11

Fuzzy Logic Applied to Decision Making in Wireless Sensor Networks

Antonio M. Ortiz and Teresa Olivares
Albacete Research Institute of Informatics
Spain

1. Introduction

This chapter presents a real application of fuzzy logic applied to decision making in Wireless Sensor Networks (WSNs). These networks are composed by a large number of sensor devices that communicate with each other via wireless channel, with limitations of energy and computing capabilities. The efficient and robust realization of such large, highly dynamic and complex networking environments is a challenging algorithmic and technological task.

Networking is important because it provides the glue that allows individual nodes to collaborate. Radio communication is the major consumer of energy in small sensor nodes. Thus, the optimization of networking protocols can greatly extend the lifetime of the sensor network as a whole.

Organizing a network, composed in many cases by a high number of low-resourced nodes, is a difficult task since the algorithms and methods have to save as much energy as possible while offering good performance. Power saving has been the main driving force behind the development of several protocols that have recently been introduced.

The design and implementation of routing schemes that are able to effectively and efficiently support information exchange and processing in WSNs is a complex task. Developers must consider a number of theoretical issues and practical limitations such as energy and computation restrictions.

Self-organization algorithms also provide network load balance to extend network lifetime, improving efficiency, and reducing data loss. Another feature to bear in mind is network monitoring, necessary to control topology changes and the addition or elimination of nodes in the network.

We propose the use of fuzzy logic in the decision-making processes of the AODV routing protocol, in order to select the best nodes to be part of the routes. In this chapter, fuzzy logic improve the selection of routing metrics. It details parameter selection and definition, and fuzzy-rule set design. Finally, we show a complete series of results, where our intelligent proposal is compared to AODV, the routing protocol for mesh networks used by the ZigBee standard, and with AODV-ETX, an interesting metric commonly used in wireless networks.

From results obtained we can afford that AODV-FL (AODV with Fuzzy Logic) consumes less energy, since it sends less discovery messages resulting in fewer collisions; the number of hops for the routes created is lower with respect to AODV and the end-to-end delay is also reduced.

Therefore, the use of fuzzy logic as a metric in network routing improves the performance of the overall network.

2. Wireless Sensor Networks

Wireless Sensor Networks are composed by a set of sensor nodes, it is, embedded systems that can take data from the environment such as temperature, humidity or atmospheric pressure among others, and that can communicate via wireless (Yick et al., 2008; Zhao & Guibas, 2004). Usually, data is gather in an special node, know as Base Station, central node or sink. This node is usually connected to a PC or a high capacity device. When data is taken by sensors, nodes process the information and send it to the Base Station by using diverse communication protocols.

This kind of networks can be used in any environment where continuous monitoring is necessary, and node deployment may not follow any order. Algorithms and protocols used, must be able to work autonomously, in order to efficiently satisfy application requirements.

Due to node nature and the particular applications executed in WSNs, there are several special characteristics that define this kind of networks, as well as those inherit from traditional wireless systems:

- **Limitations:** nodes composing WSNs are small and do not permit the incorporation of powerful processors and high capacity storage devices. Furthermore, the available energy, provided by batteries, limits node-operation time.
- **Scalability:** the large number of nodes that can be deployed to fulfil a certain task, can be much larger than traditional local-area networks, so the communication techniques for WSNs must keep its functionality and efficiency as the number of network nodes grows.
- **Self-configuration:** WSNs should be able to self-configure due to manual configuration of hundreds or thousands of devices may not be possible. Moreover, the network have to self-adapt to possible changes related to the incorporation, elimination, and change of location of the nodes.
- **Simplicity:** as a consequence of node limitations and network size, applications and protocols must be as simple as possible.
- **Specificity:** there is a big variety of parameters and available options when designing a WSN that makes designs high application dependant, and this is why most of the proposals available in the literature are focused to determined applications.

All these features make WSNs a challenging field, and several universities, enterprises and research centres are working on the design and development of effective and efficient applications and protocols for these networks.

2.1 Devices

Nodes composing WSNs are quipped with a motherboard that incorporates: micro-controller, work and secondary memory, wireless interface and input/output system. Sensors are usually plugged in the input/output system, but some recent nodes already incorporate several sensors in the motherboard (see Fig. 1).

Fig. 1. Maxfor Tip node (*Maxfor Technology INC. http://http://www.maxfor.co.kr*, 2011)

Since the wireless interface is the component with highest energy consumption, communication protocols should be energy efficient, with the aim of increasing, as much as possible, the network lifetime.

Data collected by nodes are usually sent to a central node or Base Station, that have higher computation capabilities that sensor nodes, higher storage capacity and used to be connected to a wired network in order to be able to access network data by using a common Internet connection.

There is a wide variety of sensors that fulfil the requirements of any application, such as temperature, humidity, atmospheric pressure, presence, energy consumption or CO_2.

2.2 Applications

There exists a wide range of applications for wireless sensor networks. The variety in parameters that can be read by sensors makes the number of applications to grow every day. The application range includes industrial monitoring, building and home automation, medicine, environmental monitoring, urban sensor networks or energy management among others (Vasseur, 2010). These networks can also be used for security, military defense, disaster monitoring and prevention, etc.

Applications based on sensor networks are usually focused on monitoring parameters along time, in zones where it is not possible to deploy a wired network. This parameter monitoring collects data by using wireless nodes equipped with several sensors, and the information is normally sent to a central node that gathers the information of all network nodes. Figure 2 shows a WSN node attached to a vine in the Wisevine project (*Wisevine project, http://www.wisevine.info/*, 2011).

Due to the high number of nodes that can be deployed, and its battery-based nature, nodes must be able to self-organize by themselves, in order to perform efficient and automatic

Fig. 2. WSN node attached to a vine in the Wisevine project.

communications. Self-organization is an important issue in the world of sensor networks that ensures the correct operation of the networks and its efficiency.

2.3 Architectures

Architectures in WSNs are defined with the objective of organize protocols and communication services that can be executed by sensor nodes. This structure helps developers to create products that are completely functional when combining with other protocols, services and devices in the system (Forouzan, 2006).

Wireless sensor networks have adopted (with some changes) the five-layer architecture used in TCP/IP networks, as a result of the simplification of the OSI architecture. The most important changes are related to the inter-layer communication. While in TCP/IP there exists several interfaces that allow inter-layer communications, the architectures for WSNs incorporate global services to allow transparent inter-layer communication. The most popular architectures used in the field of sensor networks are 6LoWPAN and ZigBee.

2.3.1 6LoWPAN

IPv6 over Low power Wireless Personal Area Networks (Z. Shelby and C. Bormann, 2009) is an architecture that defines the use of IPv6 addressing for WSNs, allowing so the inclusion in the global network, favouring the access to network nodes from everywhere. Same as ZigBee, 6LoWPAN uses IEEE 802.15.4 for the definition of physical and medium access layers, while in the network layer it uses IPv6 addressing adapted to WSNs by using the LowPAN layer, that provides encapsulation and the necessary methods to allow the co-existence of 802.15.4 and IPv6. Transport layer can use UDP or ICMP, depending on the requirements of the particular application.

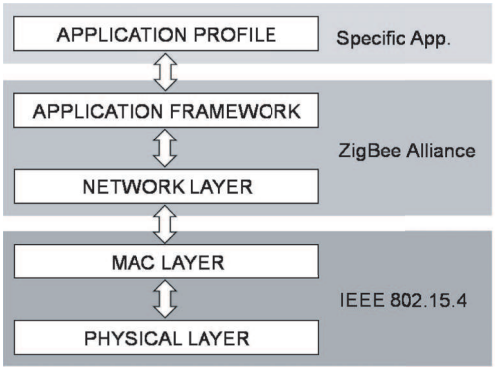


Fig. 3. ZigBee protocol stack.

2.3.2 ZigBee

The ZigBee Alliance *ZigBee Specification, ZigBee Alliance* (2011) and the IEEE 802.15.4 *IEEE Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (WPANS)* (2011) Task Group are leading the efforts to define a standard protocol stack for the implementation of wireless sensor networks. IEEE 802.15.4 is focused on the standardization of the MAC and physical levels, while ZigBee defines network layer and application framework (see Fig. 3).

The ZigBee network layer includes three different topologies, namely, tree, mesh, and cluster-based topologies. This chapter is focused on mesh topology networks for which ZigBee uses the Ad hoc On demand Distance Vector protocol (AODV), that will be detailed below.

2.4 Self-organization and routing

The correct operation of both wired and wireless networks requires some kind of network organization. Most of networking systems follow some kind of organization, well centralized or distributed to make data to effectively reach the destination. In wired networks, routers and switches define the network structure, but in wireless networks, and particularly in WSNs where hundreds or thousands of nodes have to be organized without any specific device to perform organization, the nodes themselves have to implement efficient self-organization mechanisms.

Self-organization in WSNs covers several tasks such as topology discovering, medium access control, data routing, and specific application controls. Self-organization can be defined as *the execution of local tasks by the individuals that take part in the network in order to get a global objective without using any centralized control* (Zvikhachevskaya & Mihaylova, 2009).

One of the most important tasks in self-organization in WSNs is routing, since it allows the network to stablish the routes necessary to correct and efficiently deliver network data to the destination in a reliable manner (Royer & Toh, 1999).

The special features of WSNs make that the development of routing schemes for this kind of networks must consider the following aspects (Pantazis et al., 2009; Yang & Mohammed, 2010):

- **Resource limitations:** restrictions such as available energy, memory and processing capabilities should be considered in order to extend, as much as possible, the network lifetime without overloading the network and the nodes themselves.
- **Node heterogeneity:** it is possible the coexistence of different node models in the same network. So, the routing protocol should solve the problems that can arise when nodes with different hardware or radio interface have to collaborate.
- **Transmission medium:** problems regarding the wireless channel such as interferences, signal attenuation or collisions must be considered.
- **Coverage and connectivity:** since the node coverage is limited, the connectivity of all the network must be ensured, avoiding node isolation, and enabling multi-hop communication if necessary.

The consideration of these factors will ensure the achievement of the routing protocols, but it is important to consider some requirements such as scalability, fault tolerance, efficiency or quality of service, in order to get the desired result when using the routing approach.

Next, AODV routing protocol is analysed in order to illustrate its main features and drawbacks.

3. Ad-hoc On demand Distance Vector routing (AODV)

AODV is a pure on-demand routing protocol which bases route discovery on a route request and route reply query cycle and the metric used is the number of hops from the source to the destination. In general terms, when a source node aims to send data to a destination node, the source broadcasts a route-request packet in order to discover a route to the destination. Intermediate nodes will forward the route-request, and eventually, any node which has a route to the destination or the destination itself will reply (unicast) with a route-reply message to the source. Once the source has received the route-reply, it is ready to send data to the destination. Routes are maintained and if any error occurs during the route valid time (or lifetime), a route-error message is propagated in order to avoid the use of broken links and out-of-date routes.

Messages used in AODV during route discovery and maintenance processes are:

- **Route Request (RREQ)**: this kind of messages are used to discover network routes. An RREQ contains: ID, source and destination addresses, sequence number, hop count, time-to-live (TTL), and control flags. RREQ ID, combined with the source address, uniquely identifies an RREQ.
- **Route Reply (RREP)**: it is used to answer route-request messages. It contains source and destination addresses, route lifetime, sequence number, hop count and control flags.
- **Route Error (RRER)**: these messages are used to notify of link failures, and avoid their use. They contain the addresses and corresponding destination sequence number of all active destinations that have become unreachable due to the link failure. A node receiving an RRER message, will invalidate the corresponding entries in its routing table.

In AODV, the route discovery process starts when a source node intends to communicate with a destination node. If the route is unknown, data packets are buffered, and the source node broadcasts an RREQ intended for the destination node. A node receiving an RREQ will verify the destination address to check if it is the destination node, or if it has a route to the

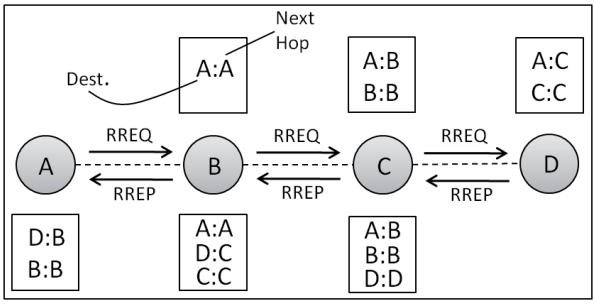


Fig. 4. AODV route discovery example.

destination. In this case, it will send (unicast) an RREP to the originator of the received RREQ. Otherwise, the intermediate node will save the request in order to forward an eventual RREP, and the RREQ will be re-broadcast if TTL (Time-To-Live) value is greater than zero. Figure 4 shows an example of the messages sent during route discovery between the source node (A) and the destination node (D).

To control network-wide broadcasts of RREQs, the source node uses an expanding ring search technique, which allows a search of increasingly larger areas of the network if a route to the destination is not found. In order to avoid loops and forwarding storms, both RREQ and RREP packets are forwarded just once unless an intermediate node receives an RREQ or RREP with the same source and destination addresses, but with a lower number of hops. In that case, it will be forwarded in order to discover the route with the lowest number of hops. Eventually, the source node will receive an RREP if there is a route to the destination. Then, buffered data packets can be sent to the destination node using the newly-discovered route.

In the case of a link failure, implied nodes will generate an RRER message in order to notify communicating nodes about the invalidation of the routes using that link.

3.1 AODV drawbacks

Due to its on-demand-based nature, AODV presents several problems that are mainly related to high packet drop ratios and high routing overheads (Alshanyour & Baroudi, 2008). These problems cause packet loss, collisions, high end-to-end delay and high latency, among others.

- **Packet overhead**: AODV requires an enormous number of packets to complete path discovery and perform routing tasks (Lin, 2005; Sklyarenko, 2006). RREQ broadcasts represent a high network load, and this load is increased when packets have to be re-injected due to high channel occupancy and collisions. As the node density increases, the number of messages sent and received per node appears to increase quadratically (Sklyarenko, 2006). This occurs because when nodes broadcast RREQ messages, those messages are received by more nodes, and these nodes occupy the channel rebroadcasting them. As more nodes come together, the channel scheduling becomes more difficult.
- **Redundant discovery**: routes frequently become saturated causing blocks, thereby leading to new route discoveries. These route discoveries increase the routing overhead, thus aggravating the problem (Pirzada & et al., 2007). Moreover, the path discovery overhead and the routing overhead are sometimes very high, with the consequent time and energy costs to complete routing tasks.

- **High route discovery delay**: as a reactive protocol, AODV has an evident weakness: its latency, since routes are discovered on demand. The route discovery process can take some time and this delay can be increased due to problems in the medium access, such as busy channel and collisions. The time taken by the network to create routes exhibits cubic growth in relation to the number of network nodes (Sklyarenko, 2006). AODV's end-to-end delay is also a weakness of this protocol since it becomes very high when a big proportion of the network nodes have to send messages. This problem is caused by collisions during the routing discovery process, and during data forwarding (Nefzy & Song, 2007).
- **High memory demand**: along with time, memory is also critical and AODV requires all nodes to reserve sufficiently large memory spaces to store possible routing entries for active sources and destinations (Lin, 2005; Ramachandran et al., 2005). This is a problem that limits scalability in WSNs and is due to nodes being resource constrained (Manjula et al., 2008). The throughput of AODV is compromised due to high packet loss (Pirzada & et al., 2007). Since data delivery is a critical issue for some applications such as health and monitoring, packet loss has to be minimized.
- **Duplicated messages**: the route discovery process also has some problems due to the absence of a delay between receiving and forwarding discovery packets. For example, a node that has just forwarded an RREQ from a source node, may receive the same RREQ with a lower number of hops, and it will have to forward it again, thus increasing energy consumption and network traffic.
- **Deficient metric**: another problem in AODV, is the metric used to make routing decisions. AODV forms routes using only the number of hops as a metric. Even though one may agree that AODV can always choose the route that minimizes the delay (Boughanmi & Song, 2007), it does not take into account other important parameters, such as available node energy, route traffic, or the signal strength of the received packets, among others.

In order to solve some of these problems, next section details the use of fuzzy logic in WSNs, as a backgraund of the proposal detailed in Section 5

4. Fuzzy Logic and Wireless Sensor Networks

In the literature, there exists several techniques oriented to improve the performance of routing approaches for WSNs. Most of these techniques are focused on changing the metric used to optimize parameters in order to determine the best path between source and destination, reduce the number of packets used, or reduce the end-to-end delay, among others.

The use of fuzzy logic to optimize the metric used in routing approaches for WSNs is a promising technique since it allows combine and evaluate diverse parameters in an efficient manner. Moreover, several proposals have shown that the use of fuzzy logic in this kind of networks is a good choice due to the execution requirements can be easily supported by sensor nodes, while it is able to improve the overall network performance.

Fuzzy logic is used in (Bacour et al., 2010) to perform link quality estimation. The system takes as input the information about link capacity to transport information, asymmetry, stability and channel quality. The experiments in a network in which all nodes are reachable from the base station show improvements in terms of reliability and stability.

In (Wang et al., 2009) is presented a method based on fuzzy logic and implemented in ZigBee nodes, with the aim of reducing the on/off frequency of an air conditioner system. To do

that, they use as input variables the temperature, humidity, fan speed, and engine speed. The experiments show good results compared to a traditional control system based on discrete temperature values.

An example of the use of fuzzy logic in routing for WSNs is LEACH-FL (Ran et al., 2010), where the selection of cluster-heads is based on several variables: node battery level, node density and distance to the base station. The experiments show that the use of fuzzy logic helps to reduce the energy consumption, so extending the overall network lifetime. Another example of fuzzy logic in WSN routing is (Ortiz et al., 2011) where the metric of the Tree Routing protocol used in ZigBee is replaced with the output of a fuzzy-logic based mechanism that allows a reduction in the path length, in the network discovery time and in the number of forwarding nodes.

In summary, the fuzzy logic is a powerful tool to be used in WSN approaches, since it provides effective parameter combination, and it is able to be executed in the low-resourced nodes that compose these networks. The next section details AODV-FL, a routing approach for wireless sensor networks that makes use of the fuzzy logic to evaluate several parameters that are considered during the route-creation process.

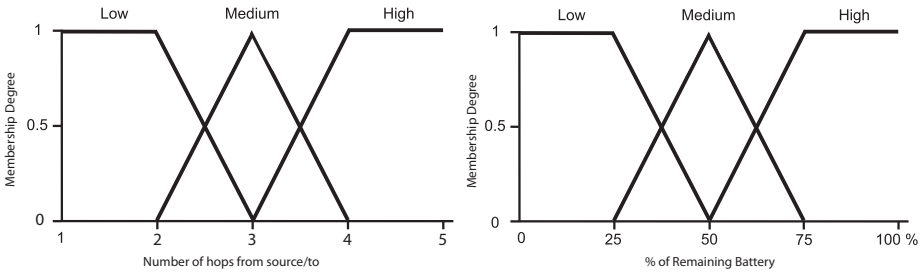
5. Ad-hoc On demand Distance Vector Routing with Fuzzy Logic (AODV-FL)

The use of fuzzy logic in the decision-making processes is detailed herein in order to select the best nodes to be part of the routes, and the incorporation of a timer when a new RREQ is received, to be able, if necessary, to evaluate several RREQs received (with the same ID and sequence number) and just forward the best of all those, instead of sometimes forwarding a worse RREQ and later a better one, as the traditional AODV does. With this timer we aim to reduce the number of messages used to discover routes, and so the network congestion caused by this high number of messages.

The lack of an efficient metric to evaluate node conditions in AODV has been solved by the definition of a new metric based on the combination of different node and network parameters by using a fuzzy-logic system. The idea is to specify the input parameters in natural language and, with the help of a fuzzy-rule set, to define the relationship among different inputs with the output, which represents the suitability or quality of a node to be selected as a part of the incoming route.

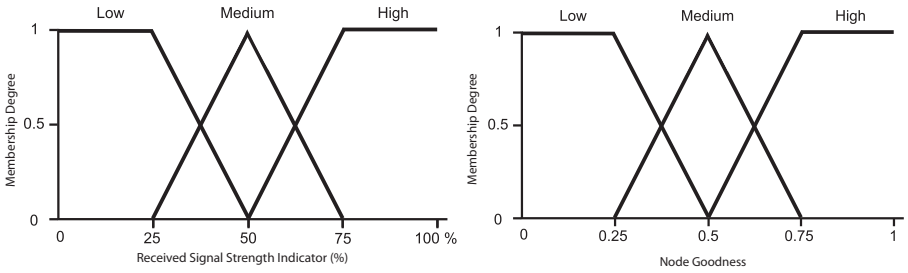
The input parameters to be considered are:

- **Number of hops**: this is the length of the path. In general, a lower number of hops will represent a better route, but this is not true at all, since it is possible that some nodes in the route have low battery or bad Received Signal Strength Indicator (RSSI), so it is very important to consider more variables to decide the route. This input fuzzy set is shown in Fig. 5a. The maximum number of hops observed in our experiments has been 5. Fuzzy sets have been declared to deal with any extreme situation that can occur during the execution. These fuzzy sets can be customized depending on each particular network size.
- **Local Battery level**: this parameter must be considered in order to avoid nodes with low battery taking part in data paths since they can cause failures in communication. Route construction considering nodes with high energy levels will help to save the energy of low-battery nodes and will cooperate to balance network lifetime. Moreover, the consideration of the battery level will ensure data transmission, preventing nodes in the



(a) Fuzzy Sets for Number of Hops. (b) Fuzzy Sets for Battery Level.

Fig. 5. Input Fuzzy sets.



(a) Fuzzy Sets for RSSI. (b) Output Fuzzy Sets.

Fig. 6. Input and Output Fuzzy sets.

route from running out of battery. Fuzzy sets for battery level are shown in Fig. 5b. The X-axis represents (as %) the remaining battery of the node.

- **RSSI (Received Signal Strength Indicator)**: the strength of the received signal is an indicator of the quality of communications between two nodes. In order to ensure quality communications and prevent data loss, data paths will consist of nodes that are able to communicate with a certain level of signal quality. Figure 6a shows the fuzzy sets declared for this variable. The X-axis represents (as %) the strength of the received signal.

The output of the fuzzy system (see Fig. 6b) represents the suitability of a node to be considered for inclusion in the route.

The geometric pattern of triangles is commonly used to determine the appropriate membership functions and control rules in many theory applications (Wang et al., 2009). In this paper, the geometric pattern of triangles to define input and output variables has been adopted.

Input and output sets are combined through a set of rules in order to obtain the corresponding output. Table 1 depicts the fuzzy-rule base used in the experiments. The objective of the fuzzy rules is to serve as a basis to determine, during the route discovery process, the best node to

Nhops	Bat.	RSSI	Output	Nhops	Bat.	RSSI	Output	Nhops	Bat.	RSSI	Output
Low	Low	Low	**Low**	Med	Low	Low	**Low**	High	Low	Low	**Low**
Low	Low	Med	**Low**	Med	Low	Med	**Low**	High	Low	Med	**Low**
Low	Low	High	**Med**	Med	Low	High	**Med**	High	Low	High	**Med**
Low	Med	Low	**Low**	Med	Med	Low	**Low**	High	Med	Low	**Low**
Low	Med	Med	**Med**	Med	Med	Med	**Med**	High	Med	Med	**Low**
Low	Med	High	**High**	Med	Med	High	**Med**	High	Med	High	**Med**
Low	High	Low	**Med**	Med	High	Low	**Low**	High	High	Low	**Low**
Low	High	Med	**High**	Med	High	Med	**Med**	High	High	Med	**Med**
Low	High	High	**High**	Med	High	High	**High**	High	High	High	**Med**

Table 1. Fuzzy rule base

forward its request/reply packet, with the objective of reducing packet overhead and energy consumption.

The input parameters, sets and rules shown herein, are just an example for the particular application and network model used in our experiments. Note that both fuzzy sets and rules, as well as considered parameters, can be customized depending on the application requirements, node features, network size and capabilities.

In AODV-FL, a node receiving an RREQ calculates the fuzzy-logic value associated to that RREQ, and if it is the first RREQ received (no RREQ with the same ID and sequence number has been received), it starts a timer. During the duration of the timer, if the node receives more RREQs with the same ID and sequence number, the stored request will be updated if the calculated FL-value for the received RREQ is higher than the one stored. When the timer expires, the node will forward the received RREQ with the highest FL value.

The destination node, or any intermediate node having a route to the destination, will reply with an RREP to the best RREQ received (for a given ID and sequence number).

Flow charts for AODV and AODV-FL are shown in Figs. 7 and 8. There are two main differences between both proposals: first, the change of metric, the number of hops used in AODV, for the output of the FL-evaluation process in AODV-FL; and second, the use of a timer to allow the reception (if necessary) of several RREQs from the same source node, and select the best (fuzzy-logic evaluation based) RREQ to be forwarded, thus avoiding multiple forwarding for the same RREQ. This event is frequent in AODV when using a realistic MAC protocol, because sometimes a node may receive first an RREQ with $numhops = x$ and later another RREQ with $numhops = x - n$, and both will be forwarded. In contrast, the timer implemented in AODV-FL allows nodes to wait for more RREQs (with the same ID and sequence number) when the first one is received. This timer is randomly calculated by considering one-hop packet delivery time and the *MaxBackOff* parameter from the MAC layer.

With these premises we aim to:

- Reduce the number of packets sent, so reducing the global energy consumption.
- Improve route formation by selecting, at each hop, the best available node, ensuring route stability and avoiding data loss.
- Maintain routing table size, not making the use of extra memory space.

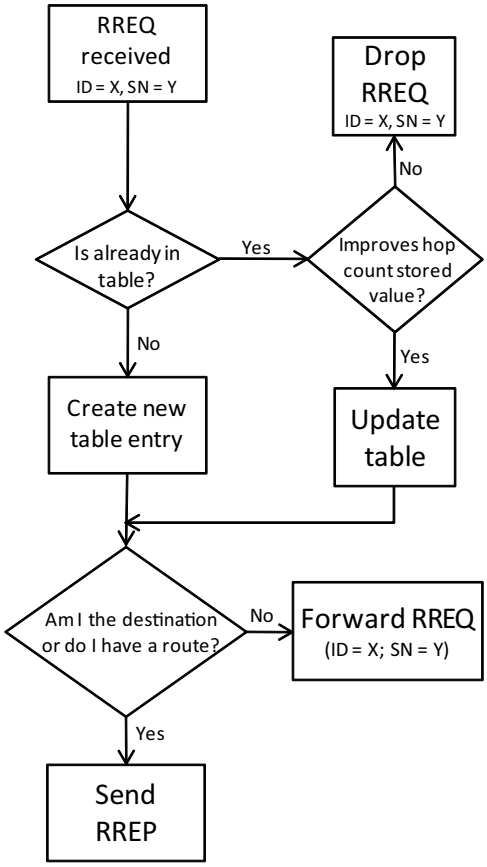


Fig. 7. AODV decision flowchart.

- Provide adaptability: AODV-FL is able to deal with different networks in various applications, it is just necessary to tune the fuzzy parameters to be used, as well as the fuzzy sets and rules.

Figure 9 shows an example of message exchange during a part of route discovery for both AODV and AODV-FL. The topology used in this example is shown in Fig. 9a, in which the dotted line shows the connections in terms of the coverage of each node. *SOURCE* node aims to send data to *DEST* node, and broadcasts an RREQ. Lett's detail the operation of AODV, and our proposal, AODV-FL:

- **AODV**: (shown in Fig. 9b) nodes 1 and 3 receive the RREQ from *SOURCE* and both aim to forward it. Let's suppose that CSMA/CA (implemented in MAC layer) makes node 1 own the channel, so it forwards the RREQ, and node 3 buffers it to forward it later. Nodes 2 and 3 receive that packet, and just node 2 will forward it since node 3 has buffered an RREQ with a lower number of hops. Suppose that node 2 finds the channel free, and forwards the RREQ. Nodes 1, 3 and 4 receive it. Nodes 1 and 3 discards the packet since it does not improve the hop count stored for that RREQ. Remember that node 3 has an RREQ buffered.

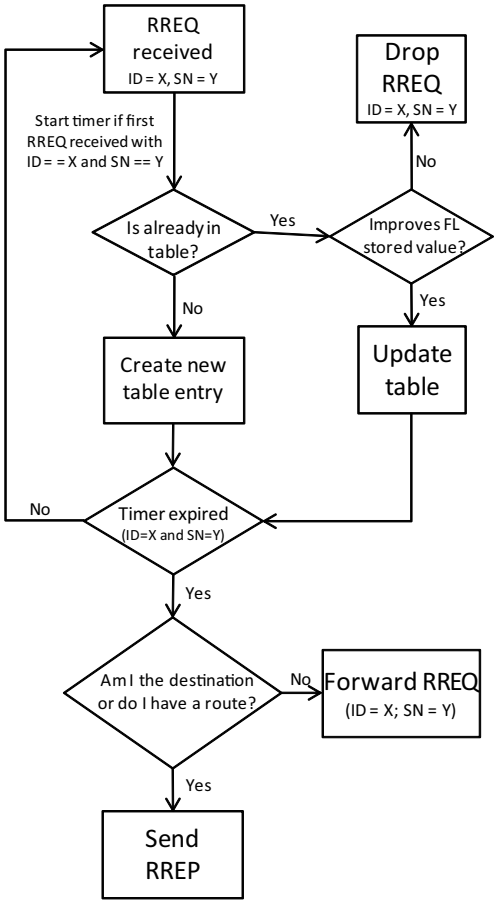
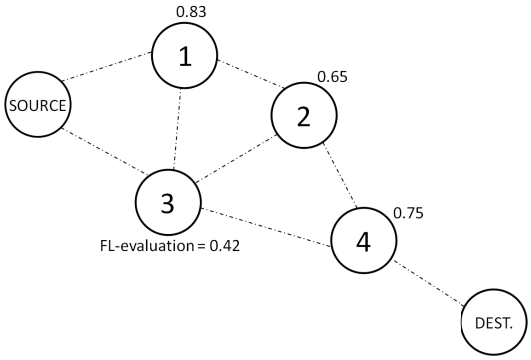


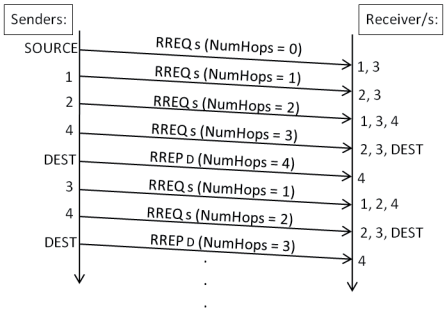
Fig. 8. AODV-FL decision flowchart.

So nodes 3 and 4 compete to forward the RREQ. Let's suppose once again that node 4 owns the channel and forwards the RREQ which is received by nodes 2, 3 and *DEST*. Nodes 2 and 3 discard it and *DEST* generates an RREP and sends it to node 4. This RREP will be forwarded by nodes 2 and 1 until it reaches *SOURCE*. Now, node 3 finds the channel free, so it forwards the RREQ that received from *SOURCE*. Nodes 1, 2 and 4 receive this packet. Nodes 1 and 2 discard it since it does not improve their hop counts, and node 4 forwards it since it improves the hop count (previously 3, now 2). *DEST* receives this RREQ and generates a new RREP, because it improves the stored hop count. The new route now has 3 hops instead of the 4 hops of the previous route. Then (not shown) Node 4 will forward the RREP to 3, which will forward it to *SOURCE* (not shown in Fig. 9b).

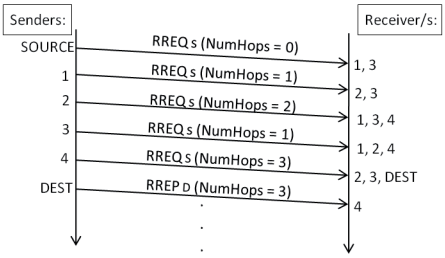
- **AODV-FL**: (shown in Fig. 9c) nodes 1 and 3 receive the RREQ from *SOURCE* and both start a timer in order to wait to receive more RREQs with equal ID and sequence number. Let's suppose that the timer in node 1 finishes first(note that timers are set with a random time proportional to the number of different RREQs received). So node 1 forwards the packet. Nodes 2 and 3 receive the RREQ; node 3 discards it since it does not improve its



(a) Example topology



(b) AODV timeline.



(c) AODV-FL timeline.

Fig. 9. Message exchange example for AODV and AODV-FL.

FL-value, and node 2 starts a timer. Let's suppose that the timer of node 2 finishes before the one in node 3. So node 2 forwards the RREQ, which is received by nodes 1, 3, and 4. Node 1 discards it, since it has already forwarded that RREQ; node 3 discards it, and node 4 starts a timer. Now, the timer in node 3 finishes and it forwards the RREQ from *SOURCE*. Node 4 ignores it, due to as it does not improve the stored FL-value (node 2, 0.75). When the timer in node 4 expires, it forwards the RREQ. *DEST* receives the RREQ and generates an RREP for node 4. Node 4 will forward (not shown in Fig. 9b) the RREP to node 2 since the best RREQ received by node 4 came from node 2. Now the route has 4 hops instead of the 3 selected by AODV, but it is important to consider the low FL-value obtained by node 3, which may be a sign of packet loss.

The example shows the efficiency of route discovery with AODV-FL, which even selects routes with more hops but that are able to avoid data loss. AODV selected the shortest route, but node 3 may present battery or signal strength problems that cause packet loss, with the consequent energy consumption caused by re-injection. Besides the reliability of the routes created by AODV-FL, it is important to consider the energy saving achieved: only with six nodes, AODV-FL reduces the number of packets by 25%. This packet reduction will rise when the network size increases.

Parameter	*Value*
max MAC Frame Size	80 bytes
MAC Frame Overhead	14 bytes
MAC Buffer Size	32 frames
min Exponential Backoff	3
max Exponential Backoff	5
max CSMA Backoffs	4
max Frame Retries	3

Table 2. MAC parameters used in the experiments with AODV, AODV-FL and AODV-ETX

6. Experiments

In order to evaluate the performance of our proposal, we have implemented AODV, AODV-FL, AODV-ETX (AODV using ETX-based metric), and CSMA/CA in the Omnet++ (*Omnet++ Network Simulation Framework*, 2011) module for wireless sensor simulation. The use of a realistic MAC protocol will provide us with reliable results in order to include our proposal in a real wireless sensor network.

In AODV-ETX Ni et al. (2008), the hop-count metric is replaced with a new metric based on expected transmissions, ETX (Expected Transmissions Count) Couto et al. (2003) aims to find high-throughput paths on multihop wireless networks, by minimizing the expected total number of packet transmissions required to successfully deliver a packet to the ultimate destination.

In the experiments, nodes decide whether to discover a route and send data to a random destination with a probability of 25%. Routes are established on demand and the experiments consists on the sending nodes executing the discovery process and sending one data packet. Nodes are deployed randomly with a separation between nodes which varies between 1 and 50 meters. The number of nodes varies from 25 to 200, and each experiment has been executed 50 times to get reliable results.

In order to ensure route discovery, and taking into account that CSMA/CA is used to perform channel access, when the MAC layer reports *MAX NUMBER OF BACKOFF* or *MAX FRAME RETRIES* achieved for a particular packet, this packet will be re-injected by the network layer. Table 2 shows the main MAC parameters used in the experiments.

To make a fair comparison, the results for AODV-ETX do not show the process of ETX calculation which is carried out prior to the first RREQ send.

6.1 Results

The variables to be evaluated are: energy consumption, number of RREQ and RREP packets sent, number of collisions, end-to-end delay, and number of hops.

The energy consumption is a key element in WSNs; energy saving is a key objective of protocols for this kind of networks. Figure 10 shows (as %) the average energy saving achieved by AODV-FL and AODV-ETX with respect to the original AODV. The energy consumption of AODV-FL and AODV-ETX have been normalized according to the energy consumed in AODV.

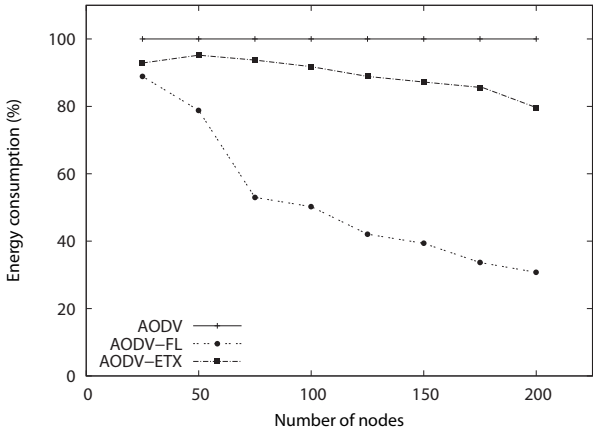
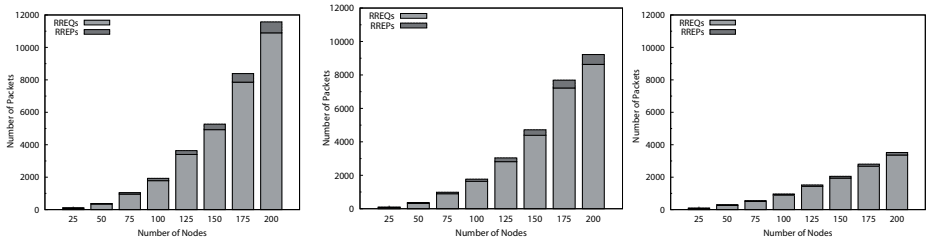


Fig. 10. AODV-FL and AODV-ETX energy saving with respect to AODV energy consumption.



(a) AODV. (b) AODV-ETX. (c) AODV-FL.

Fig. 11. Messages sent during route discovery phase for AODV, AODV-ETX and AODV-FL.

The energy consumed by AODV-FL is considerably lower than that consumed by AODV and AODV-ETX. This reduction will allow WSNs running AODV-FL to increase their lifetime. This energy saving is given due to the reduction in the number of packets sent during the route discovery phase. The number of RREQs and RREPs directly affects energy consumption, and is an important factor to be considered in the evaluation. Figure 11 depicts the average number of discovery messages sent by AODV (a), AODV-ETX (b) and AODV-FL (c) during the experiments.

The RREQ evaluation carried out by AODV-FL before packet forwarding, drastically reduces the number of discovery packets necessary to perform route creation. The high number of RREQs and RREPs sent in AODV and AODV-ETX, besides a higher energy consumption, it also leads to a high number of collisions. In AODV-FL, the RREQ evaluation, performed prior to forwarding, decreases the number of RREQ forwardings, and so reduces the number of collisions. The average number of collisions during the experiments is shown in Fig. 12, which confirms that the reduction in the number of RREQ and RREPs obtained by AODV-FL also reduces the number of collisions.

Collisions directly affect the communication delay since nodes have to re-inject collided packets. Networks with real-time requirements, such as industrial and building monitoring

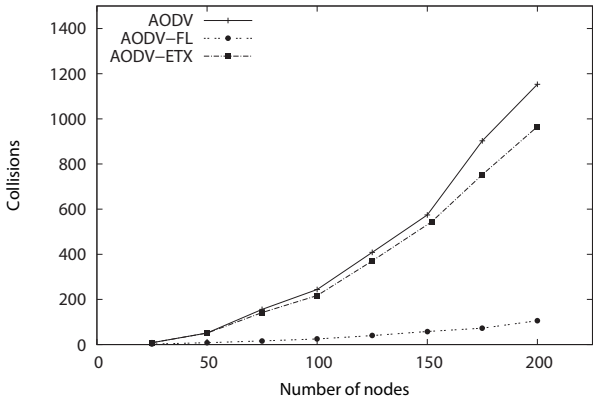


Fig. 12. Number of collisions.

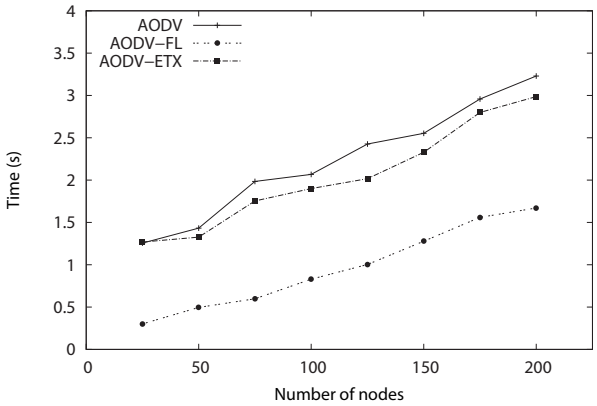


Fig. 13. End-to-end delay.

ones, require low end-to-end communication time, which includes route discovery, and data delivery. Figure 13 shows the average end-to-end delay since the first RREQ is sent until the last data packet arrives to the destination.

The delay introduced with the timer in AODV-FL is not a failing, because the high number of collisions makes AODV and AODV-ETX spend a lot of time re-injecting packets, around 40 to 60% more than AODV-FL.

Another important result is the number of hops. The example in Section 5 shows that AODV-FL may not select the route with lowest number of hops, while AODV does. In that example, AODV firstly selects a non-optimum route (in terms of the number of hops) and later the best route. Figure 14 shows the average number of hops (route length) for the routes created with the first RREP received by the source node for AODV, AODV-ETX and AODV-FL.

The number of hops for the routes created when the source nodes receive the first RREP is higher for AODV with respect to AODV-FL. This is so because in AODV the source nodes may

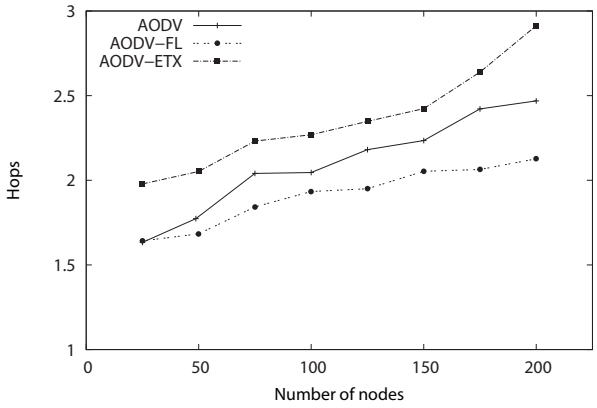


Fig. 14. Route length (number of hops).

receive a non-optimal route first and later the optimal one. Note that for small networks (50 nodes or less), the average number of hops is similar for both proposals, but when the network size increases, so does the number of alternative routes, and the probability of receiving a non-optimal route first in AODV increases. This fact can be a disadvantage for networks with real-time requirements due to as source nodes will either have to wait and see if a better RREP is received, or send data using a route that can be non-optimum. As for AODV-ETX, it obtains higher route lengths due to it selects paths not considering the number of hops, but the expected transmissions.

All these results show that AODV-FL is more effective than the original AODV, and the ETX-based approach in all the experiments, reducing the energy consumption by up to 70%. The performance of the route discovery has also been improved, not only in the number of packets (around 60-70% reduction), but also in the path lengths (20% reduction) and end-to-end delay (40-50% reduction).

7. Conclusions and future research

Monitoring applications in wireless sensor networks require effective, robust and scalable routing protocols, above all in applications with resource-constrained nodes. This chapter details the use of fuzzy logic to improve the routing protocol used by the ZigBee standard in mesh networks, AODV. The use of fuzzy logic as a metric in network routing improves the performance of real networks. AODV-FL uses this metric, achieving an energy reduction of 70% in network route creation, due to a considerable reduction in the number of RREQs generated, reducing collisions and the end-to-end delay. In contrast with other proposals that require additional memory or processing costs, the use of fuzzy logic does not imply an extra load on the system, and it improves the performance of the intelligent dense monitoring of physical environments.

Experimental comparisons with AODV and AODV-ETX endorse the suitability of AODV-FL for implementation in real wireless sensor networks.

Future research can be oriented to the addition of new parameters to the fuzzy logic system, studying the performance achieved by these new variables, such as the number of child nodes,

or node density. The use of fuzzy logic in other layers, such as the MAC layer, will help to provide priority in the contention period to those nodes with better conditions.

In summary, fuzzy logic is a powerful approach that has demonstrated to be effective when combining with other disciplines such as routing approaches for WSNs. The potential of fuzzy logic goes beyond traditional control systems and can be used on many research fields, allowing multidisciplinary approaches and performance improvements.

8. References

Alshanyour, A. M. & Baroudi, U. (2008). Bypass AODV: Improving Performance of Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol in Wireless Ad Hoc Networks, *Proceedings of the First International Conference on Ambient Media and Systems (Amby-Sys)*.

Bacour, N., Koubaa, A., Youssef, H., Jamaa, M. B., do Rosario, D., Alves, M. & Becker, L. B. (2010). F-LQE: A Fuzzy Link Quality Estimator for Wireless Sensor Networks, *Proceedings of the European Conference on Wireless Sensor Networks (EWSN)*.

Boughanmi, N. & Song, Y. (2007). Improvement of ZigBee Routing Protocol Including Energy and Delay Constraints, *Proceedings of the Junior Research Workshop on Real-Time Computing*.

Couto, D. D. J. D., Aguayo, D., Bicket, J. & Morris, R. (2003). A High-Throughtput Path Metric for Multi-Hop Wireless Routing, *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom)*.

Forouzan, B. A. (2006). *Transmisión de datos y redes de comunicaciones*, Mc. Grawn Hill.

IEEE Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (WPANS) (2011). http://standards.ieee.org/getieee802/download/802.15.4c-2009.pdf.

Lin, C. (2005). AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulations (SWANS). JIST/SWANS, http://jist.ece.cornell.edu/.

Manjula, S. H., Abhilash, C. N., Shaila, K., Venugopal, K. R. & Patniak, L. M. (2008). Performance of AODV Routing Protocol using Group and Entity Mobility Models in Wireless Sensor Networks, *Proceedings of the International Multiconference of Engineers and Computer Scientists*.

Maxfor Technology INC. http://http://www.maxfor.co.kr (2011).

Nefzy, B. & Song, Y. (2007). Performance Analysis and Improvement of ZigBee Routing Protocol, *Proceedings of the 7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems*.

Ni, X., Lan, K. & Malaney, R. (2008). On the Performance of Expected Transmission Count (ETX) for Wireless Mesh Networks, *Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS)*.

Omnet++ Network Simulation Framework (2011). http://www.omnetpp.org/.

Ortiz, A. M., Olivares, T. & Orozco-Barbosa, L. (2011). Smart Routing Mechanism for Green ZigBee-based Wireless Sensor Networks, *Proceedings of the 16th IEEE Symposium on Computer and Communications (ISCC)*.

Pantazis, N. A., Nikolidakis, S. A. & V., D. D. (2009). Energy-efficient routing protocols in wireless sensor networks for health communication systems, *Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments*, PETRA, pp. 34:1–34:8.

Pirzada, A. A. & et al. (2007). High performance AODV routing protocol for hybrid wireless mesh networks , *Proceedings of The Fourth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*.

Ramachandran, K. N., Buddhikot, M. M., Chandranmenon, G., Miller, S., Belding-Royer, E. M. & Almeroth, K. C. (2005). On the Design and Implementation of Infraestructure Mesh Networks, *Proceedings of the IEEE Workshop on Wireless Mesh Networks (WiMesh)*.

Ran, G., Zhang, H. & Gong, S. (2010). Improving on LEACH Protocol of Wireless Sensor Networks Using Fuzzy-Logic, *Journal of Information and Computational Science* 7(3).

Royer, E. & Toh, C. K. (1999). Self-Organization in Communication Networks: Principles and Design Paradigms, *IEEE Personal Communications* 6(2): 46–55.

Sklyarenko, G. (2006). AODV Routing Protocol. Seminar Technische Informatik. Institute für Informatik, Freie Universität Berlin.

Vasseur, J. P. (2010). Terminology in Low power And Lossy Networks. Internet draft, Networking Working Group. http://tools.ietf.org/html/draft-ietf-roll-terminology-04.

Wang, T. M., Liao, I. J., Liao, J. C., Suen, T. W. & Lee, W. T. (2009). An Intelligent Fuzzy Controller for Air-Condition with ZigBee Sensors, *International Journal in Smart Sensong and Intelligent Systems* 2.

Wisevine project, http://www.wisevine.info/ (2011).

Yang, Z. & Mohammed, A. (2010). A survey of routing protocols of wireless sensor networks, *Proceedings of the Sustainable Wireless Sensor Networks*.

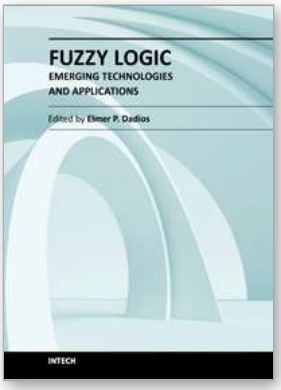
Yick, J., Mukherjee, B. & Ghosal, D. (2008). Wireless Sensor Network Survey, *Computer Networks* 52.

Z. Shelby and C. Bormann (2009). 6LoWPAN: The Wireless Embedded Internet. Wiley.

Zhao, F. & Guibas, L. (2004). *Wireless Sensor Networks, an Information Processing Approach*, Elsevier.

ZigBee Specification, ZigBee Alliance (2011). http://www.zigbee.org/.

Zvikhachevskaya, A. & Mihaylova, L. (2009). Self-organisation in wireless sensor networks for assisted living, *Proceedings of the IET Assisted Living Conference*.



Fuzzy Logic - Emerging Technologies and Applications
Edited by Prof. Elmer Dadios

ISBN 978-953-51-0337-0
Hard cover, 348 pages
Publisher InTech
Published online 16, March, 2012
Published in print edition March, 2012

The capability of Fuzzy Logic in the development of emerging technologies is introduced in this book. The book consists of sixteen chapters showing various applications in the field of Bioinformatics, Health, Security, Communications, Transportations, Financial Management, Energy and Environment Systems. This book is a major reference source for all those concerned with applied intelligent systems. The intended readers are researchers, engineers, medical practitioners, and graduate students interested in fuzzy logic systems.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821