Journal of Mobile Multimedia, Vol. 8, No.3 (2012) 181-203

FUZZY TECHNIQUES FOR ACCESS AND DATA MANAGEMENT IN HOME AUTOMATION ENVIRONMENTS

MARIO COLLOTTA, VINCENZO CONTI, GIOVANNI PAU, GIANFRANCO SCATA'

Facoltà di Ingegneria, Architettura e delle Scienze Motorie
Università degli Studi di Enna - Kore
Cittadella Universitaria, 94100 Enna, ITALY
{mario.collotta, vincenzo.conti, giovanni.pau, gianfranco.scata}@unikore.it

SALVATORE VITABILE

Dipartimento di Biopatologia e Biotecnologie Mediche e Forensi
Università degli Studi di Palermo
Via del Vespro, 90127 Palermo, ITALY
salvatore.vitabile@unipa.it

Received November 1, 2011
Revised May 25, 2012

Home Automation Environments are characterized by the integration of electronic devices as well as by the performance of communication and control systems. Environment infrastructure has to meet several requirements including Quality of Service (QoS), safety, security, and energy saving. However, Home Automation deals with complex environments, so that advanced data management systems are required to meet the above constraints. Fuzzy Logic based techniques can be successful used to improve system performance management. This work proposes and describes the use and application of fuzzy rules on a two-tiered architecture integrating a biometric authentication module and communication real-time constraints. The goal is to combine the advantages of wired and wireless networks as well as the biometric recognition accuracy to increase the flexibility and the performance of the proposed deadline oriented architecture. The experimental results of the user authentication module, the energy consumption module and the scheduling module for real-time mobile communication are also outlined.

Key words: Wireless Sensor Networks, Real-time scheduling, Biometric Authentication, Data Management, Fuzzy Techniques.
Communicated by: D. Taniar

1 Introduction

The popularity and the evolution of mobile computing devices together with fast affordable mobile networks have increased the range and the complexity of mobile multimedia applications and services provided to end-users. The astonishing growth in number, types, novelty and complexity of mobile multimedia applications and services require advanced data management systems. In this scenario,

there is an increasing demand to protect data and resources from unauthorized access heterogeneous mobile and multimedia devices. Conventional authentication procedures, based on the simple username-password pair, are insufficient to provide a suitable security level for those applications requiring security and privacy on data and services access.

Biometrics plays an important role in surveillance and security applications. Biometric devices and sensors surrounding people are capable to acquire biometric traits in both obtrusive and unobtrusive way. Environments can be equipped with contact, contact-less and at-a-distance sensors. Contact sensors require user active cooperation for biometric trait acquisition. Contact-less devices include all sensors that require a short user distance for biometric traits acquisition. At-a-distance sensors can acquire biometric traits from long distance and they do not require active user collaboration. As example, fingerprint acquisition involves contact sensors or contact-less sensors, iris acquisition involves contact-less sensors or at-a-distance sensors, while voice acquisition involves contact-less or at-a-distance sensors, as well. Biometric systems automatically verify or identify involved subjects using acquired human biometric traits. A typical biometric authentication system requires an enrolment phase for storing user biometric templates and a verification or identification phase for matching acquired biometric traits against the stored templates [1].

Wireless technologies in multimedia environments increase flexibility but pose challenges to the design of security strategies to meet real-time constraints. The network infrastructure shall implement advanced Quality of Service (QoS) mechanisms and policies to guarantee high performance for both wired and wireless communication tasks. Due to heterogeneous mobile devices involvement and interaction, Home Automation environments represent one of challenging application fields. Smart homes are characterized by the integration of electronic devices, and communication and control systems. A smart home has to meet several requirements including: (*i*) safety, i.e. the protection from possible malfunctions; (*ii*) security, i.e. authentication, authorization and data protection; (*iii*) energy saving, i.e. a smart mechanism to reduce power consumption.

Most of the above functions can be controlled by a system characterized by the coexistence of electronic, computer and automation equipment managed through smartphones or tablets. While factory automation represents a steady market thanks to available financial resources, home automation market is almost stationary because lower budgets do not allow Home and Building Automation systems diffusion to a great number of private users.

This work describes the use and the application of the fuzzy logic based techniques on a two-tiered architecture integrating a biometric authentication module. The first tier is a wireless network, organized in Home Automation Cells (HAC), each of one served by a Cell Coordinator integrating several modules (Ethernet Module, 802.11 Module, 802.15.4 Module, Scheduling Module, Power Consumption Fuzzy Controller, and Biometric Fuzzy Authentication Module). The second tier is a wired backbone. The goal is to combine the advantages of both wired and wireless networks as well as the reliability of biometric user authentication to increase flexibility and performance of the proposed mobile multimedia architecture. With more details, it will be possible to use the wired network for highest critical tasks, the wireless network to cut maintenance costs and increase network flexibility, biometric traits to increase user authentication accuracy.

The information exchange over wired and/or wireless networks anticipates the implementation of a complex, distributed and well-structured mobile multimedia service system. This implies a practical technology configuration, delivering services based on context sensitivity. Many methodologies and techniques have to be merged together including embedded and intelligent computational devices, context awareness for user recognition and profiling and personalization of services to design such environments. The paper also outlines some experimental result in terms of user authentication accuracy, energy consumption and data transmission management.

The paper is organized as follows. Section 2 reports the main literature works on fuzzy techniques for the wireless sensor networks and secure access. Section 3 describes the proposed architecture for

mobile multimedia management. Section 4, Section 5 and Section 6 analyze the proposed user authentication module, the energy consumption module and the scheduling approach for real-time mobile communication, respectively. Section 7 outlines the performance evaluation of the proposed architecture. Finally the conclusions are reported in Section 8.

2 Related Works

In the follows, some of the main literature works based on the well-known fuzzy techniques have been reported.

2.1 Fuzzy Techniques in Wireless Networks

Fuzzy approaches are used in Wireless Networks especially in Wireless Sensor Networks (WSNs) scenarios, where sensor nodes are powered by batteries with limited capacity. Power consumption in Wireless Sensor Networks (WSNs) is an interesting research field. To this end, fuzzy logic can be used, through several and different approaches, in order to prolong network life time. In [27] the authors propose a fuzzy logic approach to perform cluster-head election based on energy, concentration and centrality. Appropriate cluster-head election can drastically reduce power consumption and, at the same time, increase network lifetime. This mechanism allows to properly deciding only some nodes to communicate with the base station in order to reduce power consumption. These nodes are called cluster-heads and after a gathering phase, during which they collect information detected by their cluster nodes, they send aggregated data to the base station. In [28] the authors try to resolve energy saving issue in WSNs focusing on hierarchical clustering routing protocol problem. Clustering mechanism helps to reduce the complexity of network overhead that is strictly related to number of nodes inside the network. Authors used a fuzzy search algorithm in order to simplify cluster formation and cluster head selection. Another technique for cluster head selection to reduce power consumption in WSNs is described in [29]. As known, one of the most famous clustering algorithms is LEACH [30]. It elects cluster heads based on a probability model. The authors of [29] improved LEACH algorithm using fuzzy logic taking into account some parameters like battery level, distance and node density in order to prolong nodes lifetime. In [31] the authors show a wireless sensor network architecture where each node is empowered by a fuzzy logic system for environment monitoring. In this case, fuzzy logic is used in order to prolong sleep times when there is no data to transmit. Work shown in [32] deals with a mechanism for power consumption management using fuzzy logic to dynamically vary sampling times of wireless sensor nodes. The main aim of this work is to wake-up sensor nodes only in case of real need increasing energy savings. Sampling times calculation is made through information coming from the WSN. All these information are processed through several fuzzy inference rules in order to determine the new sampling period. In [26], the authors use fuzzy logic for QoS management in Wireless Sensor/Actuator Networks (WSANs). A fuzzy logic controller is used inside each source sensor node to adapt sampling period to the deadline miss ratio associated with data transmission from the sensor to the actuator. The deadline miss ratio is maintained at a pre-determined desired level in order to achieve the required QoS. Another research area related to power consumption optimization is routing. In [33] the authors propose a fuzzy logic based approach for energy-aware routing decisions. Routing protocols often use fixed metrics for making energy-aware decisions where short multiple-hops reduces transmission power but, at the same time, reduces the energy of a larger number of nodes involved. Fuzzy logic has potential for dealing with conflicting situations and imprecisions in data using heuristic human reasoning without needing complex mathematical modelling. An energy efficient unequal clustering scheme for large scale wireless sensor networks is presented in [34]. The authors worked on energy efficient clustering scheme and inter-cluster routing protocol to balance power consumption of each node and prolong network lifetime as long as possible. Inside a cluster, fuzzy logic is used to determine the cluster head through some local information like

energy level, distance to base station and local density. The inter-cluster routing is performed by an application of Ant Colony Optimization (ACO) that realizes the energy-aware routing between cluster heads and base station, reducing the energy consumption of cluster heads.

2.2 Fuzzy Techniques in Biometric Authentication

Due to the advantages offered by the fuzzy logic techniques for enhancing the recognition accuracy in the field of multimodalities, several approaches are proposed in the current literature to improve biometrics fusion using fuzzy logic. In [3] the authors present a multi-biometric verification system that combines speaker verification, fingerprint verification with face identification. Fusion of the three systems by majority voting gave a relative improvement of 48% over speaker verification (i.e. the best-performing biometric). Fusion by weighted average scores produced a further relative improvement of 52%. They propose the use of fuzzy logic decision fusion, in order to account for external conditions that affect verification performance. The fuzzy logic framework incorporates some external factors relating to face and fingerprint verification and achieved an additional improvement of 19%. In [4] the authors utilize the physiological attributes (face, ear and iris) along with soft biometric information (gender, ethnicity and eye colour). A fuzzy fusion mechanism for robust and reliable multimodal biometric based security systems is developed. The proposed fuzzy fusion scheme adopts rank, match score and soft biometrics information as the input and produces final identification decision via a fuzzy rule-based inference system. The experimental results show that the fuzzy fusion method can provide us faster, higher and more reliable recognition performance than conventional unimodal methods. In [5] the authors propose a novel fusion protocol based on fuzzy fusion of face and voice features for checking liveness in secure identity authentication systems based on face and voice biometrics. Liveness checking can detect fraudulent impostor attacks on the security systems, and ensure that biometric cues are acquired from a live person who is actually present at the time of capture for authenticating the identity. The proposed fuzzy fusion of audio visual features is based on mutual dependency models which extract the spatial-temporal correlation between face and voice dynamics during speech production. Performance evaluation in terms of Detector Error Tradeoff (DET) curves and Equal Error Rates (EERs) on publicly available audiovisual speech databases shows a significant improvement in performance of proposed fuzzy fusion of face-voice features based on mutual dependency models over conventional fusion techniques. In [6] the authors conducted detailed studies to model individual driving behavior in order to identify features that may be efficiently and effectively used to profile each driver. Feature extraction techniques based on Gaussian Mixture Models (GMMs) were proposed and implemented. Features extracted from the accelerator and brake pedal pressure were then used as inputs to a Fuzzy Neural Network (FNN) system to ascertain the identity of the driver. Two fuzzy neural networks, namely, the Evolving Fuzzy Neural Network (EFuNN) and the Adaptive Network-based Fuzzy Inference System (ANFIS) are used to demonstrate the viability of the two proposed feature extraction techniques. The performances were compared against an artificial Neural Network (NN) implementation using the Multilayer Perceptron (MLP) network and a statistical method based on the GMM. Extensive testing was conducted and the results show great potential in the use of the FNN for real-time driver identification and verification. In addition, the profiling of driver behaviors has numerous other potential applications for use by law enforcement and companies dealing with buses and truck drivers. In [7] the authors proposed a fuzzy multimodal technique capable of guaranteeing the desired level of security, while keeping under control the high costs typically associated to some biometric authentication devices. Specifically, a fuzzy controller within a palette of authentication techniques to continuously check and confirm its trust in user identity tasks is described.

3 System Architecture and Requirements

Automation environments are characterized by applications in which small embedded devices, like sensors and actuators, spend most of their time in a "sleep" state and wake up with a given periodicity (known "a priori") or when a critical event occurs. To design such environments, many methodologies and techniques have to be merged together, networking intelligent computational devices, strong authentication module, data/resources/services remote management modules, and so on.

3.1 System Requirements

In order to effectively use wireless networks for home automation communication, a number of requirements have to be met. In the following, system requirements driving the design of the proposed architecture are focused:

- Predictability & simulation of system performance: the system shall provide tools allowing the End User to simulate its network environment and determine, in advance, end-to-end system performance (across multiples cells and wired and wireless sections): end-to-end latency (min, max, average), jitter, throughput;
- Quality of Service (QoS) provisioning: the system shall implement advanced QoS mechanisms and a clear policy to ensure guaranteed performance for predefined processes for both wired and wireless communication. The system shall provide high QoS degree for all kind of operations (wired or wireless) involved in the system;
- Timing requirements between command giving and its execution should be met: should meet the timing requirements of its applications. In particular, the system shall target those applications which have strict timing requirements, between command giving and its execution;
- Real-time communication guaranteed for wireless nodes: nodes need to communicate in real-time. Real-time requirements like latency or jitter depends on the application;
- Differentiated QoS classes: as end-users require multiple types of traffic with different real-time or security constraints within the same network, the system should support different QoS class for the different classes;
- Resources allocation should be provided for communications between coordinators and end nodes: to grant several system resources like bandwidth, reaction time etc., the system should provide a mechanism to allow needed resources allocation to a node;
- Real-time traffic classes: the system shall handle traffic flows according to real-time requirements. Better Scheduling Algorithms to increase nodes performance;
- The system shall enable the use of wireless protocols in home automation environments: home automation environments are increasingly characterized by noise and multiple propagation behavior. The system shall be usable in such home automation environments;
- The system shall support multiple wireless cells: when a large area must to be covered, multiple wireless connection points will be required to provide coverage;
- High communication reliability: the system shall provide high reliability in terms of communication services. The message error rate shall be kept acceptable for the automation-application. This should be ensured both for wireless and wired communication (backbone).
- High availability of the backbone: the backbone of the system shall have at least the availability of the wireless part of the system;

- Real-time communication within the backbone: the backbone of the system shall provide real-time latency guarantees that are very small compared to the overall end-to-end guarantees required by the system.
- Reducing non-determinism in wireless communication: the system should reduce the sources of non-determinism as much as possible on the wireless channel and on the wired medium;
- Fault tolerance: the architecture shall prevent performance degradation in case of fault to any part of the system. It is mandatory to conduct a fault analysis of the system in order to provide fault tolerance mechanisms. Moreover, the system shall be self-healing: a communication system is self-healing, if the system detects communication errors and fixes these errors by its own means;
- The system shall enable device interoperability and interchangeability: devices developed by different manufacturers shall interoperate with each other within the architecture. It shall be possible to replace a component from one manufacturer by an equivalent device from other manufacturer;
- User Authentication and security*:* network security is mandatory feature to allow adoption of wireless communications. The system shall provide solutions to insure end-to-end security in the context of a heterogeneous network (wired and wireless sections). Security shall cover strong authentication, integrity, confidentiality (high end devices) and filtering of unauthorized protocols (firewall).

3.2 The proposed two-tiered Architecture

The following reasons drive our architectural proposal:

- actual home automation systems use wired connection. It's useful the integration of wireless control into home automation which already provides a wired network;
- it is currently unfeasible to manage all traffic flows to a wireless network;
- some very important system requirements should be meeting.

This work proposes a two-tiered architecture (Figure 1). The first tier is a wireless sensor network organized in Home Automation Cells (HAC). WSNs can continuously monitor environments with less human effort and are low cost and low power. Each HAC is served by a Cell Coordinator that provides several modules:

- Ethernet [39] Module: it allows wired connection between each Home Automation Cell and the Ethernet Backbone;
- IEEE 802.11 [38] Module: it allows communication between mobile devices (smartphones or tablets) and the Home Automation Cell. Through this module, people can authenticate themselves inside the home automation system and subsequently monitor data detected by sensor nodes and, in case of need, send commands.
- IEEE 802.15.4 [37] Module: through this module, the coordinator receives and processes data detected by RFD nodes (Reduced Function Devices) placed inside the HAC. It also allows sending user commands or system commands to RFD nodes.
- Scheduling Module: this module is a QoS manager for Real-Time (RT) communications performing a schedulability test for admission control in order to accept a new traffic flow.
- The Power Consumption Fuzzy Controller is necessary on order to ensure another

fundamental WSNs requirement: power consumption management. This module dynamically manages sampling times in order to prolong sleeping periods of RFD nodes. In this way, it is possible to improve energy savings and, at the same time, prolong batteries and network lifecycle.

Biometric Fuzzy Authentication Module: this module performs a strong user authentication process based on fingerprint traits. The goal is to manage data, resources and services inside the architecture through remote control.

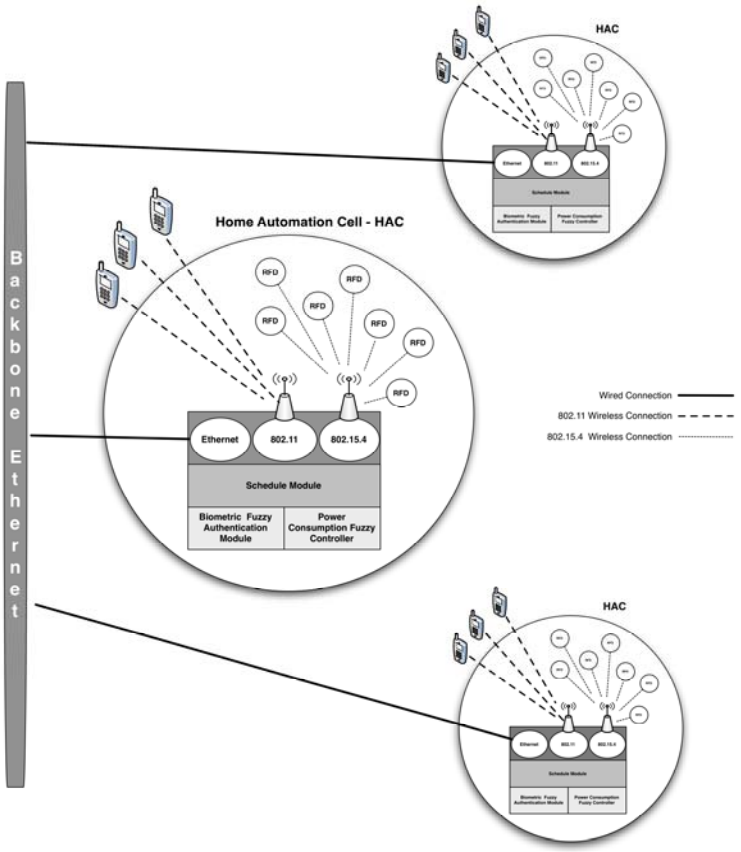

Figure 1. The proposed two-tiered architecture integrating a strong biometric authentication module

The second tier is a wired backbone. So, it is possible to combine advantages of both wired and wireless networks (i.e. it will be possible to use the wired network for highly critical tasks which could not be implemented over an unreliable medium, while the wireless network can be used to cut maintenance costs and increase network flexibility).

4 The Fingerprint Authentication Module

The Automation Device (sensor and actuator), combining two fingerprint authentication systems and fuzzy techniques, is described to increase the security mechanism in a proposed multimedia environment. With the proposed approach some biometric unimodal authentication system limitations

have been reduced. The used fusion techniques are based on fuzzy logic considering fingerprints image quality as in particular, two fusion methods have been tested: the first one implements a decision level fusion, the second one implements a matching score fusion. The proposed approach uses the images quality as goodness index, as the authors in [18], but nothing weight is obtained from fuzzy rules to characterize the system phases. The developed approach can be adopted with general multimodal authentication systems involving different biometric features.

Multimodal biometric systems are a recent approach developed to overcome common problems of unimodal biometric authentication systems. These systems demonstrate significant improvements over unimodal biometric systems, in terms of higher accuracy and high resistance to spoofing [9], [11], [16] and [17]. A typical multimodal authentication system is composed by two or more parallel unimodal systems and a fusion module. Fusion module takes two or more data and combines them in order to obtain the classification result: impostor or genuine user.

In this work the fuzzy module estimating input image quality has been added to a traditional Automated Fingerprint Authentication System (AFAS). Image quality has been estimated through the analysis of two specific parameters of the image: the number of *erased segments* (*ES*) and the number of the *candidate minutiae* (*CM*). The *eliminated segments* are portions of fingerprint too much noisy, so no useful information can be found inside them. The adopted matching algorithm is based on a structural matching executed on similar geometric forms between input fingerprint and the stored template. In particular triangle forms, produced by triplet of minutiae, have been used to perform the matching. The produced score by a single AFAS is named "*recognition degree*".

With regard to the fusion strategies, they can be grouped into two main categories [15], [16]: *pre-mapping fusion* (before matching) and *post-mapping fusion* (after matching). The first strategy deals with the *sensor data fusion level* and *feature vector fusion level.* The second strategy can be realized through the *decision level fusion*, based on some algorithms which combine single decisions for each component system, and through the *matching score level fusion,* which combines the matching scores of each component system. Figure 2 shows the blocks scheme of a recognition process with many fusion levels.

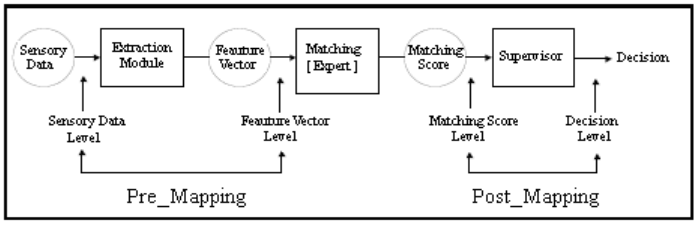

Figure 2. Distinction of the different fusion levels: on the left the pre_mapping fusion, on the right the post_mapping fusion (used in this work).

In this paper the post_mapping fusion strategies have been implemented and evaluated using two fingerprints based subsystems using the fuzzy logic principles and methods to combine the information coming out by two AFAS. The whole recognition system also incorporates the knowledge about the image quality [21]. As started before, image quality is based on both *ES* and *CM* features. Experimental trials aimed to find a global image Goodness Index (*GI*) in term of *ES* and *CM* values have been performed. Figure 3 shows the experimental obtained results about *ES* and *CM* ranges with relative membership function values and the membership function range of the *GI*.

The Goodness Index *GI=f(ES, CM)* is obtained applying "*moment defuzzify function*" [23]. The *moment defuzzify function* returns a defuzzified floating point value, which represents the defuzzified fuzzy set using the first moment of inertia function. This is a good method to use in many processes since it tends to smooth out the fuzzy region [23]. Figure 4 shows three different fingerprint images with a different *GI* value. The image on the left is a fingerprint of good quality, *GI=82.01*, on the center a fingerprint of medium quality, *GI=55.01*, and on the right a fingerprint of bad quality, *GI=0*.

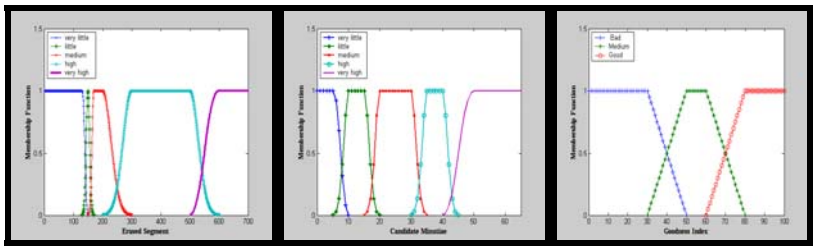

Figure 3. *ES*, *CM* and *GI* ranges. On the left *ES* values, on the center *CM* values and on the right *GI* values.

Figure 4. Two typical fingerprints of different quality. On the left a fingerprint image of good quality (*GI=82.01*), on the center a fingerprint image of medium quality (*GI=55.01*), while on the right a fingerprint image of bad quality (*GI=0*).

4.1 Fuzzy Fusion Techniques

Decision level fusion

The authentication system is composed by two modules AFAS to realize a multimodal authentication system combining the obtained scores from the single systems (see Figure 5). With more details, the proposed authentication system is composed by *AFAS1* subsystem that performs index fingerprint processing and recognition, and by *AFAS2* subsystem that performs the middle finger's fingerprint recognition and processing.

The proposed and implemented fusion module uses the fuzzy logic to combine the scores products by two subsystem AFAS [11], [19]. Fuzzy logic processes imprecise information like human thinking and it allows to obtain intermediate values between true and false, accepted and refused, by partial membership set.

A fuzzy inference system composed of two inputs variables and one output variable has been implemented. The output represents the decision taken by whole system.

The fuzzy logic conditions are formulated by a group of sixteen fuzzy rules. Some of the used rules used with this index quality are the following:

1. if *recognition degree of AFAS1* is high and *recognition degree of AFAS2* is high then final decision is *genuine user;*
2. if *recognition acknowledgment degree of AFAS1* is low and *recognition degree of AFAS2* is low then final decision is *impostor user;*
3. if *recognition degree of AFAS1* is medium low and *recognition degree of AFAS2* is medium low then final decision is *indecision.*

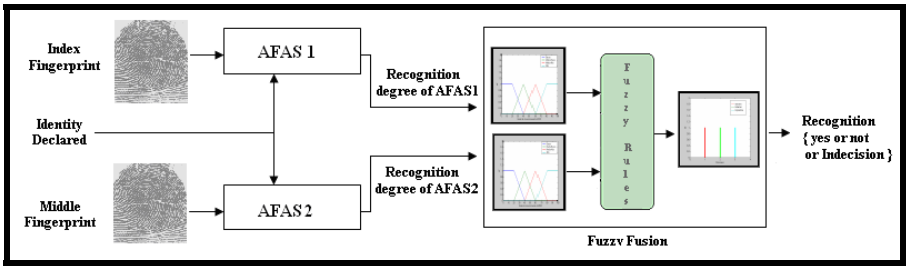

Figure 5. The general scheme of the proposed system architecture with decision fusion.

Matching score level fusion

The proposed architecture integrates two AFAS modules, while the fusion is implemented combining both the AFAS matching scores and the fingerprint image quality measures.

The fusion has been obtained by a fuzzy system with four inputs and one output. The output represents the decision of the whole system. The fuzzy system uses the knowledge base built with above fuzzy rules. Each rule has the following common guidelines:

1. if the input images have good quality and fingerprints are very similar to the stored fingerprints then certainly the user is who he/she claims to be.
2. if the input images have good quality and fingerprints are not very similar to the stored fingerprints then certainly the user is an impostor".
3. if AFAS1 works with an input bad quality image and AFAS2 works with an input good quality image then the AFAS2 decision will be more discriminant than AFAS1.

The Figure 6 shows the scheme of the proposed architecture with matching score level fusion.

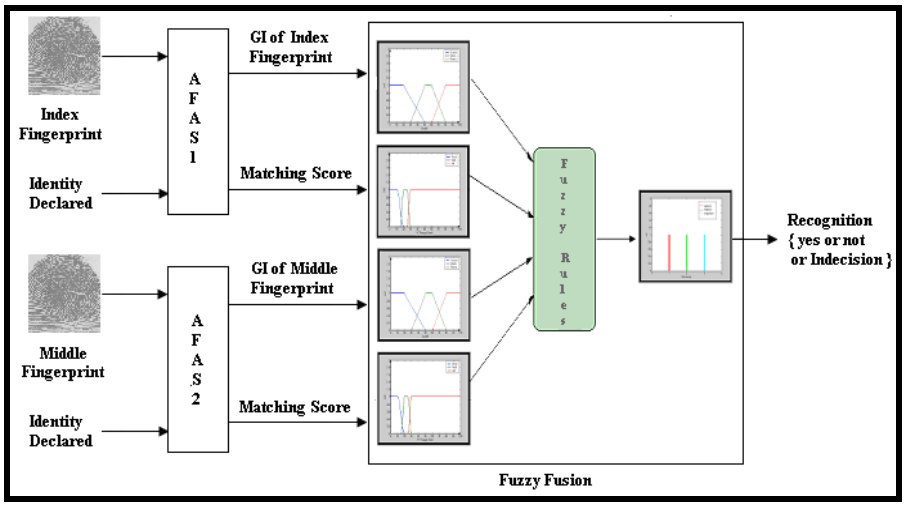

Figure 6. General scheme of the proposed architecture with matching score level fusion.

5 The Fuzzy Energy Consumption Approach Management

End nodes continuously work inside the monitored environment. In order to optimize power resources and, at the same time, increase devices lifecycle, it is necessary to develop an energy management paradigm to ensure network flexibility, adaptability and scalability. The idea is to realize a power consumption controller that can make decisions based on real-time constraints changes and environment real needs. The behavior is similar to WSN scenario, where it is not possible to determine "a priori" nodes behavior since they are often used to monitor sporadic events. However, traffic flows generated by WSNs can be considered as periodic [24]. The mechanism here proposed, called Fuzzy Logic Controller-Sampling Adapter (FLC-SA), manages network nodes sampling time in order to reduce power consumption and increase battery lifecycle. The FLC-SA manages nodes energy resources dynamically varying the sampling time through a fuzzy logic controller, based on information coming from the WSN. The FLC-SA is implemented inside a cluster coordinator, a Full Function Device (FFD) through which it determines when to increase or decrease end nodes (Reduced Function Devices – RFDs) sleeping times. A cluster tree topology has been considered, because it guarantees best performance in terms of reliability and energy savings [25], [26]. The flow-chart diagram, shown in Figure 7, explains how the FLC-SA works.

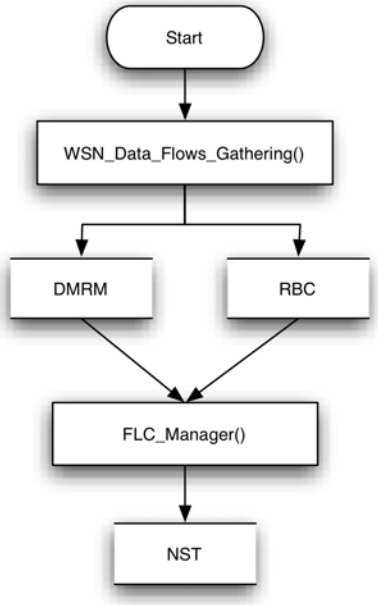

Figure 7. FLC-SA flow chart

The cluster coordinator receives data flows related to information detected (position values, temperature, pressure, humidity, etc.) through the *WSN_Data_Flows_Gathering()* function. Based on network performance (Deadline Miss Ratio Measured - DMRM) and end-nodes power consumption information (Remaining Battery Capacity - RBC), the fuzzy controller evaluates, through the *FLC_Manager()* function, the new end-devices sampling time. Based on predetermined "membership" functions [23], inputs are converted into "linguistic" values: Positive Big (PB), Positive Small (PS), Zero (ZE), Negative Small (NS), Negative Big (NB). Subsequently, an inference mechanism, based on several IF-THEN rules, determines the output linguistic value (PB, PS, ZE, NS, NB) representing the New Sampling Time (NST) that will be defuzzified with a centroid algorithm. Figure 8 shows how the fuzzy logic controller works.

Figure 8. Fuzzy logic controller functioning scheme

Instead, Figure 9 shows the inference mechanism functioning scheme.

NST		RBC				
		NB	**NS**	**ZE**	**PS**	**PB**
DMRM	**NB**	PB	PB	PB	PB	PS
	NS	PS	PS	PS	PS	ZE
	ZE	PS	ZE	ZE	ZE	NS
	PS	ZE	ZE	NS	NS	NB
	PB	NS	NS	NB	NB	NB

Figure 9. Inference mechanism general scheme

To better understand Figure 9, IF RBC value is NS (Negative Small) and DMRM value is ZE (Zero), THEN NST value will be ZE (Zero). Finally, this value is defuzzified into a numeric value, which represents the New Sampling Time (NST) of RFD nodes. In our algorithm, for each variable, a range of values has been defined. Therefore the range has been divided in sub-ranges (called fuzzy sets). Established that Deadline Miss Ratio Measured (DMRM) can assume values between 0 and 1.25, this range can be divided into fuzzy sets as shown in Figure 10.

NB	0	0.0015	0.03
NS	0.00265	0.0326	0.203
ZE	0.15	0.225	0.3
PS	0.25	0.5	0.7
PB	0.55	1.001	1.25

Figure 10. Deadline Miss Ratio Measured (DMRM) fuzzy sets

In other words, if the value of DMRM is between 0 and 0.03, it will be fuzzified as Negative Big (NB). At the same way, Remaining Battery Capacity (RBC) can assume values inside a range divided in fuzzy sets too, as shown in Figure 11.

NB	0	2	4
NS	0	4	8
ZE	4	8	12
PS	8	12	16
PB	12	16	20

Figure 11. Remaining Battery Capacity (RBC) fuzzy sets

So, if Remaining Battery Capacity has a value between 0 and 4, it will be fuzzified as Negative Big (NB). As seen previously, outputs are input functions. According to fuzzy logic, these functions are expressed through IF-THEN rules. To better understand, the following construct (from Figure 9) can be taken as model:

IF DMRM_1 ***is*** NB ***and*** RBC_1 ***is*** NS ***THEN*** NST_1 ***is*** PB

IF the DMRM value (measured by FFD node with ID number = 1) is Negative Big, and RBC value (related to FFD node with ID number = 1) is Negative Small, THEN the NST value (New Sampling Time for FFD node with ID number = 1) will be Positive Big. For each node, 25 fuzzy rules combined inside the controller using MAMDANI [35] triangular membership functions have been implemented.

6 The Scheduling Approach for Real-Time Mobile Communication

In the proposed architecture, a Quality of Service (QoS) management level and a Real-Time (RT) scheduling level are needed, in order to meet QoS and RT requirements. For each data packet transmission request coming from a wireless node, the system performs a schedulability test for Admission Control to accept a new traffic flow. If the request, added to system workload, respects a certain QoS level, it is admitted. Admission control and resource reservation depend on used scheduling algorithm. Therefore, the scheduling modules and the implemented admission control rules are described. First of all, it is necessary to classify traffic flows:

* *periodic real-time*: this traffic is characterized by regular arrival times and real-time constraints. Critical control activities, with hard time constraints aimed to guarantee regular activation rates, are executed;

* *aperiodic real-time*: this traffic flow has irregular and unpredictable arrival times. In this case, since there is not information about inter-arrival time, the system specifies real-time guarantees only to one-shot critical messages through a server process;

* *sporadic real-time*: this traffic does not have regular arrival pattern. However, the system can define a minimum inter-arrival time between two consecutive sporadic requests;

* *non-real-time*: this traffic has different arrival patterns and does not require strict real-time constraint.

An approach providing an integrated support for deadline-aware scheduling of periodic and aperiodic/sporadic traffic flows is proposed. The system schedules periodic traffic flows using Earliest Deadline First (EDF) algorithm [36] and aperiodic/sporadic flows through a Deferrable Server (DS) [36]. If period value is equal to the minimum inter-arrival time, the system could schedule corresponding sporadic flows using EDF. But, in hard real-time systems, the minimum inter-arrival time refers to worst case. Then, these suppositions are very strict in Home Automation System. In fact, when a sporadic flow occurs the system schedules it through a Deferrable Server, in order to avoid unnecessarily utilization of wireless channel bandwidth.

EDF is a dynamic scheduling algorithm that selects traffic flows according to their absolute deadlines d_i. Specifically, flows with earlier deadlines will be managed at higher priorities. Another time parameter is relative deadline D_i that represents the time interval measured from the arrival of the request within which data has to be transmitted. Considering a periodic transmission request arriving at time r_i, with relative deadline D_i equal to period T_i, the absolute deadline d_i can be defined as follow:

$$d_i = r_i + D_i \tag{1}$$

It is necessary to note that EDF does not make any specific assumption on the periodicity of the traffic; hence, it can be used for scheduling periodic as well as aperiodic flows, but in our approach the DS algorithm for aperiodic/sporadic traffic is used.

Deferrable Server algorithm creates a high priority periodic activity for servicing aperiodic requests. Like other periodic flows, the DS is characterized by a period T_s and a maximum transmission duration time C_s, in order to send an aperiodic/sporadic traffic flow; C_s is the server capacity. DS preserves its capacity if no requests are pending upon the invocation of the server. The capacity is maintained until the end of the period, so that aperiodic requests can be serviced at the same server's priority at any time, as long as the capacity has not been exhausted. At the beginning of any server period, the capacity is replenished at its full value. Thus, DS provides much better aperiodic responsiveness than polling [36], for example, since it preserves the capacity until it is needed. Also, shorter response times can be achieved by creating a DS having the highest priority among the periodic flows.

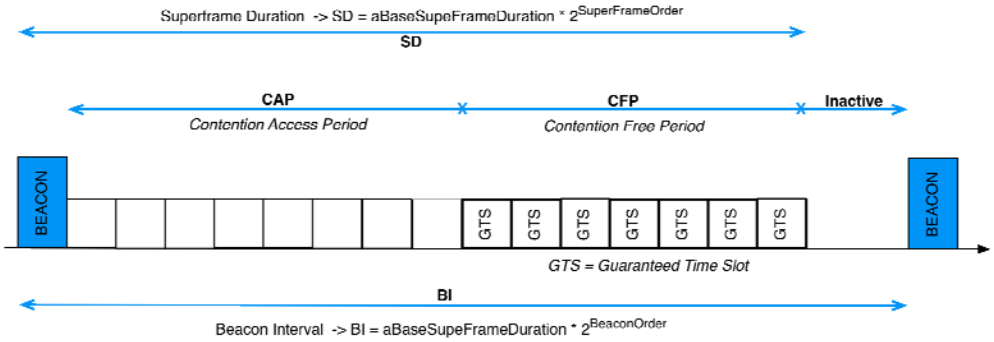

Figure 12. IEEE 802.15.4 Beacon Enabled transmission structure.

In the proposed wireless tier it should be possible to obtain numerous advantages. Due to the capability to use a higher number of nodes, the IEEE 802.15.4 [37] has been chosen. Specifically, the IEEE 802.15.4 Beacon Enable (BE) transmission structure (Figure 12) has been implemented in the proposed scheduling approach. During Contention Free Period (CFP), Guaranteed Time Slots (GTS) are allocated using EDF and DS algorithms, in order to send periodic and aperiodic/sporadic real-time flows. Also, in the Contention Access Period (CAP), no real-time traffic flows are scheduled through CSMA/CA protocol.

6.1 Admission Control Module based on EDF+DS scheduling approach

The proposed scheduling scheme is used in the Admission Control Module (ACM). At first, in order to guarantee or not each traffic request, the system evaluates traffic flows admission and, subsequently, it schedules the admitted flows. The ACM evaluates the acceptance of new flow when the flow specification is received. If resources have already been committed by earlier request, the new request may be rejected. In this case, the admission control notified the acceptation of the refuse to wireless node. This happens because the system can schedule a set of periodic requests using non-preemptive EDF algorithm if *Jeffay* theorem condition [37] (equation (2) and (3)) are met:

$$U_{tot} = U_P + U_S = \left(\sum_{i=1}^{n} \frac{C_i}{T_i} + U_S \right) \leq 1 \tag{2}$$

$$1 < i \leq n; \forall L, T_1 < L < T_n; L \geq C_i + \sum_{j=1}^{i-1} \left\lfloor \frac{L-1}{T_j} \right\rfloor C_j \quad (3)$$

The periodic traffic flows are represented by a set of periodic variables $\tau p = \{p_1, p_2, \ldots, p_n\}$, where $p_i = (C_i, T_i)$, sorted in non-decreasing order by period (i.e., for any pair of variables p_i and p_j, if i > j then $T_i \geq T_j$) and C_i is the transmission time for a periodic traffic flow generated by i[th] wireless node.

The equation (2) relates to system utilization (in terms of bandwidth, since this work deals with the transmission of packets), whereas the equation (3) refers to the system demand. The equation (2) defines that total bandwidth utilization must not exceed 1; U_P is the utilization factor for periodic traffic while U_S is the utilization factor for sporadic and aperiodic traffic flows (i.e. server utilization). The inequality in equation (2) refers to a least upper bound on bandwidth demand that can be achieved in an interval of length L. This interval starts when the periodic variable is invoked and ends before the relative deadline. Then, a set of variables is schedulable if the demand in the interval L is less than or equal to the length of the interval.

Considering the equation (4), for Deferrable Server $U_S = 1\text{-}U_P$, as $U_S = C_S / T_S$; hence, setting server period T_S, it is possible to calculate C_S value:

$$C_s = \frac{U_S}{T_S} = \frac{1 - U_P}{T_S} \quad (4)$$

7 Performance Evaluation

7.1 Authentication Accuracy

The performances of an authentication system are given in terms of error rates computed during the test phase. An optimal identity verification have False Acceptance Rate (FAR) =0% and False Rejection Rate (FRR) =0%. In other words, the purpose of an authentication system is to decide if a person is who he/she says to be [20].

The overall performance of an identity verification system is well characterized by the *Receiver Operating Characteristic* (ROC) curve [14], [20], which represents the FAR as a function of FRR or its complementary GAR=1-FRR (Genuine Acceptance Rate). The Equal Error Rate (EER: i.e. when FAR=FRR), is often used as the only performance measure of an identity verification method, although this measure gives just one point of the ROC.

The proposed strategies, described in previous sections, have been used to merge the results coming from two modalities. To evaluate algorithm performance the DB3 database of the FVC2002 [22] has been used. The database is composed by eight samples coming from one hundred users. The 800 images have 300*300 pixel dimension. The experimental results have been performed using the method of FVC competition to calculate FAR and FRR indexes [22].

The results show that the multimodal system performances are better than unimodal system. In addition, tests show that the matching score level fusion strategy gives better result than the decision level fusion ones. Figure 13 shows the performance of the proposed approach on DB3 using the ROC curves. In this figure the ROC curve of the unimodal system without filter [13] is depicted. The Equal Error Rate is about 13.7% when the decision level fusion is applied and about 11.8% when the matching score level fusion is applied. The Equal Error Rate of the unimodal system is about 18.5%, so that the matching score level fusion technique produces performance enhancement of about 30% on Equal Error Rate parameter.

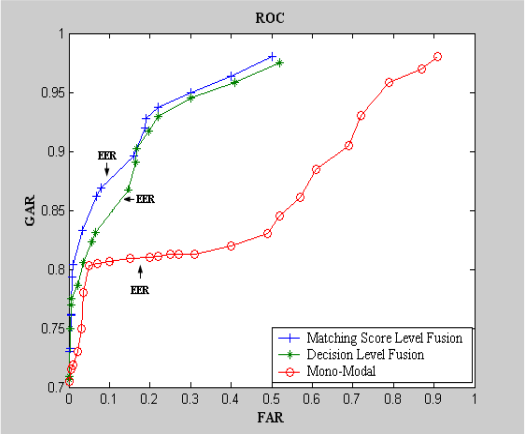

Figure 13. The ROC curves about our approach on FVC DB

7.2 Energy Consumption

In order to demonstrate advantages of our approach, several simulation campaigns were carried out, using True-Time simulator [40]. Total simulation time has been set to 540 True Time iterations (TTi). During a time slice, the Fuzzy Logic Controller-Sampling Adapter (FLC-SA) processes information coming from the WSN in order to determine new sampling period values. TTi parameter has been selected because time measure unit is strictly correlated with the hardware platform used. Start battery capacity is 20 mA. Figure 14 shows battery life cycle of a single sensor node using the FLC-SA. Results have been compared with a simulation campaign in which the network controller does not implement our algorithm. FLC-SA allows using longer a single sensor (about 300 iterations left after 540 TTi).

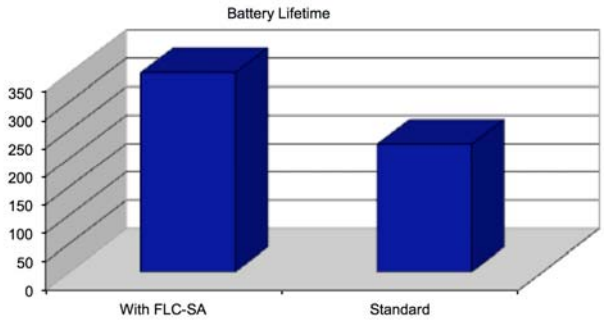

Figure 14. Battery Lifetime comparison

Figure 15 deals with energy savings in mA per minute of each sensor node battery. Results obtained after 540 TTi, show how it is possible to save on average 6 mA/min using the FLC-SA. In other words, energy consumption is lower and batteries last longer, as already shown in Figure 14.

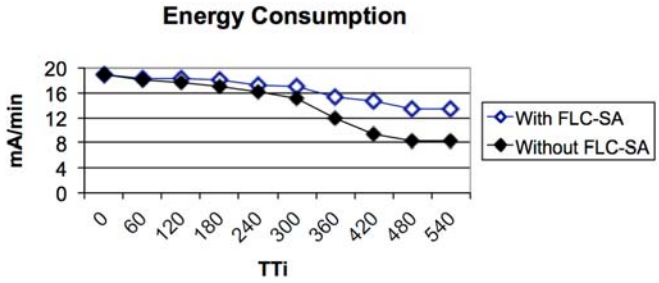

Figure 15. Energy Consumption

Finally, Figure 16 shows the percentage of alive nodes. After 540 TTi, about 50% of still active nodes have been measured using the FLC-SA in spite of the 30% obtained not using it.

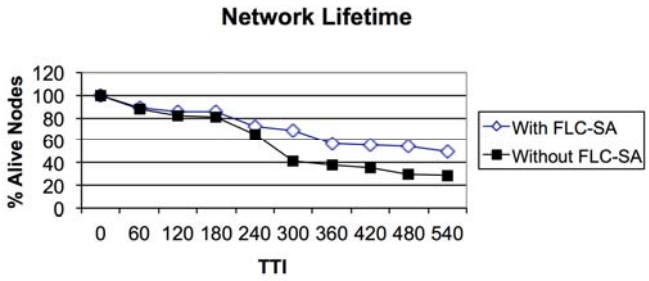

Figure 16. Network Lifetime with and without the use of the Fuzzy Logic Controller – Sampling Adapter (FLC-SA)

7.3 Data Transmission Management

OMNeT++ simulator [41] has been used to test the scheduling algorithm (EDF+DS) in an IEEE 802.15.4 scenario. Several simulations have been done to test the effectiveness and the correctness of the proposed scheduling approach. To evaluate traffic flows schedulability, for each simulation an ideal channel, free from noise and interference, has been assumed. Throughput and Deadline Miss values have been measured. A deadline miss occurs when a data packet does not reach its destination, it arrives late or it has been never sent. Simulations have been done using both the proposed approach and a standard star network topology in an IEEE 802.15.4 scenario. The simulated scenario consists of a central coordinator node, seven sensors and seven actuators. Packet size is 18Kb and data rate for each station at 180Kbps.

Moreover, considering Throughput (TH) (packet number successfully sent and received) and Workload (WL) (number of packets generated to be transmitted over the network), their ratio has been measured to evaluate network performance. Results have been compared applying our approach with standard scenario using CSMA/CA in Beacon Disabled mode; in this way all traffic flows are sent through CSMA/CA. In our architecture no-real-time traffic flows are sent separately using CFP and CSMA/CA protocol, so real-time traffic performance is only shown. In the following graphs, the IEEE 802.15.4 standard performance against the proposed approach with a varying number of traffic flows is compared.

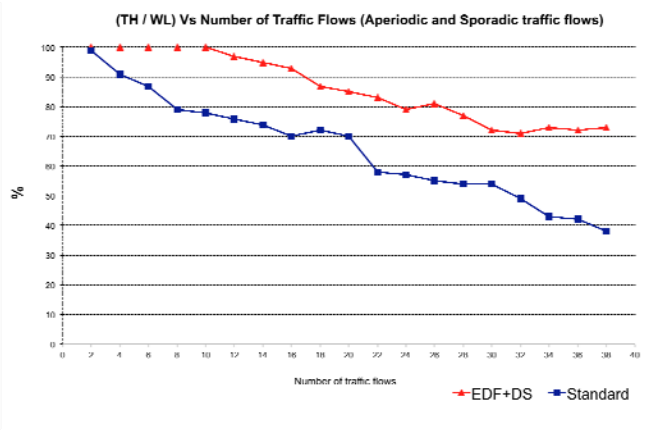

Figure 17. TH/WL vs. Number of Traffic Flows related to Aperiodic and Sporadic traffic

As shown in Figure 17 and Figure 18, our approach achieves a higher throughput than standard. Our scheduling algorithm and the separation between real-time traffic flows (scheduled in CFP section) and no-real-time traffic flows (sent in CAP section) determines these different results.

TH/WL ratio of periodic traffic flows shown in Figure 18 is equal to 100% using our approach. This result is due to the admission control module that manages data flows taking into account bandwidth utilization. Furthermore, all the admitted periodic traffic flows are sent to their destination because an ideal channel without any interference and noise is used.

Figures 19 and 20 show deadline miss behavior. In our approach the admission control rejects non-admitted request, so deadline miss ratio percentages are equal to zero. Figures show that missed deadline percentage remains approximately constant, both in periodic flow and aperiodic/sporadic flows case.

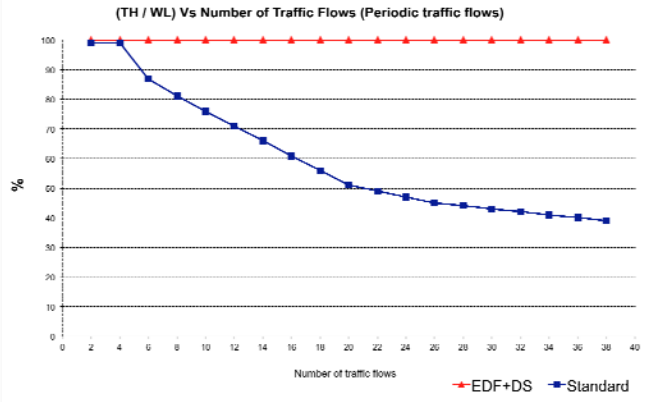

Figure 18. TH/WL vs. Number of Traffic Flows related to Periodic traffic

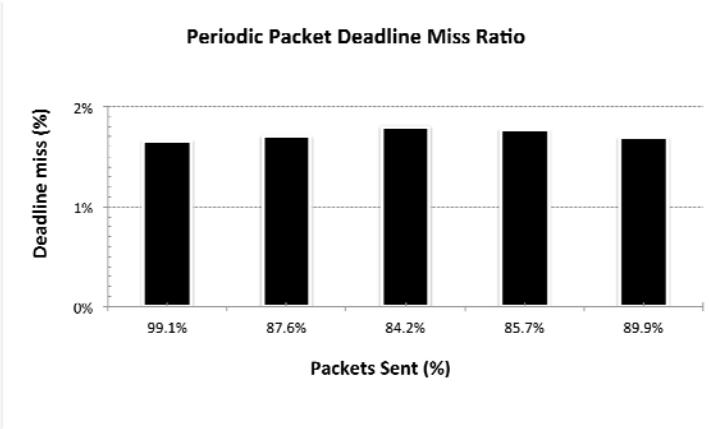

Figure 19. Periodic Packets Deadline Miss Ratio

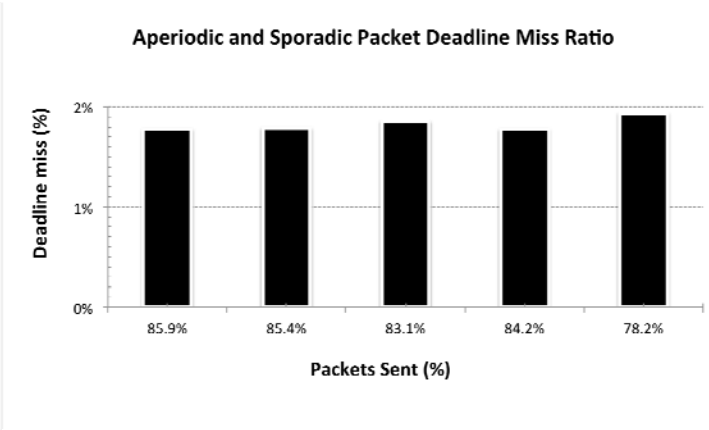

Figure 20. Aperiodic and Sporadic Packets Deadline Miss Ratio

8 Conclusions

In this work a two-tiered architecture integrating biometric user authentication, energy consumption analysis, and the real-time mobile communication scheduling has been proposed and described. Fuzzy techniques have been used to develop the different modules for interacting with complex Home Automation Environments. Fingerprint authentication module is based on a multimodal approach using a fuzzy module at score and decision levels. Module performance has been evaluated against the FVC2002 DB3 database. The Equal Error Rate is about 13.7% for decision level fusion and about 11.8% for matching score level fusion, while the same parameter is 18.5% for the corresponding unimodal systems. True-Time simulator has been used to demonstrate the advantages of the proposed approach on WSNs in terms of power consumption. Total simulation time has been set to 540 TTi (True Time iterations). Results obtained after 540 TTi show how it is possible to save on average 6 mA/min using the Fuzzy Logic Controller – Sampling Adapter (FLC-SA). OMNeT++ simulator has been used to test the scheduling algorithm (EDF+DS) in an IEEE 802.15.4 scenario. The achieved results show higher throughputs than the standard, while TH/WL ratio of periodic traffic flows is equal to 100%. This result is due to the admission control module that is able to manage data flows optimizing bandwidth utilization.

References

1. S. Vitabile, V. Conti, M. Collotta, G. Scatà, S. Andolina, A. Gentile, F. Sorbello, "*A Real-Time Network Architecture for Biometric Data Delivery in Ambient Intelligence*", Journal of Ambient Intelligence and Humanized Computing (AIHC), © Springer-Verlag Editor, 2012, ISSN (Print) 1868-5137 - ISSN (Online) 1868-5145

2. IEEE Std 802.11-2007 for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, C1-1184, June 2007.

3. Chun Wai Lau, Bin Ma, Helen M. Meng, Y.S. Moon and Yeung Yam, "Fuzzy Logic Decision Fusion in a Multimodal Biometric System", proc. of Interspeech, 2004

4. Md. Maruf Monwar, Marina Gavrilova, and Yingxu Wang, "A Novel Fuzzy Multimodal Information Fusion Technology for Human Biometric Traits Identification", proc. of 10th IEEE conference on Cognitive Computing, 2011, pp. 112-119

5. Girija Chetty, "Biometric Liveness Checking Using Multimodal Fuzzy Fusion", proc. of IEEE International Conference on Fuzzy Systems (FUZZ), pp. 1-8, 2010

6. Abdul Wahab, Chai Quek, Chin Keong Tan, and Kazuya Takeda, "Driving Profile Modeling and Recognition Based on Soft Computing Approach", IEEE Transactions on Neural Networks, Vol. 20, no. 4, pp. 563-582, april 2009

7. A. Azzini, E. Damiani, S. Marrara, "Ensuring the identity of a user in time: a multi-modal fuzzy approach", proc. of IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, pp. 94-99, 2007

8. C. Militello, V. Conti, S. Vitabile and F. Sorbello, "Embedded Access Points for Trusted Data and Resources Access in HPC Systems", The Journal of Supercomputing - An international journal of High-Performance Computer Design, Analysis and Use, Springer Netherlands Publisher, 2011, ISSN 0920-8542, Vol. 55, N° 1, pp. 4 – 27, (ISSN Online 1573-0484), doi:10.1007/s11227-009-0379-1

9. V. Conti, C. Militello, F. Sorbello, S. Vitabile. "A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", IEEE Transactions on Systems, Man, and Cybernetics (SMC) Part C: Applications & Reviews, Vol., 40 issue 4, pp. 384-395. 2010, ISSN 1094-6977, doi:10.1109/TSMCC.2010.2045374

10. C. Militello, V. Conti, S. Vitabile, F. Sorbello, "An Embedded Iris Recognizer for Portable and Mobile Devices", Special Issue on "Frontiers in Complex, Intelligent and Software Intensive Systems" of International Journal of Computer Systems Science & Engineering, Vol. 25, n° 2, pp. 119-131, © 2010 CRL Publishing Ltd., ISSN: 0267-6192

11. V. Conti, C. Militello, S. Vitabile and F. Sorbello, "A Multimodal Technique for an Embedded Fingerprint Recognizer in Mobile Payment Systems", International Journal on Mobile Information Systems - Vol. 5, No. 2, 2009, pp. 105-124, IOS Press Ed., ISSN: 1574-017X, doi:10.3233/MIS-2009-0076

12. S. Vitabile, V. Conti, G. Lentini, F., Sorbello, "An Intelligent Sensor for Fingerprint Recognition", Proc. of on International Conference on Embedded and Ubiquitous Computing (EUC-05), Lecture Note in Computer Science (LNCS), Springer-Verlag, vol. 3824, pp. 27-36, ISBN 3-540-30807-5, 2005

13. G.Milici, G.Raia, S.Vitabile, F.Sorbello, "Fingerprint Image Enhancement Using Morphological Filter", IEEE EUROCON 2005 - The 8th International Conference on Computer as a tool. Belgrade, Serbia & Montenegro 21-24 November 2005. (pp. 967-970).

14. A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol.14, NO. 1, January 2004.

15. Uwe M.Bubeck, “Multibiometric Authentication – An Overview of Recent Developments” San Diego University, Spring 2003, www.thuktun.org/cs574/papers/multibiometrics.pdf.

16. N. Poh, S. Bengio, and J. Korczak, "A multi-sample multi-source model for biometric authentication," in Proc. IEEE 12th Workshop on Neural Networks for Signal Processing, 2002, pp. 375--384. URL: http://citeseer.ist.psu.edu/thian02multisample.html.

17. A. Jain, L. Hong, Y. Kulkarni, “A Multimodal Biometric System Using Fingerprint, Face and Speech”, Conference on Audio-Video based Biometric Person Authentication 1999.

18. C.W. Lau, B. Ma, H.M. Meng, Y.S. Moon, Y.Yam, “Fuzzy Logic Decision Fusion in a Multimodal Biometric System”, Proceedings of the 8th International Conference on Spoken Language Processing (ICSLP), Korea, October 2004.

19. S. Prabhakar, A.K.Jain, “Decision-level Fusion in Biometric Verification”, Pattern Recognition, Vol. 35 (4), 2002, pp. 861-874.

20. K. Dahel, Q.Xiao, “Accuracy Performance Analysis of Multimodal Biometrics”, Proceedings of the 2003 IEEE, Workshop on Information Assurance.

21. P. Verlinde, G. Chollet, and M. Acheroy, “Multi-Modal Identity Verification Using Expert Fusion”, Information Fusion, 1(1):17-33, July 2000.

22. http://bias.csr.unibo.it/fvc2002/

23. L.A. Zadeh, “Fuzzy sets”, Information and Control 8, 338-353 (1965)

24. O. Khader, A. Willig, A. Owlish, “Distributed wakeup scheduling scheme for supporting periodic traffic WSNs” European wireless, 2009

25. I.F. Acidly, W. Su, Y. Sankarasubramanian, E. Cayirci “Wireless sensor network: a survey” Computer Networks Volume 38, Issue 4, 15 March 2002, Pages 393-422

26. Feng Xia , Wenhong Zhao, Youxian Sun and Yu-Chu Tian, “Fuzzy Logic Control Based QoS Management in Wireless Sensor/Actuator Networks”, Sensors 2007, 7, pp. 3179-3191.

27. I. Gupta, D. Riordan, S. Sampalli, “Cluster-head election using fuzzy logic for wireless sensor networks”, Proceedings of the 3rd Annual Communication Networks and Services Research Conference. pp. 255-260, 2005

28. S. S. Kumar, M. N. Kumar, V.S. Sheeba, “Fuzzy Logic based Energy Efficient Hierarchical Clustering in Wireless Sensor Networks”, International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN), Vol.1, N° 4, pp. 53-57, Dec 2011

29. G. Ran, H. Zhang. S. Gong, “Improving on LEACH Protocol of Wireless Sensor Networks Using Fuzzy Logic”, Journal of Information & Computational Science”, Vol.7 N° 3, pp. 767-775, 2010

30. W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks” IEEE Transaction on Wireless Communications, Vol. 1, Issue 4, pp. 660-670, 2002

31. M. R. Tripathy, K. Gaur, S. Sharma. G.S. Virdi, “Energy Efficient Fuzzy Logic Based Intelligent Wireless Sensor Network”, Progress In Electromagnetics Research Symposium Proceedings, pp. 91-95, 2010

32. M. Collotta, G Pau, V. M. Salerno, G. Scatà, “A fuzzy based algorithm to Manage Power Consumption in Industrial Wireless Sensor Network”, 9th IEEE International Conference on Industrial Informatics (INDIN), pp. 151-156, 2011

33. M. Yusuf, “Energy-aware fuzzy routing for wireless sensor networks”, Proceedings of the IEEE Symposium on Emerging Technologies, pp. 63-69, 2005.

34. L. Chengfa, "An energy-efficient unequal clustering mechanism for wireless sensor networks", IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, pp. 604-612, 2005

35. P. Codara, D. Maccari, V. Marra, "A logical analysis of Mamdani-type fuzzy inference, I theoretical bases", IEEE International Conference on Fuzzy Systems (FUZZ), pp. 1-8, 2010

36. G.C.Buttazzo, "Hard Real-Time Computing Systems – Predictable Scheduling Algorithms and Applications", Springer, ISBN 978-1-4614-0675-4, Third edition, 2011.

37. "802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR- WPANs)" – June 2006 IEEE standard for information technology. Part 15.4.

38. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

39. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

40. http://www.control.lth.se/truetime/

41. http://www.omnetpp.org/