Smart Home Security System Using Multiple ANFIS

Lee Sang-Hyun[1], Jeong-Gi Lee[2*] and Moon Kyung-Il[1]

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

Abstract

Many smart home devices provide home automation technology, but the smart home security system offers many benefits that can ensure the safety of the homeowner. Thus, Security has been an important issue in the smart home applications. 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 study is aimed to provide an intelligent solution for home security that takes decision dynamically using the pervasive devices. In particular, smart home security can be regarded as a process with multiple outputs. In this study, 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, Home Security, Smart Home, Pervasive devices, Sensors*

1. Introduction

A smart home or building is a home or building, usually a new one that is equipped with special structured wiring to enable occupants to remotely control or program an array of automated home electronic devices by entering a single command. For example, a homeowner on vacation can use a touchtone phone to arm a home security system, control temperature gauges, switch appliances on or off, control lighting, program a home theater or entertainment system, and perform many other tasks. The field of home automation is expanding rapidly as electronic technologies converge. The home network encompasses communications, entertainment, security, convenience, and information systems. Smart home is, in short, the term commonly used to define a residence that integrates technology and services through home networking to enhance power efficiency and improve the quality of living [14].

Smart home security system offers much more protection than the typical fire alarm. This type of system checks carbon monoxide levels as well as watching for signs of fire and monitors all areas of the home. In the event of a fire, the smart home security system can alert the homeowner and notify emergency services. Artificial intelligence programs are even able to pinpoint the location of the fire, and provide that information to fire department personnel as they respond. Security codes, motion detectors, and cameras provide information to a smart home security system, allowing it to determine whether an individual is a resident, a cleared visitor, or an intruder. Whenever smart home security system detects someone who is unknown, it can provide video of the visitor to the homeowner. Visitors that are welcome can be given clearance and allowed in the house remotely. Unwelcome visitors can be ignored, and individuals attempting to break in will trigger a call to the police. Intruders and fires are not the only dangers in a home.

A smart home security system also protects residents from unanticipated health problems. Using the same cameras and motion detectors that protect the outside of a home, smart houses can learn about the habits and normal movements of the residents. When the resident does something unexpected, and does not resume normal activities, the smart home can alert family members or emergency services. This aspect of a smart home is particularly helpful for the elderly, or those in fragile health [11]. It is supposed that in future people will have an invisible and ubiquitous computing infrastructure to perform different activities both at work and home. Modern home requires easy to use and synergistic devices. Spinellis has proposed the idea of Information Furnace to integrate different available devices in home for different services [16]. Currently, a variety of devices is available in modern home with different access modes and interfaces which results in complexity for end user. The Information Furnace model proposes the synergies among these devices.

A smart homecare system using smart phones, wireless sensors, web servers and IP webcams is proposed by Leijdekkers, *et al.*, [10]. 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 [6]. Popescu, *et al.*, have proposed a security architecture allowing digital rights management in home networks consisting of consumer electronic devices [12]. 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 [5]. 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%.

Use of wireless sensor networks is a low cost, easy way to monitor physical environments. By integrating the context-aware capability of wireless sensor networks into surveillance systems is an attractive trend. Tseng, *et al.*, have proposed iMouse system, which combines wireless sensor networks, and surveillance technology, to support intelligent mobile surveillance services [18]. It consists of mostly inexpensive static sensors to monitor environment and few expensive mobile sensors to perform some advanced actions. Kim et al have proposed a Home Security system based on Sensor Network (HSSN) configured by sensor nodes including radio frequency (RF), ultrasonic, temperature, light and sound sensors [9]. It has the capability to acknowledge security alarm events that are acquired by sensor nodes. Initially fuzzy logic control was introduced to model free control design approach but was criticized due lack of systematic stability analysis and controller design. G. Feng has shown the current improvement in the analysis and design of model based fuzzy control systems [4]. Also, Saeed et al represent the concept of fuzzy inference module at inside/outside home security server [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. Home security tools and multiple ANFIS

Smart home environments typically are equipped with different kinds of sensors and tracking devices for context-aware service provisioning. While on the one hand, people want to take advantage of the comfort and added value of personalized context-aware services, privacy and traceability becomes a serious concern on the other hand. The question arises, how we can build up trust into inherently untrusted services in a potentially hostile environment? How can it be guaranteed that eventually all sensitive data is deleted or safely stored away? The Sentry@HOME concept, as part of our User-centric Privacy Framework, addresses these concerns. Sentry@HOME is designed to become an integral part of the user’s home environment; seamlessly embedded into the Smart home software infrastructure. The Smart home itself then can be leveraged to act as a privacy proxy for a tracked individual. On behalf of the user it constitutes the central privacy enforcement point for all privacy-relevant accesses to private or sensitive data. We are confident that our contribution, the combination of the smart homes and a privacy-aware infrastructure, substantially adds to the success of personalized pervasive computing systems.

Distributed Denial of Service (DDoS) attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. DDOS attack through spam mail is one of the new versions of common DDoS attack. In this type, the attacker penetrates the network by a small program attached to the spam mail. After the execution of the attached file, the mail server resources will be eaten up by mass mails from other machines in the domain results denial of services. This defense mechanism is a multilayer approach to defend the DDoS attack caused by spam mails. This approach is a combination of fine tuning of source filters, content filters, network monitoring policy, general email policies, educating the user & timely logical solutions of the network administrator. Fine tuning of source filters reject the incoming connections before the spam mail delivery. The content filters analyses the contents of the mails and blocks the incoming unwanted mails. Network monitoring approach provides general solution to identify the attacks prior to the attack and also during the attack. Business houses should educate the user about possible attack scenarios and reacting ways to it. The logical solutions of the network administrator play an important role during the attack period and even post attack period. The combination of these layers provides best methodology to stop the DDoS attacks established though spam mails.

From the above 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. Figure 1 denotes the graphical representation of basic logic of the ANFIS system.

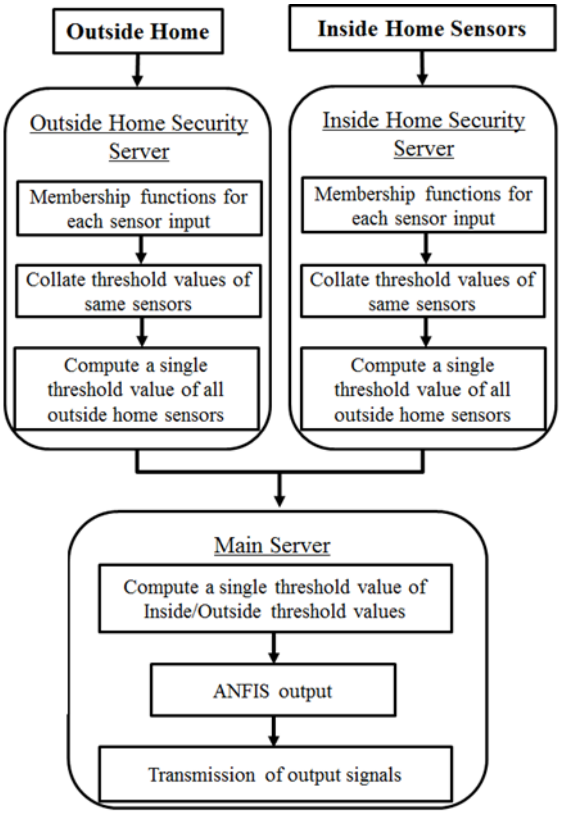
Outside Home
Inside Home Sensors
Outside Home Security Server
Membership functions for each sensor input
Collate threshold values of same sensors
Compute a single threshold value of all outside home sensors
Inside Home Security Server
Membership functions for each sensor input
Collate threshold values of same sensors
Compute a single threshold value of all outside home sensors
Main Server
Compute a single threshold value of Inside/Outside threshold values
ANFIS output
Transmission of output signals

Figure 1. Security inference structure using ANFIS

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, *etc.*) is calculated.

Multiple ANFIS is an extension of the single output neuro-fuzzy system ANFIS [8], 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. Multiple ANFIS can be viewed as an aggregation of many independent ANFIS. The architecture of multiple ANFIS is depicted in Figure 2.

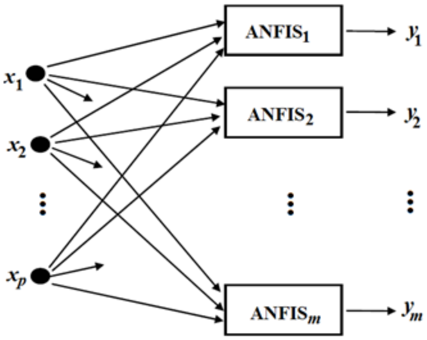

Figure 2. MANFIS architecture

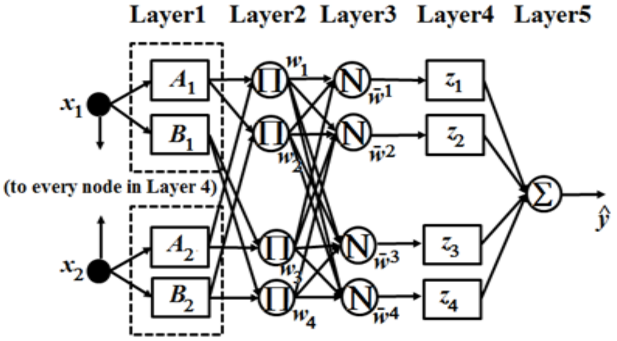

Figure 3. ANFIS architecture

Every single ANFIS in an multiple ANFIS simulates the functional relations fi, i=1,…,m. ANFIS can be considered as a network presentation of a TSK fuzzy inference system [17], and the if-then rules in TSK are comprised in the network structure. To illustrate the architecture of ANFIS, an example with a two-dimensional input is visualized in Figure 3.

3. Multiple ANFIS design for smart home security

To reflect different adaptive capabilities, the nodes in ANFIS are represented by circles or squares, in which, square nodes represent adaptive nodes and circle nodes represent fixed nodes. Adaptive nodes contain parameters that can be adjusted by learning, while the fixed nodes do not contain adjustable parameters. In this study, the adaptive nodes in layer 1 of the ANFIS are parameterized by Gaussian functions with their means and deviations. Nodes in layer 2 are fixed nodes labeled Π, which is a fuzzy conjunction operator. Functions of nodes in this layer are to synthesize the information from the first layer. The operator Π is defined as a multiplication of all of its incoming signals, and output the firing strength w_j, j=1,...,r. Nodes in layer 3 labeled by N simply performs a normalization of signals from layer 2 and output the normalized firing strength. The adaptive nodes in layer 4 of the ANFIS contain linear functions of the input variables with their coefficients as the adjustable parameters; that is, $z_j = a_jx_1+b_jx_2+c_j$, j=1,...,r. The single node in layer 5 is a fixed node, which computes the overall output as the summation of all incoming signals:

$$\hat{y} = \sum_{j=1}^{r} \overline{w}^{j} z_{j} \tag{1}$$

Assuming that we have conducted an experiment with n runs on an m-output system, n observations are collected with the format of (x_k, y_{1k}, ... , y_{ik}, ... ,y_{mk}), k=1,...,n, where x_k is the input condition at the k-th run and y_{ik} is the i-th response at the k-th run. With these observations, multiple ANFIS can approximate the multiple outputs y_i, i=1,...,m, by minimizing an error measure E defined as

$$E = \sum_{k=1}^{n} \sum_{i=1}^{m} \left(y_{ik} - \hat{y}_{ik} \right)^2 \tag{2}$$

The minimization of E is carried out in an iterative manner, which is referred to as a learning process. The learning process of multiple ANFIS terminates when the error measure E reduces to a satisfactory level. Since E is a summation of the squared errors from m independent ANFIS, the learning of multiple ANFIS can be treated as the learning of m independent ANFIS. Furthermore, since ANFIS is a multi-layered-feed-forward network, back-propagation learning algorithms used in neural networks can be directly applied to the learning process.

By means of the learning process, multiple ANFIS obtains an estimation of desired outputs with given inputs. Let f_i, i=1,...,m, be the i-th output of multiple ANFIS, and they are estimates of multiple responses y_1,...,y_m, respectively. To indicate these estimates are functions of the input variables x, they will be denoted as $f_i(x)$, i=1,...,m. Since the system under discussion has multiple responses, the optimization of the system in fact involves the optimization of several individual responses at the same time. For all the system responses, they can be divided into three sets:

1) "the larger the better," denoted by L;

2) "the smaller the better," denoted by S; and

3) "the nominal the best," denoted by N. We have formulated this optimization problem as a multiple objective decision making problem with the following form [18]:

$$\begin{cases} \max\ f_l(x), \forall\, l \in L \\ \min f_s(x), \forall\, s \in S \\ \min \left| f_t(x) - T_t \right|, \forall\, t \in N \quad s.t. x \in B \end{cases} \tag{3}$$

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

To solve the above multiple objective optimization problem, we follow the idea of Zimmermann's maximin approach. According to the maximin approach, the above solution can be obtained by maximizing an overall satisfactory degree among all individual objectives. That is, for each objective, it has its own satisfactory degree, and the overall satisfaction is an intersection of all individual satisfactory degrees, where the intersection is defined through a min operator. The satisfactory degree for each objective is evaluated by user defined membership function. Let λ be the overall satisfactory degree, and then we can convert the above equation to

$$\begin{aligned} &\max \ \lambda \ s.t. \mu_{f_i}(f_i(x)) \geq \lambda, \\ &i = 1, .. m, , x \in B, \lambda \in [0,1] \end{aligned} \tag{4}$$

Each response's membership function μ should be well chosen so as to reflect its characteristic. For the response belonged to the set of “the larger the better,” its degree of satisfaction reaches 1 when it is at $f_i^* = \max_{x \in B}\{f_i(x)\}$ and then decreases monotonically to 0 at $f_i^- = \max_{x \in B}\{f_i(x)\}$. A typical membership function for f_i, $i \in L$, could be stated as

$$\mu_{f_i} = \begin{cases} 1, \ iff_i > f_i^* \\ (f_i - f_i^-)/(f_i^* - f_i^-), \ iff_i^- \leq f_i \leq f_i^* \\ 0, \ iff_i < f_i^- \end{cases} \tag{5}$$

For the response belonged to the set of “the smaller the better,” we set the satisfactory degree to 1 when a response is at f_i^- and then it decreases monotonically to 0 at f_i^*. Such type of membership functions can be expressed as

$$\mu_{f_i} = \begin{cases} 1, \ iff_i < f_i^* \\ (f_i^* - f_i)/(f_i^* - f_i^-), \ iff_i^- \leq f_i \leq f_i^* \\ 0, \ iff_i > f_i^* \end{cases} \tag{6}$$

Similarly, for the response of the set “the nominal the best,” the degree of satisfaction is maximized when it is at its target T_i, and decreases as it is away from T_i. Membership functions of this type can be defined as

$$\mu_{f_i} = \begin{cases} 1 - \dfrac{T_i - f_i}{T_i - f_i^-}, \ iff_i^- < f_i \leq T_i \\ 1 - \dfrac{f_i - T_i}{f_i^* - T_i}, \ ifT_i \leq f_i \leq f_i^* \\ 0, \ elsewhere \end{cases} \tag{7}$$

The maximum of λ cannot be directly solved by the use of derivative-based methods due to unknown functional forms of f_i. Derivative-free methods are ideally suited for solving problems where derivative information is unavailable. Alternatively, we can approximate the derivatives with 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. Inputs to the system and respective outputs from MANFIS are shown in Figure 4. Member functions of each sensor are the same as Figure 5 for the sample scenario.

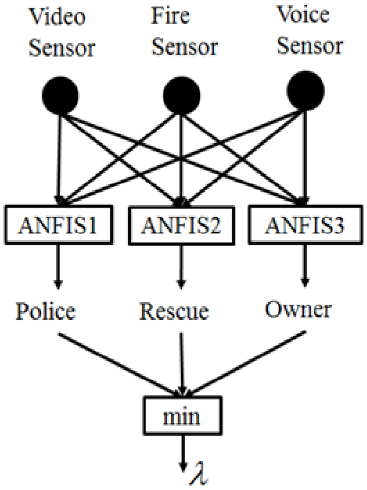

Figure 4. MANFIS for Dynamic Home Security.

For the sample scenario, five layers of neural networks resulting from the ANFIS have been provided in Figure 6. Effect of threshold 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.

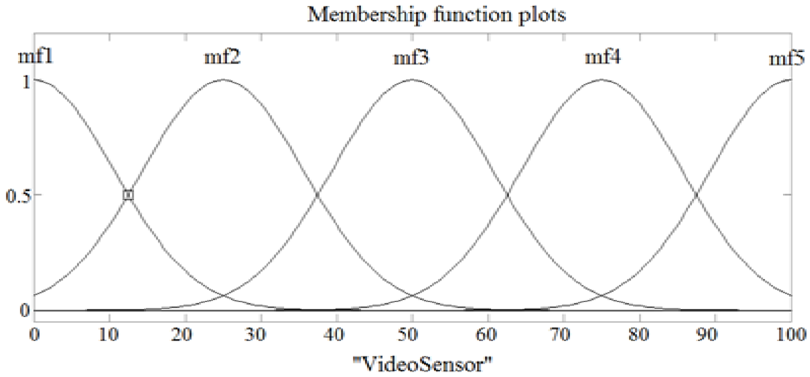

Figure 5. Member Functions of “Video sensor”.

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.

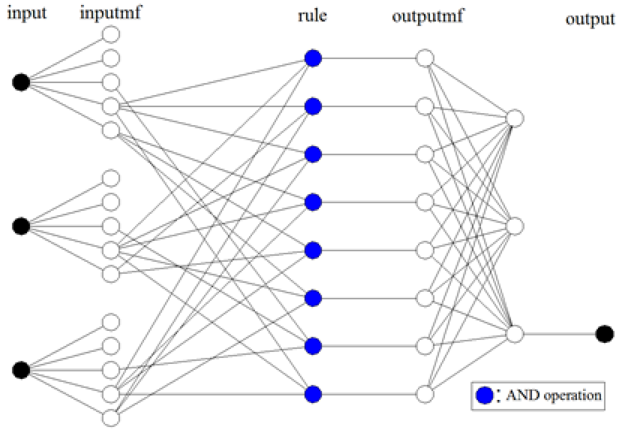

Figure 6. ANFIS structure for sample scenario

After completing the training of multiple ANFIS, the multiple outputs are solved by using the formulation of (1). Since the outputs “Owner” and “Rescue” belongs to the set of “the larger the better,” its membership function should take the form of (2); and the output “Police” has a nominal target, so it will take the membership function (4). In order to determine these membership functions, the maximum and minimum for individual output must be obtained. Maximum and minimum of outputs can be obtained by formulating single objective programming problems for individual responses, and solving the problems with any derivative-free algorithm. Alternatively, they can also be subjectively determined according to 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 as the minimum and maximum of this output, respectively. Similarly, the minimum and maximum of “Police” are set as 70 and 91, respectively. In Figure 7, 3D graph show the relationship between voice sensors, fire sensors and output threshold for rescue. Effect of threshold values is represented very well than simple fuzzy logic based output.

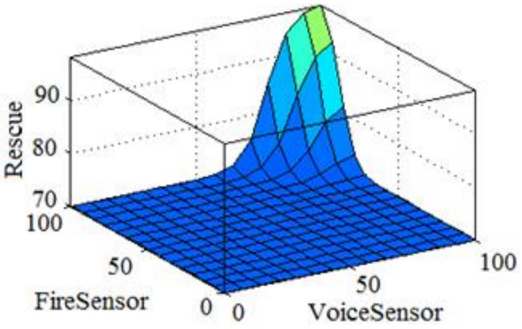

Figure 7. “Rescue” surface for fire and voice sensor.

In Figure 8, 3D graph show the relationship between voice sensors, fire sensors and output threshold for police. It is more reasonable than the relationship by simple fuzzy logic.

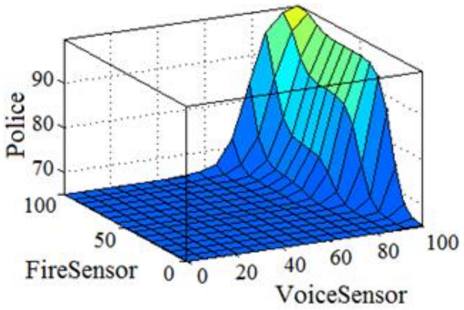

Figure 8. “Police” surface for fire and voice sensor.

Figure 9 represents the relationship between voice sensors, fire sensors and output threshold for owner. It is similar to that of simple fuzzy logic. Figure 10 shows the relationship between voice sensors, video sensors and output threshold for police. It is more reasonable than the relationship by simple fuzzy logic. In Figure 11, 3D graph show the relationship between voice sensors, video sensors and output threshold for Owner. It is similar to that of simple fuzzy logic. From the sample scenario, it is observed that ANFIS based home security system provides more flexibility to detect different nature of threats and respective outputs.

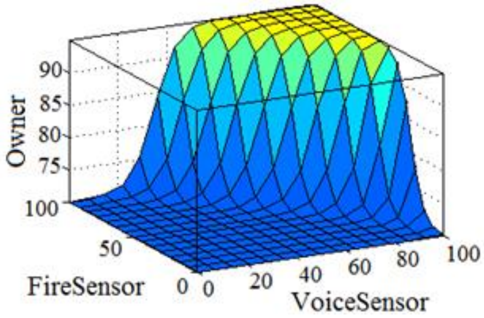

Figure 9. “Owner” surface for fire and voice sensor

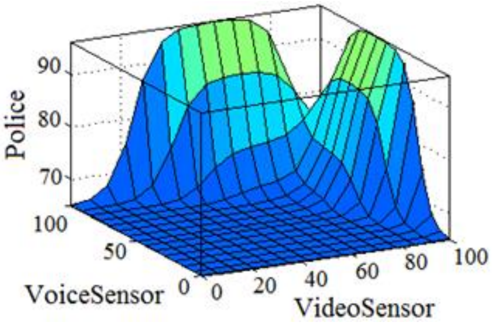

Figure 10. “Police” surface for video and voice sensor.

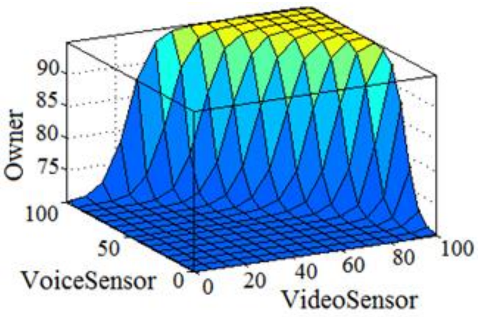

Figure 11. "Owner" surface for video and voice sensor

5. Concluding Remarks

This study used a neuro-fuzzy network, multiple ANFIS, to model a multiple output system. Multiple ANFIS provides the advantage of modeling a nonlinear and complicated system without the need of finding suitable functional forms for the system, and its neural network learning ability also equips multiple ANFIS with high efficiency in smart home security system modeling. It was observed that using this proposed concept, a better and flexible home security is provided than simple fuzzy logic based method. Proposed system inherits the properties of ANFIS and thus provides intermediary values as compare to Boolean logic bi-value outputs. However, since we use the nonparametric regression tool for multiple ANFIS to model outputs, exact functional forms of outputs are not known and hence derivative-based optimization cannot be directly applied to obtain the optimal solution. Therefore, we will use a genetic algorithm as well as a numerical method to search optimal solutions on the output surfaces in further research.

References

[1] P. M. L. Chan, R. E. Sheriff, Y. F. Hu, P. Conforto, C. Tocci and G. Losquadro, "Mobility management incorporating fuzzy logic for a heterogeneous IP environment", IEEE Communications Magazine, vol. 39, no. 12, **(2001)**, pp. 42-51.

[2] C. B. Cheng, "Multi-response optimization based on a neuro-fuzzy system", Neural Network World, vol. 10, **(2000)**, pp. 545-551.

[3] G. Edwards and R. Shankar, "Microcellular handoff using fuzzy logic techniques", Wireless Networks, vol. 4, **(1998)**, pp. 401-409.

[4] G. Feng, "A Survey on Analysis and Design of Model-Based Fuzzy Control Systems", IEEE Transactions on Fuzzy Systems, vol. 14, no. 5, **(2006)** October, pp. 676-697.

[5] G. Gao, and K. Whitehouse, "The Self-Programming Thermostat: Optimizing Setback Schedules based on Home Occupancy Patterns", Proceedings of BuildSys'09, **(2009)** November 3, Berkeley, CA, USA.

[6] M. Ghorbel, M. Segarra, J. Kerdreux, R. Keryell, A. Thepaut and M. Mokhtari, "Networking and Communication in Smart Home for People with Disabilities", Computers Helping People with Special Needs, Springer Berlin / Heidelberg, vol. 624, **(2004)**.

[7] J. Hou and D. C. O'Brien, "Vertical handover-decision-making algorithm using fuzzy logic for the integrated radio and OW system", IEEE Transactions on Wireless Communications, vol. 5, no. 1, **(2006)**, pp. 176-185.

[8] J. S. R. Jang, "ANFIS: Adaptive network based fuzzy inference system", IEEE Transactions on Systems, Man and Cybernetics, vol. 23, no. 3, **(1993)**, pp. 665-685.

[9] Y. Kim, H. Kim, S. Lee and K. Lee, "Ubiquitous Home Security Robot based on Sensor Network", Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'06) **(2006)**.

[10] P. Leijdekkers, V. Gay and E. Lawrence, "Smart Homecare System for Health Tele-monitoring", Proceedings of the First International Conference on the Digital Society, IEEE Computer Society, **(2007)**.

[11] V. Nicks, "AI Enhances the Smart Home Security System", http://artificialintelligence.suite101.com /article.cfm/ai_enhances_the_smart_home_security_system, **(2009)**.

[12] B. C. Popescu, B. Crispo, A. S. Tanenbaum and F. L. A. J. Kamperman, "A DRM Security Architecture for Home Networks", Proceedings of the 4th ACM workshop on Digital rights management, **(2004)** October 25, Washington, DC, USA.

[13] S. Z. Reyhani and M. Mahdavi, "User Authentication Using Neural Network in Smart Home Networks", International Journal of Smart Home, vol. 1, no. 2, **(2007)** July.

[14] R. J. Robles and T. H. Kim, "Applications, Systems and Methods in Smart Home Technology: A Review", International Journal of Advanced Science and Technology, vol. 15, **(2010)**.

[15] M. A. Saeed, M. S. Khan, K. Ahmed and U. Farooq, "Smart Home Security System using Fuzzy Logic", International Journal of Scientific & Engineering Research, vol. 2, no. 6, **(2011)** June.

[16] D. D. Spinellis, "The information furnace: consolidated home control", PersUbiquitComput, vol. 7, **(2003)**, pp. 53-69.

[17] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its application to modeling and control", IEEE Transactions on Systems, Man, and Cybernetics, vol. 15, **(1985)**, pp. 116-132.

[18] Y. Tseng, Y. Wang and K. Cheng, "An Integrated Mobile Surveillance and Wireless Sensor (iMouse) System and Its Detection Delay Analysis", MSWiM'05, **(2005)** October 10-13, Montreal, Quebec, Canada.

* Corresponding author: Jeong-Gi Lee, Ph.D.
Korea Electronics Technology Institute, Korea
E-mail: jklee@keti.re.kr

Authors

Sang- Hyun LEE

He received the BS and MS in Department of Computer Engineering from Honam University. in 2002 and 2004, respectively. He received Ph.D. degrees in Computer Science from Chonnam National University. in 2009. He has been a professor at Honam University. since 2012. His research interests include artificial intelligence, Software Engineering, Early Warning System, claim analysis, intelligence automotive.

Jeong-Gi Lee

He received a Ph.D. Managerial researcher at the Department of IT Convergence Technical Support Center from Korea Electronics Technology Institute in Korea. His theoretical work began at Chosun University as a Computer Science, and then expanded into embedded Software, network security, and healthcare

Kyung-li Moon

He received a Ph.D. Ph.D, is a professor at the Department of Computer Engineering, Honam University in Gwang-Ju, Korea. His theoretical work began at Seoul University as a statistical computing scientist, and then expanded into complexity science, chaos theory, and cognitive science generative sciences.