A. Nieto, and J. Lopez, "Traffic Classifier for Heterogeneous and Cooperative Routing through Wireless Sensor Networks", *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, pp. 607-612, 2012.
http://doi.org/10.1109/WAINA.2012.202
NICS Lab. Publications: https://www.nics.uma.es/publications

Traffic Classifier for heterogeneous and cooperative routing through Wireless Sensor Networks

Ana Nieto, Javier Lopez
Computer Science Department
University of Malaga, Spain
Email:{nieto,jlm}@lcc.uma.es

***Abstract*—Wireless Sensor Networks (WSN) are networks composed of autonomous devices manufactured to solve a specific problem, with limited computational capabilities and resource-constrained (e.g. limited battery). WSN are used to monitor physical or environmental conditions within an area (e.g. temperature, humidity). The popularity of the WSN is growing, precisely due to the wide range of sensors available. As a result, these networks are being deployed as part of several infrastructures. However, sensors are designed to collaborate only with sensors of the same type. In this sense, taking advantage of the heterogeneity of WSN in order to provide common services, like it is the case of routing, has not been sufficiently considered. For this reason, in this paper we propose a routing protocol based on traffic classification and role-assignment to enable heterogeneous WSN for cooperation. Our approach considers both QoS requirements and lifetime maximization to allow the coexistence of different applications in the heterogeneous network infrastructure.**

***Index Terms*—WSN; heterogeneous; routing;**

I. Introduction

Wireless sensor networks are nowadays commonly deployed as part of the network infrastructure in diverse scenarios. For example, control of shipping traffic in port infrastructures, monitoring of urban infrastructures as bridges or tunnels, and the control and monitoring of critical parameters within critical infrastructures. The self-configuring, autonomy and cost of deployment of WSN, are good arguments for their use, and are largely responsible of their growing popularity. With the raise of concepts such as the Future Internet (FI) and the Internet of Things (IoT), that propose the interconnection of heterogeneous networks around the globe, several research works have focused on the adaptation of WSN in order to work in these and other new similar paradigms. One part of this adaptation requires the adoption of quality of service (QoS) mechanisms to ensure that the application requirements are satisfied throughout the network. The use of QoS mechanisms in WSN creates a big challenge because the traditional QoS techniques are resource-intensive and sensors are resource-constrained. Moreover, one of the major problems in WSN is power consumption, due to the fact that sensors are not usually connected to a power supply. Instead, sensors have their own battery and in some cases they are rechargeable using, for instance, solar power or friction, with the corresponding increase in price that this entails. Due to the difficulty that changing the battery of the sensors represents, that in most cases require human intervention, energy consumption is directly related with the lifetime of the network.

We are convinced that the increasing popularity of the WSN being deployed as part of several infrastructures will promote the deployment of WSN with different purposes coexisting in the same environment. Furthermore, it makes sense to take advantage of this new situation where more sensors could mean more allowable resources for traffic routing. In order to do this, it is essential to take into consideration the influence that traffic routing collaboration could have on the behaviour and overhead of neighbours networks. This is a necessary task because collaboration is carried out via messages among the nodes of the network, and may involve a considerable consumption of energy that is a valuable resource in WSN. In fact, the routing protocols for WSN are developed to be energy-aware in order to maximize the network lifetime. This design requirement is necessary because most of the energy consumed by a sensor is due to data transmission. For this reason, until now, most of the research works related to QoS in WSN considers the lifetime as the unique parameter to be enhanced, not considering the QoS requirements specific for each application. However, this approach does not allow the deployment of collaborative networks, where different sensors can work together to provide a common service, for example, data delivery in emergency scenarios.

In this paper, we define a routing protocol based on role-assignment in order to establish a collaborative environment to send data of different nature with some QoS guarantees in WSN (R2WSN). The main idea behind R2WSN is to improve the use of the WSN without excessive lifetime utilization, as well as to open up the possibility for deploying specific-purpose WSN that can cooperate with each other, even sharing resources, in order to offer common services such as the routing service. In that sense, collaboration can provide us with the possibility of increasing the overall network capacities to achieve common objectives.

Our work is structured as follows. Section II presents an introduction to traditional routing, traffic classification and role assignment in WSN. Section III shows an analysis about the relationship between lifetime and QoS mechanisms in WSN. Section IV describes R2WSN, our routing strategy for heterogeneous and cooperative routing through WSN, while Section V defines the mathematical model to perform traffic classification and role-assignment. Finally, Section VI contains the conclusions and future work.

II. Traditional Routing, Classification and Role assignment in WSN

There are several works focused on defining efficient routing protocols for WSN. Two possible classifications of routing technologies are based on network infrastructure (flat or data-centric, hierarchical and location-based routing) and protocol operation (proactive, reactive and hybrid) [4]. Moreover, there are additional techniques to safe energy while avoiding data redundancy, as for example data aggregation [12]. This technique performs data compression by increasing the complexity of the node, although increases the lifetime by reducing the amount of data to be sent. Moreover, Tang et al [17] propose an approach to extend the lifetime of WSN while reducing delivery delay by data aggregation. Although some QoS restrictions are considered in various studies, lifetime is the most important parameter for performance in traditional WSN. For this reason, various QoS-based approaches in WSN are focused on extending the lifetime but do not consider the application requirements, and those that consider applications requirements are focused on providing real-time end-to-end guarantees [2].

Unlike routing, traffic classification is not widely studied in WSN. Indeed, traditional traffic classification has not been used by service providers to manage different types of traffic differently [13]. Moreover, traffic classification may be performed by using the statistical performance values extracted from the transmission layer that defines the behaviour of the traffic [9]. When traffic classification is used to improve the QoS, the traffic is classified according to common QoS requirements. Therefore, given that our solution will be deployed in a WSN, we have to include the energy consumption as a requirement for the calculation of the class. Rajkamal and Ranjan [15] consider the use of traffic classification for network processors in WSN. However, our aim is to enable each sensor in the network to perform data classification, the previous step to role-assignment.

Some uses for role-assignment in WSN are: role-based access control (RBAC), topology optimization and collaboration. For example, Misra and Vaish [11] use role-assignment for RBAC. Specifically, they define role-assignment based on reputation, bootstrap time and energy of the node. The aim is to define a reputation scheme in which role-assignment is used to minimize communication and delay overhead in WSN. Moreover, Dasgupta et al [7] use role-assignment in order to optimize the role-based topology of the network for maximizing the lifetime. This study is based on the existence of two roles in WSN: nodes used for information gathering and nodes used to aggregate and transmit data packets. In principle, all nodes in the network can have both roles, although some nodes are better qualified than others to perform these actions. This approach consists of using the role-assignment for increasing the lifetime without taking into account the applications requirements. Frank and Romer [10] use role-assignment to identify the functionality of nodes in WSN (e.g. gateway, cluster head) also based on topology. Finally, Weis et al [18] use role-assignment in sensor/actuator networks (SA-nets) to assign roles to devices based on their capabilities. The aim of this approach is to use the roles to allow the collaboration among the devices of the network (e.g. e-home). With this purpose they use a publish/subscribe infrastructure. This approach does not take into account the lifetime and is only focused on collaboration. Then, all the roles are based on the capabilities of the nodes, and the solution does not consider the energy level of the nodes. Role-assignment can be also used in conjunction with routing protocols for efficient data aggregation [14].

The main idea behind our work is to define a routing algorithm for WSN using traffic classification and role-assignment to enhance lifetime while improving QoS. This is directed to improve the cooperation between heterogeneous networks, that is key in future scenarios[5].

III. Lifetime and QoS in WSN

The vast majority of deployed WSN are limited in use because sensors are constrained devices with limited memory and battery, and are usually built with an unique purpose and for a specific application in order to increase the performance and to save energy. Thus, for this kind of equipment the traditional approaches to provide QoS guarantees (e.g. differential services) are not valid. Moreover, while in general networks we take into account diverse QoS parameters in some cases with the same relevance among them, such as bandwidth or data peak rate, in WSN the most important parameter to be considered is the lifetime. We understand the lifetime as the period that a WSN is still operative, either because the number of sensors that are alive are able to enable the total communication through the network (connectivity requirement) or because the network is able to perform the purpose for which it was deployed within an area of interest (this may imply the connectivity requirement, but not necessarily). In a WSN, the lifetime is generally calculated as a function of the rest of parameters that defines the node's behaviour and its characteristics (e.g. range, battery, operative system, etc.) [8]. For this reason, the lifetime can be seen as a global measure of the boundary of the network.

It is therefore understandable that improving the lifetime of WSN is a widely studied topic in the research community. For example, in [3] the authors propose the utilization of classification techniques based on fuzzy logic to improve the routing protocol with the aim of extending the lifetime of the network. They also define the cooperative routing in the sense that the nodes of the network have to specify the energy capacity that they will share with the rest of the nodes. However, with the growing popularity of WSN to achieve different goals, within different contexts and with new proposals in mind, sensors are becoming more complex and this fact impacts directly on the lifetime, as well as requiring the use of some QoS mechanisms to perform end-to-end QoS guarantees. For example, in [19] the authors try to adapt traditional differentiated services to Wireless Multimedia Sensor Networks (WMSN), where there is real-time traffic that has to be sent through the network

maintaining a low latency and high reliability. Along the same lines, in [16] the problem of traffic prioritization in WSN is considered for time-critical information flows, where only two types of flow (low and high priority) are defined. In this kind of network, we have to consider data with different priorities and this means an implicit classification of the data to be delivered through the network. However, none of these schemes are flexible or consider the selection of different paths based on the functional requirements of the nodes (eg. security).

In most cases, the actual solutions for adapting the traditional QoS mechanisms to the WSN are focused on increasing the lifetime, and forget that in the future the increment of functionality in the sensors will require a more strict control of traffic (including QoS mechanisms). Therein lies the problem, because the traditional QoS mechanisms are resource-intensive in general, and their adaptation to WSN is very complex. For example, in WSN the routing is performed hop-by-hop in an usually inaccurate topology with the corresponding delay when the path to the destination node is a long way. For this and other reasons, the adaptation of traditional mechanisms to perform QoS guarantees from traditional networks to WSN is a very hard challenge.

IV. Proposed Solution

The basic idea behind R2WSN is that the different pieces of information to be sent to the Sink require different paths to be efficiently sent through a WSN. In other words, we have two problems to solve: perform a traffic-classification (1) and identify the QoS requirements based on such traffic classification (2). First, one question to solve is whether it is possible to classify the traffic flow based on the resources that such traffic consumes and therefore on the energy wasted in sending such data through the network. So, if our objective is to prolong the lifetime of the WSN, one possible approach is to identify those flows whose transmission produces in the network a considerable decrease of energy, and send the packets using a route where the nodes have sufficient energy available to act as routers for this type of traffic. Intuitively if the most aggressive traffic (in terms of power consumption) is sent using the paths with a longer lifetime, then we are balancing the traffic through the network and increasing the total lifetime. Second, different types of traffic may require different QoS requirements. For example, if a node needs to send confidential information through the network (e.g. key interchange), it is preferable that the path chosen is composed of nodes with some security characteristics (e.g. encryption mechanisms). In that case, security can be seen as a QoS requirement because the application that sends the data needs the path to be secure to achieve the objective.

RSWSN provides (1) and (2). First, the lifetime of the network is maximized by selecting the path with more resources available, where the nodes can decide whether they have enough resources to guarantee the communication without an excessive waste of energy. Moreover, QoS guarantees are given by traffic classification and role-assignment. Figure 1 shows an example of WSN where our solution is deployed. In the example, the sensor source (s) has to send a message with security information to the destination node (d). Different colours are used to illustrate the role of each node from the perspective of s, based on the resources and characteristics of each one. Thus, although s cannot see the entire network, the message that it sends is interpreted by the intermediate nodes as if s decides the next hop in the path. The result is a map of colours that shows the role assigned to each node taking into account the information that s wants to send. In general we consider two types of roles: service-based and behaviour-based. On the one hand, service-based roles specify the type of service that a node can provide. Then these roles are the result of performing a node classification based on the characteristics of the data to be sent. On the other hand, behaviour-based roles specify a behaviour defined by the node. In this case, behaviour-based roles are the result of a decision process performed by the node. For example, Figure 1 shows five roles: security (pentagon), control information (circle), real-time (cross), charitable (triangle) and egoist (rhombus). The service-based roles are security, control information and real-time, while the behaviour-based roles are charitable and egoist. In this case the behaviour-based roles are focused on safe energy. Then, when the node is in charitable mode it means that the node can be used to route all kind of data. However, if the node is in egoist mode, then it means that this node is preserving their energy to perform their own operations. Using the behaviour-based roles to safe energy it is possible to add more roles or to delete some of the first four roles, while the role egoist is irremovable in the definition.

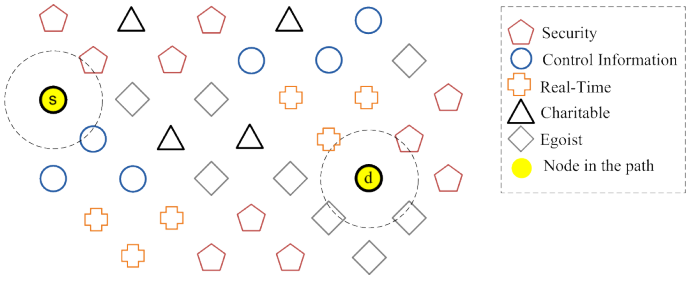

Figure 1. Example - Network view from S perspective

The goal is that the information to be transmitted from s to d is sent using the path that best satisfies a criterion. In the example the criterion is that the path has to be secure. For this reason, it is preferable to maximize the sensors in the path with security characteristics. Moreover, from any sensor the next hop has to be chosen depending on which direction the next cluster of security sensors are. Figure 2 shows a possible solution for the example, where the solid arrows represent the final path and the dotted arrows show an alternative path. Looking at picture it seems natural to wonder if the alternative path is better than the chosen path. The answer is affirmative in this case; however, we need to have information about where the destination node is. Without the location of d we only can use the local node information about general characteristics of the network, as for instance the

direction to take in order to find a security cluster. In this case, our solution consumes more energy without a significant gain in security. One possible solution is to perform a preliminary search of d from s; however, the discovery algorithm could consume more energy that the deviation previously mentioned. In conclusion, it is preferable that the final decision is made taking into account the characteristics of the network to be deployed and the purpose for which will be deployed. It is not always possible, but for example if we know that in our network the nodes should communicate with other nodes that are relatively close, then a discovery algorithm may be a good option. In our proposal we decide that we will use a discovery algorithm not aggressively (only to discover the position of d) before the transmission begins, because without previous knowledge of the network we do not know if both the source and destination nodes are far away or if the node d is accessible from a security cluster.

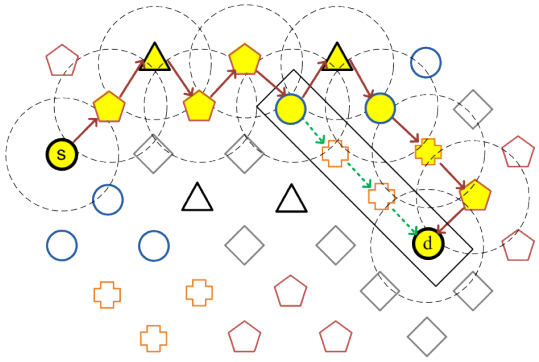

Figure 2. Example - Data transmission through a security path

Another issue is what happens if we have more than one cluster that can be used. Figure 3 represents this situation, where the node s needs to make a decision about which security cluster to use in the transmission (A or B). Intuitively, if s has to take a local decision about whether to choose e (real-time) or f (security), given the previous definition it will choose f because it belongs to the next security cluster. However, as we can see, the path through f only involves two security nodes while the rest of the nodes are real-time or control classified. It is even necessary to use an egoist node to achieve d. Instead, the path through e is better because it allows the use of the security cluster in A to protect a big part of the communication between s and d. To manage this situation, e has to know that a remote security cluster is accessible through itself. Moreover, this information has to be extensible to s. To do this, each node has to store information about their environment. In our solution, the information about the environment is summarized in a set of variables allocated to each node, one per role. Following with the example above, the security variable in e has to represent the percentage of security nodes in the path through e and the probability of reaching d from it. In that case, the security variable in e has to be higher than the security variable in f. Note that f is a security node in itself that belongs to a security cluster, so each node provides two types of information: its local role based on the local resources available, and a set of variables representing the environment of the node.

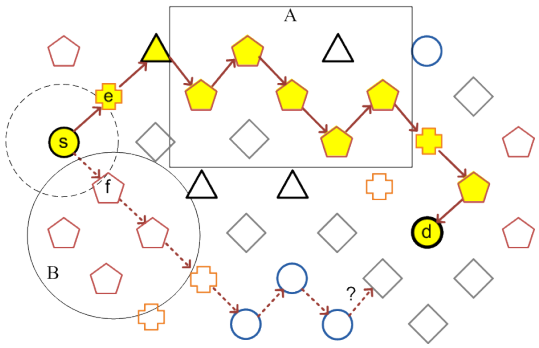

Figure 3. Example - Node Location

In our network, all the nodes have to know what they can offer to the rest of the nodes. For example, a node has to know whether its computational resources are insufficient to perform the routing of real-time traffic. Based on this, we have defined two types of behaviour in the network that are related with the role. First, we consider that a node can take the decision on whether their battery is insufficient to provide the routing service or, instead, if its resources are broad enough to provide different kinds of services to the rest of the network. If the battery is low, then a node should use its energy on its own functions, for example taking measurements of the network. In that case, the node acquires the egoist role itself. The contrary situation is when a node has sufficient resources, then it is denoted as the charitable role. Both, egoist and charitable are roles imposed by the node. The rest of the roles are denoted by the context of the network. If a node wants to send information of a certain type (e.g. security) then the intermediate nodes have to decide if they are the best nodes for routing this information based on the requirements of the node source.

V. Traffic Classifier and Role-Assignment

We consider that traffic classification is performed by the source node previously to send the data. Then, the data to be sent is marked with a service-based role in origin. We also consider that the traffic classifier is quite similar to role-assignment. In fact, the source node takes a local decision about the role of the data that can be implemented using a Bayesian network similar to Figure 4 (developed with GeNIe tool [1]) but without the behaviour-based roles. Role-assignment is somewhat more complex and involves local decisions, based only on information about the state of the node, and the collaborative decisions, that incorporate the neighbours' decisions for estimating the probabilities. Such decisions are made based on the resources available in the network, although at different levels of abstraction. For local decisions we have to take into account the local resources of the node, while for collaborative decisions we have to consider the total amount of information recovered from the neighbour nodes.

A. Local Decision: Bayesian Network

The Bayesian network defined to take local decisions is shown in Figure 4. As we can see, all the roles have to consider the Energy resource while only the roles Control, Charitable and Real-Time have to take into account the Speed, Memory and Energy resources. Moreover, the roles Charitable and Egoist have an explicit dependency on each other, denoted by the arc joining these two nodes. Indeed, one node that is Egoist cannot be denoted as Charitable at the same time and vice versa. Otherwise, the Security node is affected by the security parameters that measure the boundary of the Cryptographic method (CM) and the Trustworthiness of the node.

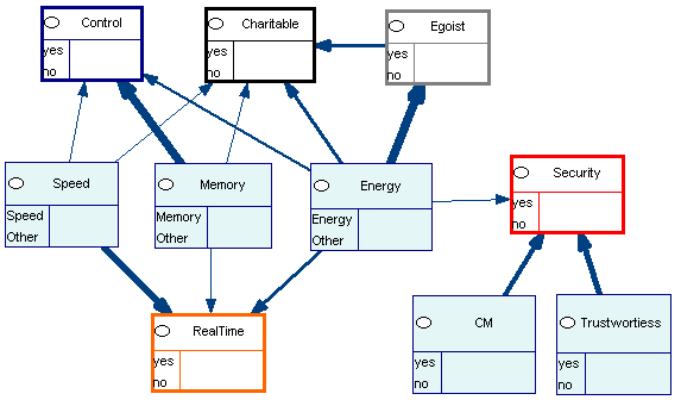

Figure 4. Bayesian Network, Local Decisions

The Bayesian network of Figure 4 has been initialized according to Table I. Said information is only representative, and indicates the importance of each parameter in the decision problem. For example, we have considered that for the Control role (first row) the Memory is the most relevant resource, followed by the Energy and Speed resources.

	Parameters (% of relevance)				
Rol	Speed	Memory	Energy	CM	Trust
Control (Co)	0.1	0.6	0.3	-	-
Real-Time (R)	0.6	0.3	0.1	-	-
Security (S)	-	-	0.1	0.3	0.6
Charitable (C)	0.3	0.3	0.4	-	-
Egoist (E)	-	-	1.0	-	-

Table I
RELEVANCE OF THE RESOURCES

Figure 4 shows graphically the relevance of each relationship in the decision process once the Bayesian network is initialized. So, the thicker the arrow, the more relevant the relationship is. For example, in our scenario we have considered that for a Control communication the Memory resource is more relevant than the Speed resource, while in a Real-time communication Speed is more important than the percentage of allowable Memory in the node.

In our approach, the blue boxes will be modified according to the internal values in each sensor, so it depends on the node state. Then, to perform the decision process, each node modifies the values Speed, Memory, Energy, CM and Trustworthiness according with its internal values (e.g. percentage of memory available), and then retrieves the probability for each service-based role.

Finally, a sensor has the local role X if the probability of the role, denoted by $p(X)$ (simplification of $p(X = yes)$), is higher than the predefined threshold U_X. For example, $p(C)_s$ is the probability that the sensor s is Charitable, so when $p(C)_s > U_C$, then s is a Charitable node. We considered that all thresholds are equal to 0.5 (50%), although these values could be modified to be more ($U_C < 0.5$) or less restrictive ($U_C > 0.5$).

B. Cooperative Decisions

Cooperative decisions are taken by considering the sum of the local probabilities of the nodes in the network. These local probabilities are extracted from the Bayesian model that was presented in the previous point (V-A). In our solution, to perform a cooperative decision, each node stores a set of variables that indicates the probability to be connected with each type of node. In the proposed scenario there are five roles, so we have to consider the probability for the node n to be connected with a set of control, charitable, real-time, security or egoist nodes. Then, given a node n in a network with N nodes, where V_n is the number of neighbours of the node n, the network probability (P) that indicates if n is near to a network with role X, is calculated based on the local probability (p) of each neighbour of n using the Expression 1. The constant K ($\cong$ 0.02) increases the global probability $P(X)$ based on V_{nx}, that is the number of neighbours of type X for the node n. K is necessary to detect clusters of sensors of a given role. Specially in the case of egoist clusters, as is shown in Figure 5, K increases $P(E)$ for the node $e1$, so the node s will chose the alternative node to send data.

$$P(X)_n = (\frac{1}{V_n}\sum_{i=1}^{N} p(X)_i * nb(n,i)) + K * V_{nx}; \quad (1)$$

$$nb(n,i) = \begin{cases} 1 & if \text{ i is neighbour of n} \\ 0 & other \end{cases} \quad (2)$$

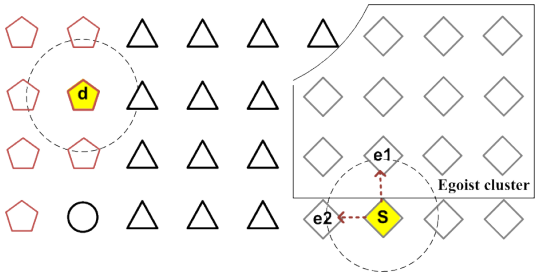

Figure 5. Egoist clusters

Nevertheless, if we use the network probability $P(X)_i$ instead of $p(X)_i$ we can indirectly collect the total measurements of data. Then, Expression 3 gives us more information than Expression 1.

$$P(X)_n = \begin{cases} p(X)_n & if\ V_n = 0 \\ \frac{1}{V_n} \sum_{i=1}^{N} \frac{P(X)_i * V_i + p(X)_i}{V_i + 1} * nb(n,i) & other \end{cases} \quad (3)$$

In fact each node decides which is the next hop by comparing the value of P for each sensor that it locates in a specific area, so the chosen sensor s to send the data of type X is the sensor with the maximum value of $P(X)$. Formally, it means that Expression 4 has to be satisfied by s.

$$P(X)_s \geq P(X)_i, \forall i \in \{k|nb(n,k) == 1\} \quad (4)$$

Besides, s should not be egoist ($p(E)_s < U_E$), and should be the nearest to the destination node d than the previous node. Then, supposing that we know the location of d and according with the law of cosines [6], Expression 5 has to be satisfied by s, where a, b and c are the results of calculating the euclidean distance between the sensors s and d, the previous sensor o and s, and o and d, respectively.

$$arcos(\frac{a^2 - b^2 - c^2}{-2bc}) < 90 \quad (5)$$

Note that, although we use Bayesian network to perform local decisions, such approach can be replaced by mathematical expressions for increasing the dynamism of the network, avoiding the redefinition of the network when a new role is included. In the same way, cooperative decisions can be performed by using other different approach more adequate to the environment in which the solution will be deployed.

VI. Conclusions and Future Work

In this paper we have introduced R2WSN, a routing protocol for heterogeneous WSN by using traffic classification and role-assignment, that considers not only the lifetime but also the QoS application preferences for data transmission. We also provide an example to perform traffic classification and role-assignment by using Bayesian Networks. There are no current routing protocols for WSN that considers QoS restrictions and lifetime at the same level as we do in this work. Moreover, the lack of an existing infrastructure for allowing such collaboration makes very difficult to test our approach. So, further steps in this direction are devised to design the problem using a simulator tool to perform performance analysis. Note that in our solution we propose an example of traffic classification and role-assignment. However, it is possible to define them based on other different criteria. For this reason, an interesting analysis can be performed by comparing different traffic classification and role-assignment solutions based on the environment to be deployed, as well as to observe what approach is more general and maximizes the lifetime while preserving the QoS restrictions more efficiently.

VII. Acknowledgment

This work has been partially supported by the Spanish Ministry of Science and Innovation through the projects SPRINT (TIN2009-09237) and IOT-SEC (ACI2009-0949), being the first one also co-funded by FEDER. Additionally, it has been funded by Junta de Andalucia through the project PISCIS (TIC-6334). The first author has been funded by the Spanish FPI Research Programme.

References

[1] Genie tool, http://genie.sis.pitt.edu/.

[2] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3):325 – 349, 2005.

[3] S.G. Akojwar and R.M. Patrikar. Improving life time of wireless sensor networks using neural network based classification techniques with cooperative routing. *International Journal of Communications*, 1(2):75–86, 2008.

[4] J.N. Al-Karaki et al. Routing techniques in wireless sensor networks: a survey. *Wireless Communications, IEEE*, 11(6):6 – 28, dec. 2004.

[5] K. Anagnostakis et al. Coverage: detecting and reacting to worm epidemics using cooperation and validation. *International Journal of Information Security*, 6:361–378, 2007. 10.1007/s10207-007-0032-z.

[6] J. Casey. *A Treatise on Spherical Trigonometry: And Its Application to Geodesy and Astronomy with Numerous Examples*. Longmans, Green, & Company, 1889.

[7] K. Dasgupta et al. Topology-aware placement and role assignment for energy-efficient information gathering in sensor networks. In *Computers and Communication, 2003. (ISCC 2003). Proceedings. Eighth IEEE International Symposium on*, pages 341 – 348 vol.1, june-3 july 2003.

[8] I. Dietrich and F. Dressler. On the lifetime of wireless sensor networks. *ACM Trans. Sen. Netw.*, 5:5:1–5:39, February 2009.

[9] J. Erman et al. Traffic classification using clustering algorithms. In *Proceedings of the 2006 SIGCOMM workshop on Mining network data*, MineNet '06, pages 281–286, New York, NY, USA, 2006. ACM.

[10] C. Frank and K. Römer. Algorithms for generic role assignment in wireless sensor networks. In *Proceedings of the 3rd international conference on Embedded networked sensor systems*, SenSys '05, pages 230–242, New York, NY, USA, 2005. ACM.

[11] S. Misra and A. Vaish. Reputation-based role assignment for role-based access control in wireless sensor networks. *Computer Communications*, 34(3):281 – 294, 2011.

[12] P. Nie and B. Li. A cluster-based data aggregation architecture in wsn for structural health monitoring. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pages 546 –552, 2011.

[13] J. Park et al. Internet traffic classification for scalable qos provision. In *Multimedia and Expo, 2006 IEEE International Conference on*, pages 1221 –1224, july 2006.

[14] M. Patel et al. Role assignment for data aggregation in wireless sensor networks. *Advanced Information Networking and Applications Workshops, International Conference on*, 2:390–395, 2007.

[15] R. Rajkamal and P. Vanaja Ranjan. Packet classification for network processors in wsn traffic using ann. In *Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on*, pages 707–710.

[16] W. L. Tan et al. Performance evaluation of differentiated services mechanisms over wireless sensor networks. In *Vehicular Technology Conference, 2006. VTC-2006 IEEE 64th*, pages 1 –5, sept. 2006.

[17] S. Tang et al. Dawn: Energy efficient data aggregation in wsn with mobile sinks. In *Quality of Service (IWQoS), 2010 18th International Workshop on*, pages 1 –9, june 2010.

[18] T. Weis et al. Self-organizing and self-stabilizing role assignment in sensor/actuator networks. In Robert Meersman and Zahir Tari, editors, *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE*, volume 4276 of *Lecture Notes in Computer Science*, pages 1807–1824. Springer Berlin / Heidelberg, 2006.

[19] M.H. Yaghmaee and D. Adjeroh. A model for differentiated service support in wireless multimedia sensor networks. In *Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on*, pages 1 –6, aug. 2008.