor (node 1) is under jamming, it consumes a lot of energy comparing with normal case (ECAth) as shown in the Figure 7.



	No jamming	Node 2 under Jamming	Jammer node near to 3 nodes
🟧 Node 1	0,90033	0,63789	0,11438
🟦 Node 2	0,88956	0,08969	0,04618
🟪 Node 3	0,87684	0,97323	0,1322

Figure 5: Packet delivery ratio values per node in WBAN (with and without jamming)

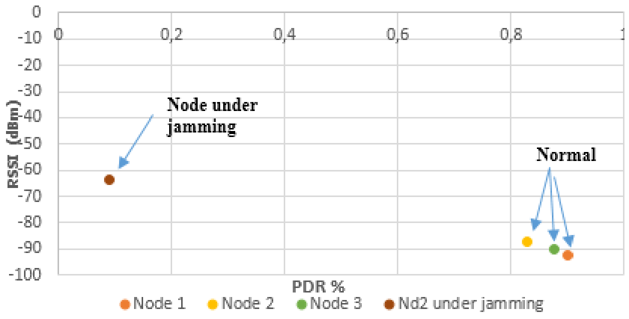
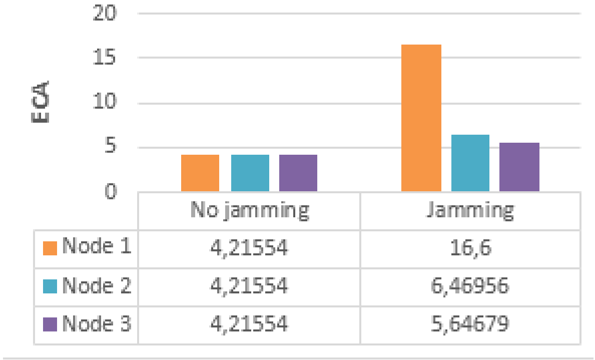


Figure 6: RSSI and PDR values in WBAN



	No jamming	Jamming
🟧 Node 1	4,21554	16,6
🟦 Node 2	4,21554	6,46956
🟪 Node 3	4,21554	5,64679

Figure 7: ECA parameter values in WBAN

Therefore, we can notice from these results that the used network parameters PDR, ECA, BPR and RSSI are very useful and have a great effect for identifying the presence of jamming attack in the WBAN system.

5. Conclusion and future work

In the recent years, many studies are interested to ameliorate and secure the healthcare industry. This paper is divided into two main parts. The first one presents our new classification of attacks in WBAN. The second one concerns a new IDS to detect three types of jamming attacks.

Thanks to our classification based on various measures, the researchers could have a deep view that helps them to understand the different attacks in order to propose a robust solution security for defending attacks in the WBAN system.

Our novel Jamming Intrusion Detection System was implemented on the medical sensors, which is based on four fundamental network parameters: PDR, RSSI, ECA and BPR. Indeed, by using a simple technique, based on these parameters, the jamming attack could identify three types of jamming as constant, deceptive and reactive. Furthermore, our mechanism detects these attacks without consuming a lot of energy. However, according to the best of our knowledge, the most of proposed techniques have some limits as consuming a lot of energy because of complex calculation techniques, detecting false alerts due to a less of parameters, and other IDS do not specify types of jamming. Our simulation carried out in two main scenarios, the first one is with jamming and the second one is without jamming, which is done with the popular WBAN's simulator tools OMNET++ and Castalia. According to the results of simulation, our method proves that the used parameters have good effects to detect the presence of jamming with less false alerts.

For future works, we aim to improve our proposed IDS by using Fuzzy Logic to make our mechanism more robust in order to increase detection and decrease the false alerts.

Acknowledgment

This research is performed inside the MATSI Lab., ESTO, University Mohammed First, Oujda (Morocco).

References

[1] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu, "A survey of routing protocols in WBAN for healthcare applications," *Sensors (Switzerland)*, vol. 19, no. 7, 2019.

[2] H. Fouad, "Continuous Health-monitoring for early Detection of Patient by Web Telemedicine System," pp. 76–83, 2001.

[3] S. Movassaghi, A. Mehran, J. Lipman, D. Smith, and A. Jamalipour, "Wireless Body Area Networks: A Survey," *IEEE Commun. Surv. TUTORIALS*, vol. 16, pp. 1658–1686, 2014.

[4] H. I. Reyes and N. Kaabouch, "Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic," *Int. J. Sci. Eng. Res.*, vol. 4, no. 2, pp. 1–7, 2013.

[5] N. A. Noureldien, "A novel taxonomy of MANET attacks," *Proc. 2015 Int. Conf. Electr. Inf. Technol. ICEIT 2015*, pp. 109–113, 2015.

[6] Z. Wu, Y. Ou, and Y. Liu, "A taxonomy of network and computer attacks based on responses," *Proc. - 2011 Int. Conf. Inf. Technol. Comput. Eng. Manag. Sci. ICM 2011*, vol. 1, pp. 26–29, 2011.

[7] Y. M. Amin, A. T. Abdel-hamid, and S. Member, "Classification and analysis of IEEE 802.15.4 PHY layer attacks," *2016 Int. Conf. Sel. Top. Mob. Wirel. Netw.*, pp. 74–79, 2016.

[8] Y. M. Amin, A. T. Abdel-hamid, and S. Member, "Classification and Analysis of IEEE 802.15.4 MAC Layer Attacks," pp. 74–79, 2016.

[9] P. Chahal, "Comparative Analysis of Various Attacks on MANET," vol. 111, no. 12, pp. 42–46, 2015.

[10] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," p. 46, 2005.

[11] B. Yu and L. Y. Zhang, "An improved detection method for different types of jamming attacks in wireless networks," *2014 2nd Int. Conf. Syst. Informatics, ICSAI 2014*, no. Icsai, pp. 553–558, 2015.

[12] V. C. Manju and K. M. Sasi, "Detection of jamming style DoS attack in Wireless Sensor Network," *Proc. 2012 2nd IEEE Int. Conf. Parallel, Distrib. Grid Comput. PDGC 2012*, pp. 563–567, 2012.

[13] M. Messai, "Classification of Attacks in Wireless Sensor Networks," *Icta*, no. April 2014, pp. 23–24, 2014.

[14] C. Del-Valle-Soto, L. J. Valdivia, and J. C. Rosas-Caro, "Novel detection methods for securing wireless sensor network performance under intrusion jamming," *CONIELECOMP 2019 - 2019 Int. Conf. Electron. Commun. Comput.*, pp. 1–8, 2019.

[15] B. Kiruthika, S. Abinaya, R. Ezhilarasie, and A. Umamakeswari, "Security

attacks and its countermeasures in wireless sensor networks - A survey," *Res. J. Pharm. Biol. Chem. Sci.*, vol. 6, no. 3, pp. 1374–1387, 2015.

[16] M. Çakiroğlu and A. T. Öozcerit, "Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 19, no. 1, pp. 1–19, 2011.