Smart Home Security System Based on ANFIS

LeeJeong-Gi[1],Lee Sang-Hyun[2], Moon Kyung-Il[2]

[1]Korea Electronics Technology Institute, Korea
[2]Dept. of Computer Engineering, Honam University, Korea
[2]Dept. of Computer Engineering, Honam University, Korea
{leesang64, kimoon}honam.ac.kr, jklee@keti.re.kr

Abstract.A smart home or building is a home or building, usually a new one that is equipped withspecial structured wiring to enable occupants to remotely control or program an array ofautomated home electronic devices by entering a single command. Conventional securitysystems keep homeowners, and their property, safe from intruders. Smart home security has two aspects, inside and outside. Inside security covers the concept of securing home from threats like fire etc. whereas, outside security is meant to secure home against any burglar/intruder etc. In this paper, we suggest an adaptive network fuzzy inference system for home security.To deal with nonlinear outputs, the system is modeled by multiple ANFIS, and the optimization of multiple outputs is formulated as a multiple objective decision making.

Keywords: Fuzzy logic, Multiple ANFIS, Smart Home Security

1 Introduction

A smart homecare system using smart phones, wireless sensors, web servers and IP webcams is proposed by Leijdekkers et al [5]. It provides facility to elderly people to check their health and status and provides an easy way to contact to hospital in an emergency. Ghorbel et al have proposed the integration of networking and communication technologies in the smart homes concept dedicated to people with disabilities. It is based on the UPnP protocol to discover and control devices indoor and uses wireless technologies to enhance mobility [2]. Popescu et al have proposed a security architecture allowing digital rights management in home networks consisting of consumer electronic devices [2]. In the proposed model, devices are allowed to establish dynamic groups in an environment where legally acquired copyrighted content are seamlessly transmitted between devices. They have claimed that connectivity between devices has a minimal reliance on public key cryptographic operations. Gao et al have suggested the concept of a self-programming thermostat that without any human intervention creates a best possible setback schedule by sensing the possession statistics of a home [1]. The system monitors possession using simple sensors in the home and the user defines the desired balance between energy and comfort using a single knob. It is observed that this approach has an advantage

over EnergyStar setback schedule approach by reducing the heating and cooling demand by up to 15%.

The purpose of this paper is to portray as to how Adaptive Network Fuzzy Inference System (ANFIS) encounters the challenges posed to the sensor based classical smart home systems and propose a methodology for implementation of these networks to build an adaptive and intelligent system. Home security has two aspects, inside and outside. Inside security covers the concept of securing home from threats like fire etc. whereas, outside security is meant to secure home against any burglar/intruder etc. This work is aimed to provide a multiple ANFIS solution for home security that takes decision dynamically using the pervasive devices. Also this solution has the feature to intimate security analysis results anywhere in the world using internet. In section 2, we review briefly the tools related to the smart home security, and represent a structure of intelligent inference module at inside/outside home security server. In section 3, a multiple ANFIS model is proposed to provide optimal home security solution. In this proposed model, sensors are used to detect abnormalities within the house or outside the house. In section 4, simulation results by the suggested model are demonstrated, and compared with simple fuzzy logic based method. Also, concluding remarks are given in the last section.

2 Smart Home security Structure

From some tools related to the smart home security, it is observed that the home security models have considered some limited security concerns. Therefore one security model may be good in one situation but cannot provide the required results in other situations. To provide optimal home security solution, a new model is required. In this model, sensors are used to detect abnormalities within the house or outside the house. There is a dedicated server for the sensors used to collect data inside the house. This server is responsible to collect information transmitted by the sensors and then analyze to detect any abnormality. Similarly, a separate server is used to process the information transmitted by sensors located outside the house. Both these servers are connected to a main server which process the information provided by these servers. ANFIS tool is used to detect any abnormality. In case a threat is detected then main server report about the threat to concern people using internet besides setting the alarms on.

Six input types are provided to the system. Multiple sensors of each type are used to collect data. All inputs of same sensor type are provided to an initial ANFIS inference module, which is responsible to calculate the threshold value. These calculated threshold value of each input type is then provided to respective server responsible for inside or outside security. An overall threshold value of these six initial threshold values is separately calculated using ANFIS module on inside/outside security servers respectively. Both inside/outside security threshold values are provide to main server for analysis. Final decision is made based on these values. If any of the value is above the critical value then alarm signal is generated to respective person/department. Using this method, it is possible to generate different output alarms considering the intensity and relevance of threshold value to that specific

person/department. Threshold values calculated at the inside/outside servers are collated at main server for decision making process. After collation process, threshold value is calculated and alarm signal type for each desired destination (police, rescue station, owner, et al) is calculated.

Multiple ANFIS is an extension of the single output neuro-fuzzy system ANFIS [4], for producing multiple outputs. Smart home security problem is a process with multiple outputs. Therefore, modeling and optimization of a process with multiple outputs is required. A neuro-fuzzy system can serve as a nonparametric regression tool, which model the regression relationship non-parametrically without reference to any pre-specified functional form. Every single ANFIS in an multiple ANFIS simulatesthe functional relations f_i, i=1,…,m. ANFIS can be considered as anetwork presentation of a TSK fuzzy inferencesystem, and the if-then rules in TSKare comprised in the network structure. Toillustrate the architecture of ANFIS, an examplewith a two-dimensional input is visualizedin Fig.1.

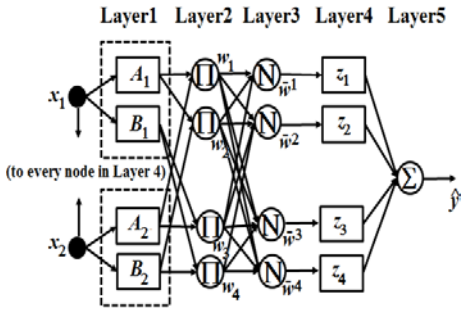

Fig. 1.ANFIS architecture

3 An ANFIS design

By means of the learning process, multiple ANFISobtains an estimation of desired outputswith given inputs. Let f_i, i=1,...,m, be the$i$-th output of multiple ANFIS, and they are estimatesof multiple responses y_1,...,y_m, respectively.To indicate these estimates are functionsof the input variables x, they will bedenoted as $f_i(x)$, i=1,...,m.Since the system under discussion has multipleresponses, the optimization of the systemin fact involves the optimization of severalindividual responses at the same time.For all the system responses, they can be dividedinto three sets: (a) “thelargerthebetter,”denoted by L; (b) “thesmallerthebetter,” denotedby S; and 3) “thenominalthebest,” denotedby N. We have formulated this optimizationproblem as a multiple objective decisionmaking problem with the following form:

$$\begin{cases} \max f_l(x), \forall l \in L \\ \min f_s(x), \forall s \in S \\ \min \left| f_t(x) - T_t \right|, \forall t \in N \ \ s.t. x \in B \end{cases} \tag{1}$$

Here$T_t$is the nominal target of the *t*-th response;and *B* is a feasible region of *x*.

We follow the idea ofZimmermann's maximin approach. Accordingto the maximin approach, the above solutioncan be obtained by maximizing anoverall satisfactory degree among all individualobjectives. That is, for each objective,it has its own satisfactory degree, andthe overall satisfaction is an intersection of allindividual satisfactory degrees, where the intersectionis defined through a min operator.The satisfactory degree for each objective isevaluated by userdefined membershipfunction.Each response's membership functionμ should be well chosen so as toreflect its characteristic. For the response belongedto the set of "thelargerthebetter," itsdegree of satisfaction reaches 1 when it is at $f_i^* = \max_{x\in B}\{f_i(x)\}$ and then decreases monotonically to 0 at $f_i^- = \max_{x\in B}\{f_i(x)\}$. Atypical membership function forf_i, $i\in L$, could be stated as

$$\mu_{f_i} = \begin{cases} 1, \ if \ f_i > f_i^* \\ (f_i - f_i^-)/(f_i^* - f_i^-), \ if \ f_i^- \le f_i \le f_i^* \\ 0, \ if \ f_i < f_i^- \end{cases}$$

(2)

For the response belonged to the set of"thesmallerthebetter," we set the satisfactorydegree to 1 when a response is at f_i^-andthen it decreases monotonically to 0 atf_i^*. Such type of membership functions canbe expressed as

$$\mu_{f_i} = \begin{cases} 1, \ if \ f_i < f_i^* \\ (f_i^* - f_i)/(f_i^* - f_i^-), \ if \ f_i^- \le f_i \le f_i^* \\ 0, \ if \ f_i > f_i^* \end{cases}$$

(3)

Similarly, for the response of the set "thenominalthebest," the degree of satisfactionis maximized when it is at its target T_i,and decreases as it is away from T_i. The maximum of λ cannot bedirectly solved by the use of derivative-basedmethods due to unknown functional forms off_i. Derivative-free methods areideally suited for solving problems where derivativeinformation is unavailable. Alternatively,we can approximate the derivativeswith numerical methods.

4 Simulation results

Home security system is configured by sensor nodes connected to server. These sensor nodes include radio frequency, ultrasonic, temperature, light, sound and video sensors. Threshold value for each input is above 90% and for a video sensor, used in outside security, distance threshold is taken as 1 feet. If value is increased from any threshold value then alarm is on, and notified to specified location through internet. For a sample scenario, where only three types of sensors are used namely video, fire and voice. Five layers of neural networksresulting from the ANFIS have been provided in figure 2.Effect ofthreshold values of input sensors and ANFIS output"Police" is somewhat lower than simple fuzzy logic based one, and effect of

threshold values of input sensors and ANFIS output “Rescue station” is somewhat higher than simple fuzzy method. Also, effect of threshold values of input sensors and ANFIS output “Owner” is somewhat higher than simple fuzzy method. For example, in case of “video Sensor=88.2”, “Fire Sensor=89.5”, and “Voice Sensor=86.4”, effect of threshold values of input sensors and respective ANFIS output is 78.8, 84.0 and 95.0. Effect of threshold values of input sensors and respective fuzzy logic based output is 81.9, 81.5 and 92.5.

Since the outputs “Owner” and “Rescue”belongs to the set of “thelargerthebetter,” its membership function should takethe form of (2); and the output “Police” has anominal target, so it will take the membershipfunction (3). In order to determine thesemembership functions, the maximum andminimum for individual output must be obtained.Maximum and minimum of outputs can be obtained by formulating single objectiveprogramming problems for individualresponses, and solving the problems with anyderivative-free algorithm. Alternatively, theycan also be subjectively determined accordingto users' judgment or their expectation. In our scenario, it is desired that the outputs of“Owner” and “Rescue”to be held between 92 and 98,therefore, it is reasonable to set 92 and 98 asthe minimum and maximum of this output,respectively. Similarly, the minimum and maximum of “Police”are set as 70 and 91, respectively.In figure 3, 3D graph show the relationship betweenvoice sensors, fire sensors and output threshold forrescue. Effect of threshold values is represented very well than simple fuzzy logic based output. In figure 4, 3D graph show the relationship betweenvoice sensors, fire sensors and output threshold forpolice. It is more reasonable than the relationship by simple fuzzy logic.

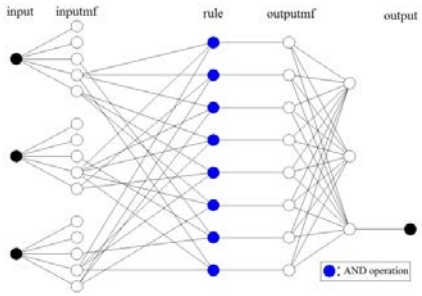

Fig. 2.ANFIS structure for sample scenario

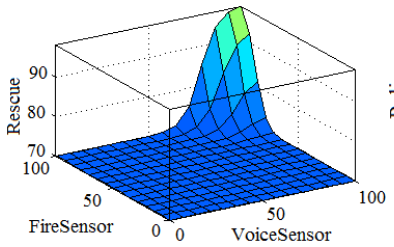

Fig. 3."Rescue" surface for fire and voice sensor

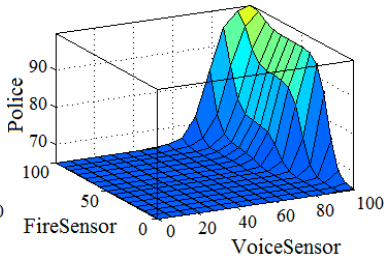

Fig. 4."Police" surface for fire and voice sensor

5 Concluding Remarks

This study used an adaptive network fuzzy inference system forsmart home security. This system provides the advantage ofmodeling a nonlinear and complicated systemwithout the need of finding suitable functionalforms for the system, and its neural networklearning ability also equips multiple ANFIS withhigh efficiency in smart home security system modeling.Proposed systeminherits the properties of ANFIS and thus providesintermediary values as compare to Boolean logic bi-valueoutputs.However,since we use the nonparametric regressiontool for multiple ANFIS to model outputs, exactfunctional forms of outputs are not knownand hence derivative-based optimization cannot be directly applied to obtainthe optimal solution.

References

1. Gao,G.,Whitehouse,K.: The Self-ProgrammingThermostat: Optimizing Setback Schedules based on HomeOccupancy Patterns, Proceedings of BuildSys'09, November 3,Berkeley, CA, USA (2009)
2. Ghorbel,M., Segarra,M., Kerdreux,J., Keryell,R., A.,Thepaut,and M. Mokhtari.: Networking and Communication in SmartHome for People with Disabilities, Computers Helping Peoplewith Special Needs, Springer Berlin / Heidelberg, 624, (2004)
3. Hou,J.,O'Brien, D. C.: Vertical handover-decision-making algorithm using fuzzy logic for the integrated radioand OW system, IEEE Transactions on Wireless Communications,5(1),176--185, (2006)
4. Jang,J. S. R.: ANFIS: Adaptive network based fuzzy inference system,IEEE Transactions on Systems, Man andCybernetics, 23(3),665--685, (1993)
5.Leijdekkers,P., Gay,V., Lawrence,E.: Smart HomecareSystem for Health Tele-monitoring, Proceedings of the FirstInternational Conference on the Digital Society, IEEEComputer Society(2007)
6. Popescu,B. C., Crispo,B., Tanenbaum,A. S.,Kamperman, F. L. A. J.: A DRM Security Architecture for HomeNetworks, Proceedings of the 4th ACM workshop onDigital rights management, October 25, Washington, DC,USA.(2004)
7. Reyhani,S. Z.,Mahdavi,M.: User Authentication Using Neural Network in Smart HomeNetworks, International Journal of Smart Home, 1(2), July (2007)