DIGITAL FINGERPRINT OF THE PROTECTED ENVIRONMENT

ROTAR DAN[1*], ANDRIOAIA DRAGOŞ[1]

[1] *Vasile Alecsandri University of Bacău, Calea Mărăşeşti 156, Bacău, 600115, Romania*

Abstract: The development of IOT (Internet of Things) technology has led to the emergence of numerous applications that use the Internet as a means of communication. The paper presents an application of this kind that represents a smart home. The main feature of this application is due to the presence of artificial intelligence. Thus, a neural network is used to predict the occurrence of adverse events. This aim is a fingerprint of the signals generated by the sensors for different regimes of the smart house. When changing the fingerprint, the neural network decides whether the modification constitutes a dangerous situation and causes the measures to be taken accordingly.

Keywords: neural network, Internet of things, intelligent house, fingerprint of signal.

1. INTRODUCTION

Released relatively recently, IOT technology has experienced an explosive development in several areas: devices, technologies and platforms. IOT is equally a technology and a concept. Due to the numerous advantages presented by this technology there is extensive research into the development of this area. There is currently a tendency to generalized connection through the Internet of many elements with which we interact in the daily work [1].

In order to integrate into this technology, an object must be capable of either receiving data and sending data either via the Internet. There are currently complex structures built on various principles that are connected to the Internet network. For example, if all devices in one enclosure can connect directly to the Internet, the solution has high reliability, but the costs can be high. On the other hand, if the devices connect to a central point, the reliability is lower, but the costs may be lower. From another point of view, a central point allows the primary processing of data before it is sent over the Internet [1] [2].

Another aspect is presented by information security over the Internet. The use of a focal point can increase information security through the implementation of advanced protection measures. You can also make primary data processing by filtering and converting them. This way the communication is simplified and the amount of data lot transmitted is reduced.

The number of objects (sensors, execution elements, smart elements) currently present at a smart house is relatively high. For this reason, detecting dangerous situations by analyzing a set of signals is generally difficult. Depending on the outcome of the analysis, sometimes local measures may be taken, other than outside intervention is required. A local decision-making factor can often be essential in such situations.

The paper presents the general structure of a smart house with a central point. In the focal point, with specific computing capabilities, a predictive neural network is deployed. This network is designed to analyze the fingerprint of the environment and to decide what measures need to be taken to remedy the situation [3].

[*] Corresponding author, e-mail drotar@ub.ro

2. THE STRUCTURE OF THE SMART ENVIRONMENT

The smart environment is a generic smart home structure. The house has three rooms, a kitchen, two bathrooms and two halls. Each room is equipped with open sensors [3] on windows and doors, broken window sensor on Windows, presence sensor, humidity sensor and temperature sensor. There are also presence sensors in the halls.

All these sensors are connected to a centralized system with the following functions:

- Monitors Opening doors and windows;
- Monitors the breaking of the windows;
- Monitors the presence of persons in rooms;
- Monitors the temperature in each room;
- Monitor the humidity in each room.

In special situations the system can also be equipped with noise sensors or microphones for capturing ambient sounds.

The smart home system can also be filled with other sensors or control elements (cameras, chemical sensors, etc.). The structure presented is a minimal structure for the intended purpose and is shown in Figure 1.

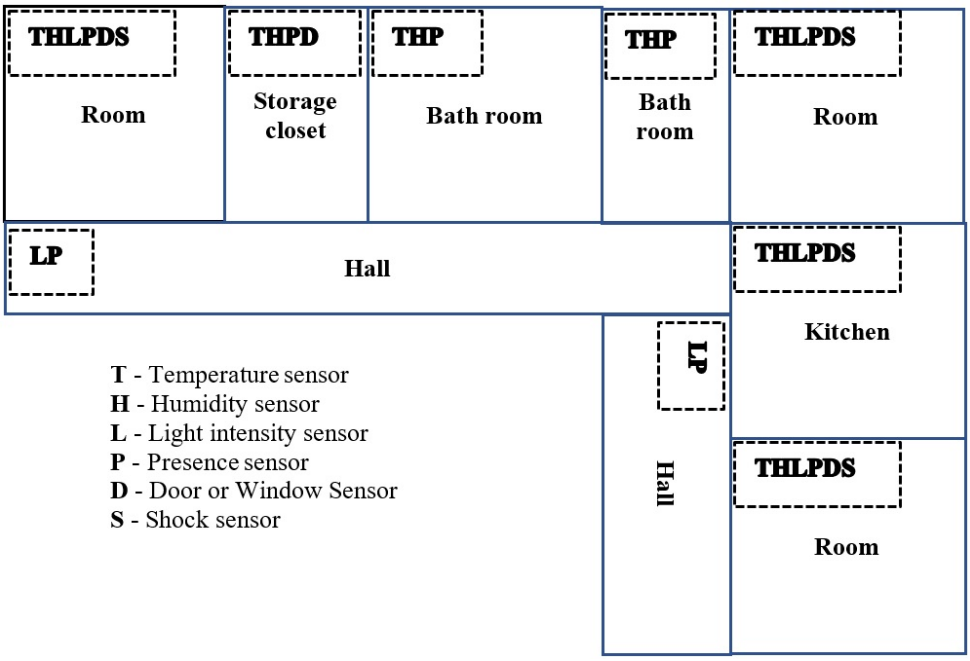

Fig. 1. The Smart House.

All these items are connected by radio to a central system [3] [4]. The central system develops alarms and local and remote alerts. The centralized system is also equipped with a prediction mechanism made with a neural network.

3. NEURAL PREDICTION NETWORK

The Neural prediction network is shown in Figure 2. This neural network is designed to generate alarm and/or warning signals based on the fingerprint of existing signals in the smart environment.

In the network training phase, it shall be presented to the group of signals for known situations and warnings and/or alarms that the network must generate. In Figure 3, the network training mechanism is presented.

Input sequences are vectors of the values of the elements in the smart environment. These forms (sequences) represent situations of ambient conditions for which there is no suspicion of the occurrence of an unwanted event. For example, a sequence is represented by the multitude of temperature and humidity values at a given time on the premises.

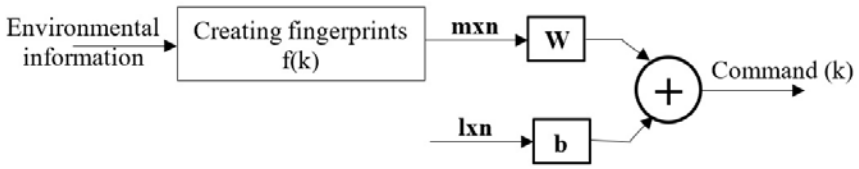

Fig. 2. The prediction neural network.

This sequence has a predictable and dependent evolution of certain factors: the presence of persons, time represented by the hour and date, the status of other objects, etc. Typically, it assumes that the network provides enough examples of input-output pairs. In this way the network is instructed to recognize those shapes that correspond to the sequences describing abnormal or dangerous states. The network is trained adaptively, step by step, to anticipate a series of sequences over time. Because the network Is incrementally trained, it can respond to changes in the relationship between previous values and future signal values.

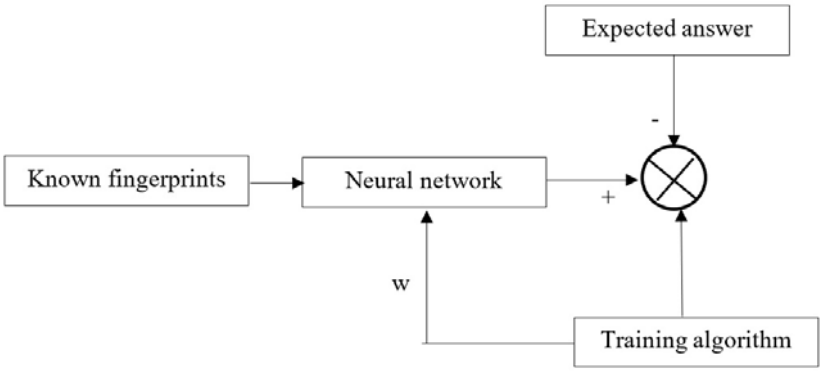

Fig. 3. Neural network training.

One of the important issues of these structures is the sampling signal rate. For example, the signals collected from the temperature and humidity sensors are continuously changing. A constant speed of the sampling rate may be established, or a threshold may be established, which if it is exceeded to trigger the sampling process (for the sequence).

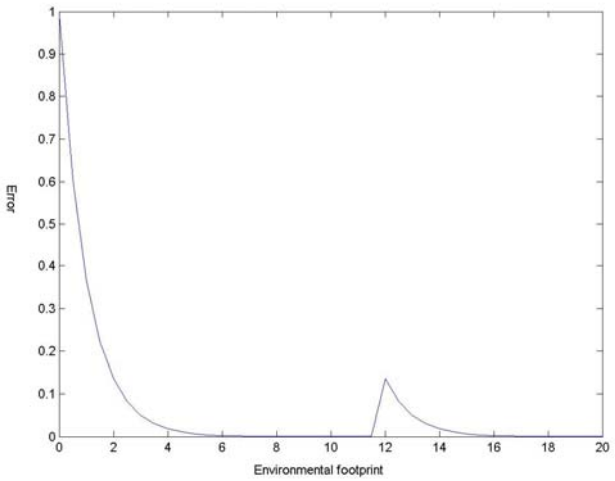

Fig. 4. Error signal.

It can be estimated that the intelligent environment considered is a nonlinear system. An adaptive model is very precise, if the restless system remains near the given operating point. If the nonlinear system moves to a different operating point, the adaptive network changes the model for the new point. This will generate an error that can negatively influence the operation of the system. Figure 4 represents the network error signal at such an event.

As seen from Figure 4, the error signal can generate false alarms since it is not a system error but is the error of adapting the network to the new conditions. Therefore, the alarm signal should be correlated with the sensor that generates this condition. It also introduces different time constants that allow the system to reach the state in which the result is a certainty.

4. CONCLUSIONS

Using a predictive neural network Improve the performance of the smart home system. Firstly, the introduction of the neural network allows the local processing of information without the need for remote transmission of information. The system sends through the INTERNET network codes corresponding to the different crash situations [7] [8].

For simple systems, the network has fewer predictive models. For this reason, high complexity systems have much better results.

The use of the predictive neural network eliminates the need for the presence of a human operator. In most cases the signals generated were correct and the situations were resolved correctly. Following the experiments resulted in a confidence degree of 87%. Further refinements can increase this confidence.

REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami Et. Al. Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems Volume 29, Issue 7, September 2013, p. 1645-1660
[2] Mung Chiang, Tao Zhang Et. Al. Fog and IoT: An Overview of Research Opportunities, IeEE Internet of Things Journal, Volume: 3IssEU: 6, Dec. 2016, p. 854–864
[3] Qian Zhu, Ruicong Wang, Qi Chen, Yan Liu, Weijun Qin Et. Al. IOT Gateway: bridgingwireless Sensor Networks into Internet of Things, IEEE/IFIP International Conference on Embedded and ubiquitous Computing, Hong Kong, China, 2011
[4] Fei Tao, Ying Zuo, Li Da Xu, Lin Zhang, IoT-Based Intelligent Perception and Access of manufacturing Resource Toward Cloud Manufacturing, IEEE Transactions On Industrial Informatics 10 (2), May 2014, p. 1547-1557
[5] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma Et. Al. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges, IEEE International Conference on Services Computing, 27 June-2 July 2015
[6] S.D.T. Kelly, N.K. Suryadevara, S.C. Mukhopadhyay, Towards the Implementation of IoT for Environmental Condition Monitoring in Homes, IEEE Sensors Journal 13 (10), 2013, p. 3846-3853 2013
[7] C. Ranhotigamage and S. C. Mukhopadhyay, "Field Trials and Performance Monitoring of Distributed Solar Panels Using a Low Cost Wireless Sensors Network for Domestic Applications", IEEE Sensors Journal, Vol. 11, No. 10, October 2011, p. 2583-2590
[8] K. Kaur, S. C. Mukhopadhyay, J. Schnepper, M. Haefke and H. Ewald, "A ZigBee Based wearable Physiological Parameters Monitoring System", IEEE Sensors Journal, Vol. 12, No. 3, March 2012, p. 423-430
[9] G. M. Mendez, M.A.M. Yunus and S. C. Mukhopadhyay, A WiFi based Smart Wireless Sensor Network for Monitoring an Agricultural Environment, Proceedings of IEEE I2MTC 2012 Conference, IEEE Catalog number CFP12MT-CDR, ISBN 978-1-4577-1771-0, May 13-16
[10] N. Bui, A.P. Castellani, P. Casari, M. Zorzi, "The Internet of Energy: A Web-enabled Smart grid system", IEEE Network, 2012, Vol.26, Issue. 4, p. 39 – 45
[11] Syed Hassan Ahmed, Dongkyun Kim, Named data networking-based smart home, ICT Express 2 (2016), p. 130–134.