Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Handling missing data in WBAN using Layer Recurrent Neural Network

P. Madhuri Paul[1], Dr Prasadu Peddi[2]

[1]*Research Scholar, Dept of computer science, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan.*
[2]*Assistant Professor, Dept of computer science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University*
Email: madhuripaul.2020@gmail.com

The Internet of Healthcare Things (IoHT) is growing in popularity today and among the key technologies used for providing better healthcare services includes wireless body area network (WBAN). WBANs comprise small devices with the capacity to significantly improve the quality of life for patients by capturing and analyzing the patient's physiological information and then sending the information to healthcare professionals so that they can evaluate a degree of criticality in a patient and then take the appropriate action. To help medical staff make accurate and timely judgements, the data gathered must be trustworthy, accurate, and representative of the actual world. By identifying dangerous data patterns that arise from a variety of causes, including sensor malfunctions, incorrect readings, and potentially malicious behaviours, The detection of anomalies is therefore the subject of discussion for ensuring the validity of the data collected. Numerous anomaly detection strategies have been suggested to be used in WBAN. But, current methods of detection, which are predominantly based on methods of machine learning and statistics but are ineffective due to large data streams and distinct pattern patterns that are context-specific within WBAN. A RNN was designed with a single variable, set to one mode in each training run. A type that RNN cell that works very well in the resource constrained settings on mobile devices is the gated Recurrent Unit (GRU) cell. The RNNs that learn from the variable may perform well with no further training even when the surrounding environment of the device used by the user alters. Missing values may result from a variety of faults in a heterogeneous environment, such as errors brought on by sensor failure, equipment exchange, battery charge and discharge problems, and near-field communication issues. The amount of mistakes that are likely to occur increases with the missing value ratio. This paper suggested a model using correlations derived from the diverse physiological data attributes and the ability of hybrid Convolutional Long-Short-Term Memory (ConvLSTM) methods to identify simple point anomalies as well as specific anomalies that are influenced by context in the huge streaming of data from WBAN. In contrast to the 64% accuracy obtained by CNN and LSTM separately, experimental evaluations revealed that the proposed model reported a median of 98% F1-measure and 99% accuracy on different themes of the datasets.

1. Introduction

WBANs are a particular kind of wireless sensor network utilised in the biomedical and health fields. They have gotten increased consideration in recent years from the government, industry, and academia. The two sensors are more advanced and costly, and is accessible in

WBAN. Numerous experiments have been done to increase the durability and energy effectiveness of WBANs.

By employing predicting values rather than real sensor values, data prediction (DP) is a highly effective approach to decrease the data transfers between the sensor and the base station (BS) without sacrificing the quality of the information to be provided. reduces the volume of data transfers from sensor nodes to the BS. One of the primary issues is the predictive accuracy of the forecast within an error range. Numerous forecasting methods provide accurate or context-appropriate predictions about upcoming sensor data. The base station generally employs the prediction model to recommend an alternative data transfer method which decreases the quantity of data sent into the drain. The model is low in processing cost and a quick recall path and it is dependable and effective as compared to other techniques of this kind. The technique permits the body's sensors to collect data about temperatures and pulse rates so that it can determine the appropriate energy level by decreasing the transmission.

Generally speaking, data transmission (DT) uses more energy than data processing and value sensing. One piece of data may be sent hundreds to thousands of times with the same amount of energy. Given this reality, using data-driven methods may lead to more energy sharing. Since the computational power of wireless sensors is constantly constrained, this issue may be particularly severe for physical sensors.

1.1 Wireless Body Area Network

To gather biological data, a patient's or person's body is implanted with a wireless sensor. When constructing a WBAN, traditional WSN concerns—such as figuring out the network's geography and how data from biosensors might sink—are paired with particular difficulties brought on by the sensors' location within the human body. It is a collection of connected wireless sensor nodes that may be placed within or outside the body to track both internal and exterior physiological processes. It is a tailored WSN that is supposed to function autonomously in order to link different medical bio-sensors and tiny devices that are found within the human body. WBAN technology connects with the internet and a variety of wireless technologies, including cellular networks, Bluetooth, ZigBee, WSNs, Wireless Personal Area Network (WPAN), and WSNs. WBAN sensors can model, monitor, analyse, and convey a variety of important symptoms while offering users and medical personnel practical real-time feedback. WBAN may be utilised to continuously track the patient's physiological characteristics, giving patients more mobility and adaptability.

In analogue mode, the sensor picks up environmental characteristics and uses an analogue to digital converter to turn the analogue data it gathers into digital data. The transformed digital data is processed by the processing unit, which then sends in the WSN environment. The internal behaviour of nodes is altered by an external attacker or hacker, and these malignant and evasive nodes. The effectiveness of current WSN networks [10,11] is negatively impacted by the quantity of malevolent or covert nodes. As a consequence, the method for locating thesis nodes in WSNs that is described in this article and that may be utilised to boost speed is quite efficient.

2. Literature Survey

The use of wireless body area networks (WBAN) for medical applications allows for low-cost, undetectable, and ongoing real-time monitoring. The security of vital data must be controlled by wearable, implantable, and mobile devices, which is a key component of WBAN. The study puts forward a wireless body area network security-focused autonomous mobile agent-based intrusion detection system. The distinct advantages of the proposed architecture were underlined [3] as they were contrasted with mobile agent-based IDS suggested in other domains using WBAN systems.

The study advises using Body Area Sensor Networks (BASNs) to solve universal healthcare issues while mentioning the financial issues with healthcare. However, these networks must be made very safe and dependable if they are to be used correctly. In order to maintain security, they provide a trust-based aware model and an entropy-based credibility assessment model that give testimony (based on historical data) about neighbours. A node's reputation is generated from its trustworthiness value, which is determined from the entire network's aggregated trust pieces of evidence. Apparently, this technique is workable [9]. In this article, we examine two key elements that are crucial for protected data in WBAN, starting with distributed and fine-grained data storage [10].

One of the numerous new developments in the world of medicine at the moment is Wireless Body Area Network, or WBAN. Despite the difficulties in overcoming security challenges for WSNs (Wireless Sensor Networks). In order to satisfy the security needs of WBANs with stringent resource limits, we need to develop a workable hybrid security solution. These processes allow for the analysis of features and the identification of the primary hazards associated with WBANs. Based on these risks, the security needs of WBANs are then outlined and examined using the available cryptographic algorithms. With frequent updates and enhancements, the suggested mechanism will continue to be useful and helpful even in the future [11] and offers basic developed, efficient, and safe WBAN systems while also having a good trade-off between security and resource restrictions.

3. Sensor Network Model

3.1 The sensor network is predicated on the following premises:

(a) Because the sensor nodes on the network are immobile, they are referred to as static sensors. can still identify their own position even if they are installed physically or distributed by aerial means. If not, the nodes could end up in their own position via the placement procedure. Furthermore, after being deployed in the field.

b) The sensor nodes can be compared with the current sensors, for instance, in terms of Berkeley MICA motes' computing, communication, and power capabilities. To provide symmetrical data transport cryptography.

c) As a laptop-class device, the base station, also called the access point, is a device which functions as a controller as well as key server, and has to have a long battery life. We also assume that there won't be any hacking of the base station.

d) We depend on how the mobile wireless network is constructed (WCN). In this setup, that encircles a portion of the region.

When they're in mobile coverage, other devices, such as mobile wireless nodes can be connected wirelessly. So long as they are within the reach of mobile access points. base stations are considered mobile in the context of a cellular network, therefore every cell has its own boundaries and mobile wireless nodes. Key characteristics of the two types of architectures (WCN and SENMA) that follow multi-CNN data transmission, lack of need for sensor synchronisation, need for sensor-to-node communication only when queried for, avoidance of complex protocols, lower reliability of individual sensor systems, and lack of need for system reconfiguration for mobile nodes.

3.2 WSN Infrastructure and peripherals Basic

Scientists are very interested in Wireless Sensor Networks (WSN) [4], a revolutionary technology. Big randomly placed nodes often underperform overhead requirements in terms of networking, compute, and energy. The wireless network described in the message is effective and widely used [12,13], enabling a large number of users to quickly aggregate and relay communications packets. The storage capacity of the node batteries is inadequate for this kind of network, therefore it's essential to make efficient and sensible use of the resources

Wireless sensor networks (named nodes) includes devices connected wirelessly, and they are also known by the name of sensor nodes. Robots, circular systems small-power systems and devices are just a few of the instances of such devices. They are comprised of various mobile, battery-operated computer systems for data collection, aggregation and distribution by the operators and for enhancing computing capabilities and processing. Nodes, or tiny computers, comprise the network.

3.3 Packet Loss Use of recurrent neural networks for detection identifying and removing phony sensor nodes with the help of a RNN predictor.

3.4 Packet Loss Detection in complex dynamic scenes

A particular neuron in the lobster brain called the Giant Lopula Motion Detector reacts significantly to pictures of an approaching item, such as a predator (LGMD). Without utilising specialised techniques to find artefacts, the computer model is capable of handling unforeseen situations. In this study, by integrating the excitement of packet loss detection into a dynamic context, we present a recurrent neural network targeted on LGMD. In addition to being able to optimise a new feature optimization mechanism. The new technique removes the many emotions produced by context data.

3.5 Problem formulation

Every sensor on the WBAN is in direct communication with the base station. It is possible to suppose that the sensors operate independently and in sync with the timer. This case study does not use any redundant sensors. The following are the fundamental presumptions of the Simulink simulation of the prediction-based data transmission model. The clock is synced with the base station and sensors. The sensor data and communication model predicts events with extremely little delay or delay. During data transport, there is no pocket loss on the network.

Layer recurrent neural network (LRNN)

In contrast to feed forward networks, layer recurrent neural networks constantly communicate with one another and have a tapping latency. As a consequence, time series data entered into the network may generate an infinite variety of dynamic responses. This is a simplified version of the Elman Neural Network (ENN) introduced by Elman. With the exception of the last layer, each layer of the LRNN network has a single-delay feedback loop. The original ENN had only two layers, with the concealed layer using a tansig transfer function and the output layer using a purelin transfer function. A back propagation approximation technique is used to train the ENN. The Matlab Toolbox's "layrecnet command" generalises the ENN such that it may have any number of layers and any kind of transfer function on each layer. It employs the appropriate variations of gradient-based methods to train LRNN.

Algorithm - LRNN MODEL

Step 1: Load input data and target/output data;

Step 2: Define the LRNN architecture;

Step 3: Define the range for number of neurons in HL, feedback delay;

Step 4: Define Size of the input;

Step 5: Define the number of epochs;

Step 6: Set training algorithm = { LM, SCG , BR }

Step 7: Set Activation function= { tansig, purlin, logsig, radbasn, elliotsig }

Step 8: Initialize the LRNN topology;

Step 9: Train the LRNN model;

Step 10: Simulate the LRNN model for prediction;

Step 11: Calculate Error = target response – predicted response;

Step 12: Calculate the root mean square error (RMSE) and MSE;

Detecting missing values

Suppose whenever Sensor Nodes (SN) sends captured data to the Base Station (BS), the SN must wait until an acknowledgment is received from BS. If the SN does not receive an acknowledgment, it will keep on transmitting the captured data to BS with timestamp value. This scheme confirms that both the BS and the SN consumed more energy for their communication concurrently. Also, the assigned serial number (seq_no) is sent to BS for each sensor data. If BS detects missing in seqno, it flags missing sensor data alert, allowing the algorithm to recreate them using the LRNN based prediction model. At the beginning of each slot, an SN must send the actual perceived data value to BS. If BS does not receive any data, it will consider that the SN has died or crashed, and it stored “NAN” value in the memory to denote missed value.

Algorithm 3.2: Detection of missing sensor data

Procedure:

1. START
2. Initialize (seqno,= 1)
3. BS will perform the following:
4. If BS received xt with a sequence number (seqno) then Send an acknowledgement (ack)

    Else

        Xt = “ NAN”

    End if

5. If (Seqno is missing) then

    xt = “ NAN”

    End If

End

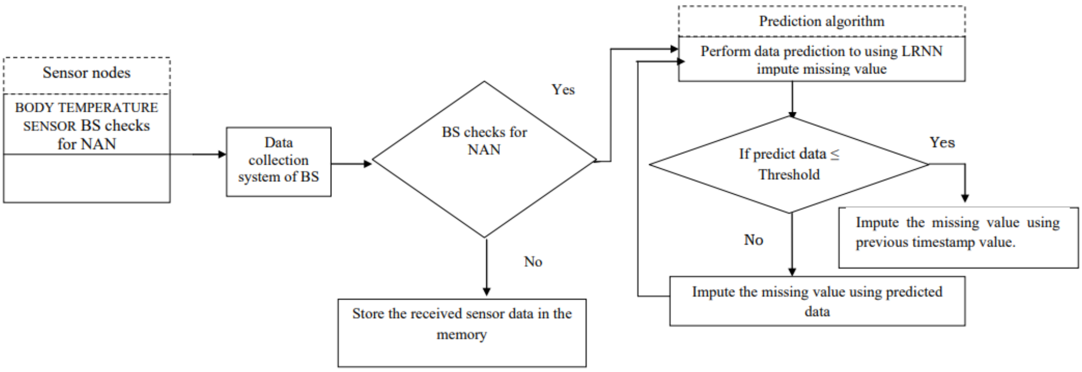

Fig 1: Data transmission reduction model using LRNN.

4. Results and Performance Evaluation

A heterogeneous healthcare platform's multimodal feature allows for the redundant collection of various data for the same variable. In this paper, we provide a strategy for dealing with the duplication issue by choosing representative values. The effectiveness of each RNN was evaluated after it was taught using the method of representative value selection. The median, the quartile and mean were all used to determine the representative value. Healthcare proof data redundancy varied depending on the device sets. There were 500 transactions in all. The amount of inaccuracy was assessed for accuracy using the RMSE.

Some of the techniques used to determine missing values include collaborative filtering (CF) as well as regression modeling (RM) as well as k-nearest neighbors (KNN) as well as deep learning (DL) [10,13(13, 10). The missing value estimation method (RMD) in this paper is based on RNN-based multimodal deep learning. Data mining employs conventional predictive methods such as CF, RM, and KNN are commonly used. In order to train deep-learning models massive quantities of data are needed however, in reality, companies and analytics generally use more traditional techniques to gather data first. The two techniques' accuracy and speed were evaluated. Healthcare data is the tests selected by the representational value-based mean method. The error level in accuracy was determined with an RMSE measure. To determine the duration of the turnaround The average of the output and input times was examined. The turnaround time and root mean square error of each missing value estimating technique. That is The study found that the suggested RMD-based technique had the lowest total error. But since there are so many different weights, RMD requires several processes and takes a long time to complete.

Computational Setup for the Proposed Work

• Experimentation platform: i7-CPU running 64-bits OS of MS Windows 10

• Simulation and Computational Software: MATLAB Toolbox 2019b.

• Initial run: Default parameters values for WSN design and development and customized network parameters' value are given in Table 1

Table 1

Parameter	Symbols	Value
BSInitial energy	EO	300 J
SNInitial energy	Es	100J
Acceptable Predictionerror	e	0.5
Numberofsensornode	N	2
Networkfieldlength	L	500m
Controldatapacket	-	2bytes
SensorDatapacket	-	10bytes
Transmissionenergy	ETX	150
Receivedenergy	ERX	50

Table 2: Energy saved by Pulse rate sensor using LRNN Tansig-WBAN Model

No.ofTransaction	No.ofMissedTransaction	EnergySavedforBaseStation	EnergysavedforSensorNode	TotalEnergySaved
T1	3	9.96	16.47	26.76
T2	5	26.56	78.30	43.89
T3	7	49.90	113.34	69.70
T4	10	83.90	167.89	87.38
T5	12	123.54	226.87	108.90

The performance of the S-WBAN and LRNN-Tansig-WBAN models with respect to the amount of energy saved by the base station during communication with the pulse rate sensor node is shown in Table 2. BS has discovered three missing transactions for the T1 transactions' pulse rate sensor. The sensor node receives the request from the standard WBAN model in order to retrieve these lost pulse rate sensor readings, using a total energy consumption of

25.32 micro joules. The prediction-based WBAN model, which used 9.96 microjoules of energy to estimate these values by BS, predicts these missing sensor values using LRNNTansig-WBAN prediction models without seeking data from the pulse rate sensor node.

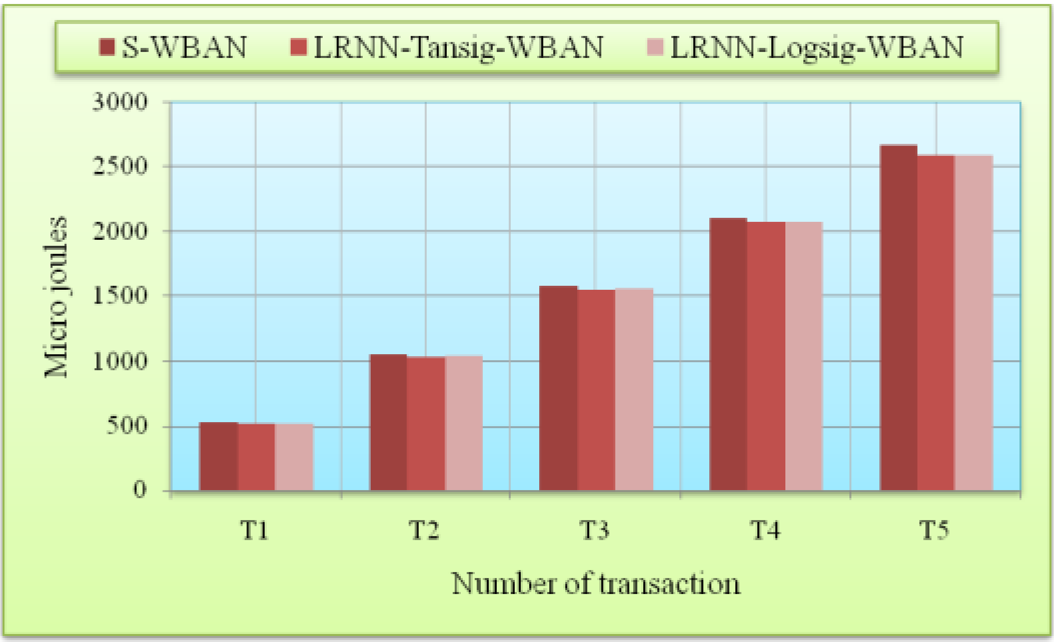

Fig 2: Comparison of all pulse rate sensor types' total energy usage.

The comparison of the pulse rate sensor's overall energy usage utilizing the S-WBAN, LRNN-Tansig-WBAN, and LRNNLogsig-WBAN models is shown in Figure 2. Given that the LRNN-Tansig-WBAN model used less energy for these transactions than the S-WBAN and LRNN-Logsig-WBAN models, it is evident that the model worked well for all of the transactions, including T1, T2, T3, T4, and T5.

5. Conclusion:

In the perspective of a WBAN, an energy-saving approach for WBAN based on the "LRNN prediction model" has been developed. The suggested LRNN-based WBAN provides an efficient method for transmitting data using less energy. In contrast to standard WBAN, this technique was developed specifically for WBAN by taking into consideration their unique properties. A WBAN based on "LRNN prediction" for data transmission is tested on simulated datasets proved to be successful and broadly applicable. The main limitation of the model proposed in this chapter is that the prediction model will be updated each time to calculate the missing values. This will take some time. To overcome this problem, a data transmission approach will be proposed in the next chapter using two different inputs, such as past sensor values and values of interrelated sensors, for better predictive accuracy without frequent prediction model updation.

References

1. Zadeh, L.A. Fuzzy logic, neural networks, and soft computing. In Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers by Lotfi A Zadeh; Word Scientific: Singapore, 1996; pp. 775–782.
2. Mitra, S.; Pal, S.K.; Mitra, P. Data mining in soft computing framework: A survey. IEEE Trans. Neural Netw. 2002, 13, 3–14. [CrossRef]
3. Yoo, H.; Chung, K. PHR based diabetes index service model using life behavior analysis. Wirel. Pers. Commun. 2017, 93, 161–174.[CrossRef]
4. Kim, J.C. Collaborative Layer Based Hybrid Multi-Modal Deep Learning for Improving Prediction Accuracy. Ph.D. Thesis,Department of Computer Science, Kyonggi University, Suwon-si, Korea, 2020.
5. Das, T.K.; Mohapatro, A. A System for Diagnosing Hepatitis Based on Hybrid Soft Computing Techniques. Indian J. Public HealthRes. Dev. 2018, 9, 235–239. [CrossRef]
6. Bernal, E.A.; Yang, X.; Li, Q.; Kumar, J.; Madhvanath, S.; Ramesh, P.; Bala, R. Deep Temporal Multimodal Fusion for Medical Procedure Monitoring Using Wearable Sensors. IEEE Trans. Multimed. 2018, 20, 107–118. [CrossRef]
7. Dehabadi, M.S.Z.; Jahed, M. Reliability Modeling of Anomaly Detection Algorithms for Wireless Body Area Networks. In Proceedings of the 2017 Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, 2–4 May 2017; IEEE: New York, NY, USA, 2017; pp. 70–75. [Google Scholar]
8. Saraswathi, S.; Suresh, G.; Katiravan, J. False alarm detection using dynamic threshold in medical wireless sensor networks. Wirel. Netw. 2021, 27, 925–937. [Google Scholar] [CrossRef]
9. Salem, O.; Serhrouchni, A.; Methaoua, A.; Boutaba, R. Event detection in wireless body area networks using Kalman filter and power divergence. IEEE Trans. Netw. Serv. Manag. 2018, 15, 1018–1034. [Google Scholar] [CrossRef]
10. Saneja, B.; Rani, R. An integrated framework for anomaly detection in big data of medical wireless sensors. Mod. Phys. Lett. B 2018, 32, 1850283. [Google Scholar] [CrossRef]
11. Pachauri, G.; Sharma, S. Anomaly detection in medical wireless sensor networks using machine learning algorithms. Procedia Comput. Sci. 2015, 70, 325–333.
12. Mugheri, A. A., Siddiqui, M. A., & Khoso, M. (2018). Analysis on Security Methods of Wireless Sensor Network (WSN). Sukkur IBA Journal of Computing and Mathematical Sciences, 2(1), 52-60.
13. Vhatkar, S., Shaikh, S., & Atique, M. (2017, February). Performance analysis of equalized and double cluster head selection method in wireless sensor network. In 2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN) (pp. 1-5). IEEE.
14. Tedeschi, A., Midi, D., Benedetto, F., & Bertino, E. (2017). Statistically-enhancing the diagnosis of packet losses in WSNs. International Journal of Mobile Network Design and Innovation, 7(1), 3-14.
15. Thrimoorthy, N., Anuradha, T., & Kumar, A. (2017, September). A virtual model to analyze congestion in a wireless sensor network (WSN). In 2017 International Conference on Advances in Electrical Technology for Green Energy (ICAETGT) (pp. 28- 32). IEEE.