The implications of Service Virtualisation on the routing procedure in Wireless Sensor Networks

Theodore Zahariadis, Lambros Sarakis, Helen C. Leligou, Antonis Hatjiefremidis, Stamatis Voliotis
Technological Educational Institute of Halkida,
Psahna, Evias, 34400
{Zahariad, sarakis, leligou ahatzi, svoliotis}@teihal.gr

Kyriakos Georgouleas,
Hellenic Aerospace Industry
Schimatari, Greece
GEORGOULEAS.Kiriakos@haicorp.com

Abstract— **The proliferation of Wireless Sensor Networks (WSNs) has driven the design of Virtual Sensor Networks (VSNs) which decouple the physical sensor deployment from the applications running on top of it. In this concept, the Wireless Sensor Networks are no longer deployed to support a specific service but are capable of collaborating among each other (even if they belong to different administrator domains or if they comprise of heterogeneous systems) towards realizing new services and applications. The design and development of VSNs are at the focus of the VITRO project and it currently develops a reference architecture [1] to enable the realization of scalable, flexible, adaptive, energy-efficient and trust-aware Virtual Sensor Network platforms. In this paper, we investigate the requirements that virtualization imposes on the routing procedure of the involved WSNs. Given that the routing protocol and the adopted routing metric affects the achieved quality of service performance, the support of different applications over the same WSN infrastructure mandates a)traffic handling differentiation from the routing protocol and b)proper coordination of the involved resource controller and VSN configuration management modules.**

Keywords-component; Wireless Sensor Networks; Virtualisation; routing protocol

I. INTRODUCTION

The proliferation of Wireless Sensor Networks (WSNs) has driven the design of Virtual Sensor Networks (VSNs) which decouple the physical sensor deployment from the applications running on top of it. In this concept, the Wireless Sensor Networks are no longer deployed to support a specific service but are capable of collaborating among each other (even if they belong to different administrator domains or if they comprise of heterogeneous systems) towards realizing new services and applications. The design and development of VSNs are at the focus of the VITRO project and it currently develops a reference architecture [1] to enable the realization of scalable, flexible, adaptive, energy-efficient and trust-aware Virtual Sensor Network platforms. Emphasis is placed on advanced interoperability, on simple deployment and low management cost. In this architecture, which uses the Internet as the physical bearer between sensor platforms and applications, sensors are deployed by some organizations and can then be used by other organizations for realizing different applications. Virtualization implies apart from service virtualization, virtualization of the node and network resources which are necessary to support each service. This dictates on one hand the advanced sensor design (to support advanced features in several fields including energy saving, routing capability, middleware) and on the other hand, middleware design to mediate between applications and sensors.

In this paper, we investigate the requirements that virtualization imposes on the routing procedure of the involved WSNs. Given that the routing protocol and the adopted routing metric affects the achieved quality of service performance, the support of different applications over the same WSN infrastructure mandates a)traffic handling differentiation from the routing protocol which is not a straightforward task and b)proper coordination of the involved resource controller and VSN configuration management modules. With respect to the routing protocol, we define how different quality of service levels can be offered based on the RPL protocol [2] which is currently under standardization by IETF ROLL group. We propose the initiation of different instances per application and the use of different routing metrics per instance to achieve the desired Quality of Service differentiation and we validate our approach using computer simulations.

The rest of the paper is organized as follows: in section II, the sensor network virtualization concept is discussed to draw its implications on routing in section II where we also describe the functionality that needs to be carried out in the different nodes in the network and the routing protocol operation to meet the requirements imposed by the virtualization. In section IV we provide simulation results to show how the different adopted metrics can lead to different performance aspect optimization over the same sensor network. Finally, conclusions are drawn in section V.

II. SENSOR NETWORK VIRTUALIZATION

Virtualization of network resources has been identified as a key technology for Future Internet architecture and is actively used in current research testbeds ([3],[4]). By virtualizing both node and link resources of a substrate network, multiple virtual network topologies with widely varying characteristics can be created and co-hosted on the same physical hardware. The main concept of VSN targets on repurposing existing WSNs to cope with different tasking functionality beyond the scope of the original sensor design and deployment and share network resources. Given the heterogeneity of the deployed WSNs, it is great challenge to make effective usage of such resources.

Until now, several attempts have been performed targeting network virtualization of legacy networks and virtualization impact in Future Internet architecture. A complete network virtualization environment must deal with a number of key issues like interfacing based on well-defined standards, bootstrapping defining the initial connectivity before virtual networks are created, admission control of user requests, resource scheduling and topology discovery that will enable service providers to identify interconnections between physical nodes and examine their availability to meet virtual network requirements. A key issue, known as virtual network embedding, is the optimization of node resources and links utilization when a mapping of multiple virtual networks over a physical infrastructure occurs. The primary objective of this function is to allow a maximum number of virtual networks to co-exist on top of the same substrate while reducing cost for users and increasing revenue for providers.

However, the situation in sensor network virtualization is different from traditional networks as WSNs are different from wired networks in many aspects:

- Every virtual network formation contributes in energy consumption, a valuable resource for VSNs which are mainly considered as battery operated devices.
- Network traffic in VSNs can be mainly considered as convergecast (or otherwise multipoint-to-point) traffic from multiple sources to a single sink node. While situations that deviate from this traffic pattern exist, in the majority of situations bandwidth stress occurs at links directly connected with the sink node where the forwarding burden is increased. This means that topology discovery and monitoring of every possible link is of less importance while in parallel it increases energy consumption bandwidth utilization for routing control messages.
- Links failures, instabilities and temporal variability are more likely to occur in VSNs than in wired networks.

These WSN system intricacies dictate the clear definition of virtualization objective to avoid unnecessary functionality whose execution consumes scarce node and network which consumes The virtualization objectives identified in VITRO and detailed in [1] include:

Resource virtualisation: Network and node resources play a very significant role at all layers of a VSN. Given that the VITRO system will consist of heterogeneous devices with different capabilities and communication resources, this is translated in a)

- Communication resources/connectivity: As the heterogeneous devices of the VITRO system may also differ in their communication capabilities, to optimise the overall network performance, routing can take advantage of the heterogeneous neighbours capabilities. Thus, the sensor transmission range or the supported wireless interface will be considered as an attribute taken into account when routing decisions are made.
- Dynamic Resource control: The (heterogeneous) devices included in a VSN may be battery or mains powered. As the energy consumption depends on a number of operational parameters, these may be tuned dynamically to prolong the network lifetime. Moreover, a node plugged to power supply may be preferred for routing purposes to battery-operated ones. On the other hand the dynamic value of the remaining energy is also valuable for the routing protocol, since taking into account the neighbour's energy levels significant reduction in the energy consumption rate can be achieved [5]. The fact that it is a requirement to exchange such information in VITRO, can and will be exploited also at the routing layer to prolong the network lifetime.
- Hardware node resources affect the complexity of the routing protocol that can be executed. For example, given that security is one of the key requirements, the implementation of trust logic can be distributed among nodes in a proportional to hardware resources manner.

Security services virtualization: Different security levels have to be supported to improve the probability of reaching the destination for special purpose messages. These messages may include alarm-related messages, service discovery messages which are of higher priority (more vital) in some applications than regular messages carrying sensed data. The distinction of different security levels implies that the applications run in the VSN have to be classified to the supported levels. To enhance security, a suitable trust management scheme will be designed and validated. Different aspects of the heterogeneous nodes will be monitored to evaluate the trust-worthiness of the nodes with respect to a set of functions. This approach will be pursued at the network layer to evaluate the sincere cooperation of node in the routing procedure.

In important requirement that in Virtual Sensor Network is the support of *scalability and mobility*. Although virtualisation targets the reduction of the number of devices installed in an area by exploiting already installed sensors, in this uncontrolled environment, the number of nodes in the neighbourhood can fluctuate. Thus, it is mandatory for the relevant protocols to support both scalability and mobility.

III. ROUTING IN VSNS

The virtualization requirements affect the design choice and directions that the routing protocol has to follow. The support of different applications over the same WSN infrastructure mandates a) traffic handling differentiation from the routing protocol which is not a straightforward task and b) proper coordination of the involved resource controller and VSN configuration management modules. In the sequel, we first deal with the routing protocol requirements and then we discuss the need to configuration management from the VSN controller.

A. Routing protocol

To differentiate among node of different capabilities (with respect to e.g. energy and connectivity), each node has to be associated with a set of attributes describing its resources (hardware, connectivity, energy, and possibly security/trust-

related functionality). To support node resource virtualization, first the necessary messages and ways to communicate the relevant information have to be defined and second, the algorithms that will use this information to turn it into benefits need to be designed. In legacy WSN routing protocols, the main routing metrics were distance or delay. In VITRO, the legacy routing metrics will be augmented to include the virtualized resources, which implies that:

- A more sophisticated routing algorithm that takes into account more node-related information
- The neighbour list becomes wider since more information per neighbour has to be maintained.
- The memory and processing requirements increase and thus specific attention has to paid to the trade-off between implementation cost with additional functionality.
- The routing protocol has to define how the information regarding the virtualized resources will be exchanged.

The target of the VSN formation is to allow a larger number of heterogeneous nodes existing in an area to communicate directly. This implies that the neighbor set of each node will increase since nodes from different administrative domains, executing different applications, and of different hardware will cooperate. Increasing the length of the neighbour list, results in higher memory and processing requirements. Given that the memory and processing resources are rather restricted in state-of-the-art sensor nodes, special care has to be taken to design a routing solution capable of dealing with this high number of neighbours.

The requirement to support different security levels mandates the realization of a trust management scheme where nodes monitor the behavior of their neighbours to evaluate their trustworthiness [6]. Once the trustworthiness is evaluated, the distinction of different security levels can be performed either a) by defining trust value thresholds or b)by defining different routing functions depending on the metric to emphasize on.

The update of the energy level and node status, in essence it coincides with the node resource virtualization and has thus been dealt with previously. Coming to the need to support scalability and mobility, the trusted routing solution has to be appropriately tailored. While geographical routing inherently support scalability and mobility, a solution that enables node differentiation and routing decision making based on different routing metrics is preferable.

A routing protocol satisfying the above requirements is currently under standardization by the IETF ROLL (Routing Over Low power and Lossy networks) group designed for Low power Lossy Link Networks (LLNs). This group has standardized the so-called IPv6 Routing Protocol for LLNs (RPL) [2] which provides a mechanism whereby multipoint-to-point traffic from devices inside the Low power and Lossy Network is routed towards a central control point, as well as point-to multipoint traffic from the central control point to the devices inside the LLN. RPL constructs Directed Acyclic Graphs (DAG) and defines the rules based on which every node selects a neighbor as its parent in the DAG, thus forming a tree. To cover the diverse requirements imposed by different applications, ROLL has specified in [7] a set of link and node routing metrics and constraints (which can be static or dynamic) suitable to Low Power and Lossy link Networks to be used in RPL. This document does not provide details on the quantification of each routing metric, *leaving it to the user to decide how to express each metric and which metric to use.* Moreover, it allows the combination of multiple routing metrics and constraints. Up to now, ROLL has specified in [8] only Objective Function 0, (OF0) where the hop count is the only routing metric adopted.

The RPL protocol offers an additional feature which is very crucial for supporting virtual networks over LLNs: it supports the construction of multiple routing trees with the same or different destination (root) node based on different routing metrics, which form the so-called routing instances. In other words, different routing paths from the sensor nodes towards the sink node can be constructed to service different applications optimized a different performance aspect each time. For example, for e-health application, high reliability and low latency are required while for temperature and condition control applications, extended network lifetime is far more important than reliability in the sense that losing a data packet generated by a temperature sensor to control the air conditioning system is less vital that a data packet generated by an electrocardiogram sensor. For this reason, we anticipate that the adoption of RPL protocol brings important benefits when Wireless Sensor Network virtualization comes into the scene.

Considering for example the WSN topology of Fig. 1, it is possible that future user requests that want to utilize part of the resources offered by the whole system of sensor nodes, may have specific routing requirements to avoid unstable links or to avoid energy weak nodes instead of selecting routes with the minimum hop count.

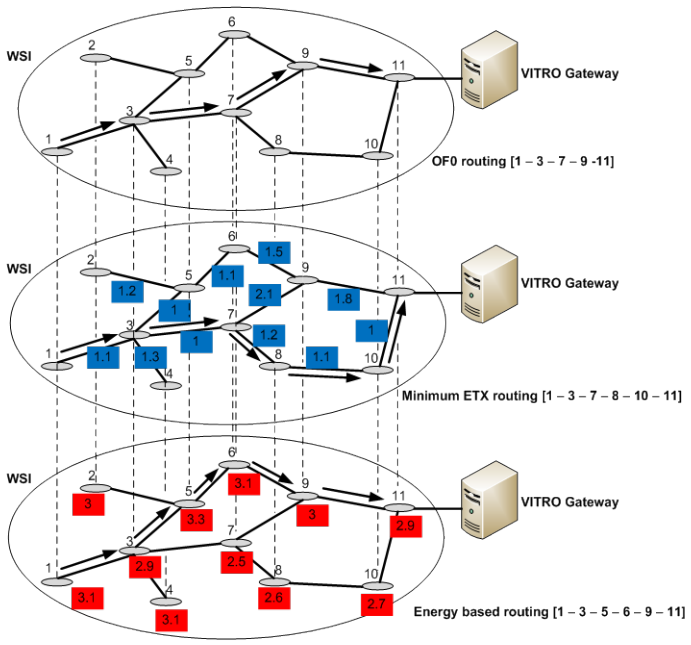

Figure 1. Multiple routing instances inside the same Wireless Sensor Island

In this case, additional routing instances that run in parallel and meet routing objectives are created. The different paths for routing from node 1 to destination node according to different QoS routing policies are presented in Fig. 1 where three routing instances are shown which may corresponds to three different applications. All instances forward traffic to node 11 which is connected to the VITRO gateway (the VSN island supporting the RPL protocol) but in each instance different quality of service is achieved since in the instance shown at the top of the figure routing is decided based only on the hop count, the next instance is decided based on the ETX metric which optimizes the link layer losses as will be further discussed later on and the last instance (shown at the bottom of the figure) optimizes energy. The different routing criteria used in the three instances lead to the construction of a different routing path from node 1 to the sink node 11 as also shown in the figure.

Unfortunately, the VSNs will be burdened with the additional control ICMPv6 control messages of every new RPL instance. While mechanisms to alleviate excessive network control traffic exist in RPL (e.g. the adaptive trickle timers), the creation of a new RPL routing instance must be balanced with its energy consumption contribution.

B. Routing procedure configuration and management

VITRO network virtualization extends to multiple entities and roles of the VITRO architecture and well-defined interfaces are required to build, maintain and keep up to date the virtual network. In this section we focus on operations and interfaces related to routing operation that participate in VSN formation and operation and we assume that the VITRO WSN routing is based on RPL with enhancements for trusted operation. RPL inherently supports coexistence of multiple instances reflecting different priorities in routing policies as already described. An overview of Resource/services advertisement and assignment to different Service Providers are part the interfacing between the routing layer of and the VITRO middleware functionality.

Once the RPL protocol has been adopted as a tool to offer different QoS to different application, the modules that map the application requirements to RPL protocol configuration specification have to be designed and implemented. While the overall VSN architecture has been presented in [1], here we will detail the modules involved in the routing procedure and will be analysed with the help of figure 2.

In fig. 2, all the participating entities of the VITRO architecture that interact and participate in sensor network virtualization are presented. Each Wireless Sensor Island (WSI) consists of a number of sensor nodes with routes established among them based on the exchange of RPL DIO (DODAG Information Object) and DIS (DODAG Information Solicitation) messages. As in sensor networks information is usually collected at a central point, the sink node is synonymous to root node in RPL DAG construction. After the graph construction, starting from the root and following the RPL rules, both routing control messages and middleware/application messages are exchanged ending at the sink node. This node is connected to a Gateway device where the VITRO Gateway Manager (VGM) software module runs through a serial/, USB or TCP/IP interface. In this way, all application data and network layer control messages destined at sink node are available to gateway.

A user request will be examined from VGM for resource/service availability and accepted for further processing only if the underlying sensor network has resources to meet user demands. As user requests arrive at arbitrary time, resource allocation is a dynamic online procedure something that complicates the optimization of resources usage. Next to acceptance of resources, availability is the examination of routing requirements of the user request to determine if a new routing instance is necessary or if it can be served from the existing instances. If a new routing instance is required, the objective function that meets user demands is derived and a new RPL instance is created. The objective function of this instance will be stored in the RPL instances repository and the new instance will be propagated from the root node to the whole sensor network. The case of a request where resource requirements are met but routing requirements cannot be guaranteed under any objective function is also possible and in this case the request is rejected. An RPL instance can also be deleted if the user request it supports has finished. In this case, VGM will inform root node to stop broadcasting DIO messages and sensors' middleware will inform network layer to stop keeping a routing table for this instance. Another dimension related to new RPL instance creation that must be taken into account is the time interval needed for instance creation, especially in large topologies, since graph connectivity of all the nodes based on the new routing requirements must be guaranteed prior to its usage.

The Routing Classifier module plays a twofold role in the examination of a new RPL instance creation. Firstly, an estimation of the availability of network resources is provided checking the impact of the new routing instance in resources like bandwidth and power consumption. If adequate resources are available and user request is better fulfilled with a new routing policy then a new OF (Objective Function) is selected and propagated from the sink node. As depicted in Figure 2, the Routing Classifier is constructed of Energy Evaluator, Bandwidth Evaluator, and Trust Management sub-modules.

Energy Evaluator is in charge of energy consumption estimation of the new routing instance.

Energy consumption in RPL can be attributed in the following parameters:

$$E_{inst} = E_{DIO} + E_{DIS} + E_{ret} + E_{loop}$$

Where

E_{DIO} = energy consumed for DIO messages,

E_{DIS} = energy consumed for DIS messages,

E_{ret} = energy consumed for retransmissions due to link failures,

E_{loop} = energy consumed where loop and inconsistencies are detected that lead to trickle timer reset.

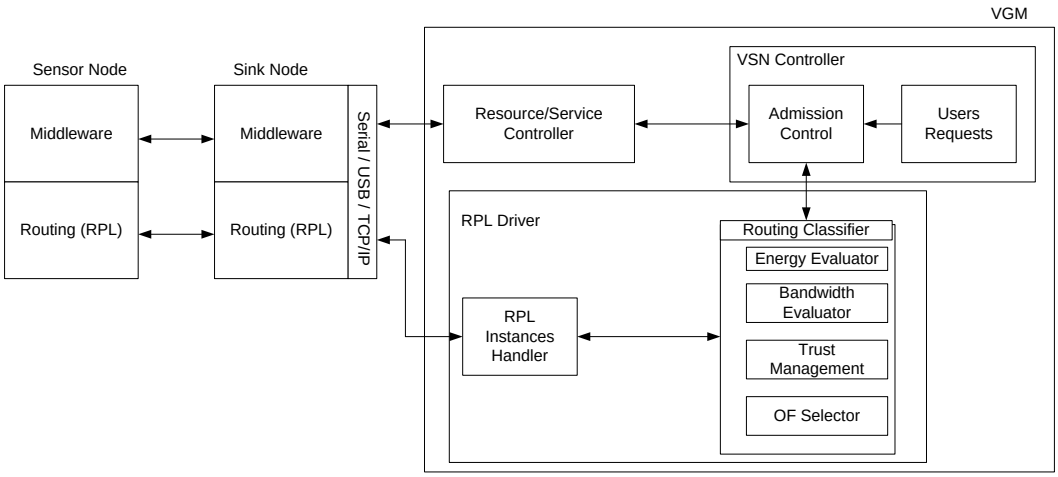

Figure 2. Participating entities for multiple RPL instances creation and management in VITRO Virtual Sensor Networks

In the above formula, the energy consumed at microcontroller unit for rank and all other computations is considered negligible and only factors related to message transmission are considered. E_{DIS} for DODAG Information Solicitation messages can be considered as a factor only present in the first RPL instance and absent in all subsequent since after the first DODAG advertisement with the DIO messages, DIS periodic transmission is suppressed. All the other three factors are present if multiple RPL instances are instantiated and all of them exhibit a highly random nature. E_{DIO} is affected by the operation of the trickle timer which randomly selects a number between the current and the double to the current transmission interval until a random maximum rate is achieved. Link failures and loops creation also cannot be deterministically calculated in advance and random factors must be inserted to determine probabilistically their future behavior. This is applicable to DIO and DIS messages under local/global repair situations.

Simulation results can be used for the derivation of RPL energy consumption contribution for different topologies and a large number of different scenarios. Based on these results, a probabilistic function for the energy consumption contribution of an RPL instance can be determined. Using this function, the knowledge of the remaining energy at each node, the duration of the new user request and the utilization of required resources, Energy evaluator permits the initiation of a new RPL routing instance only if:

$$E > \sum_{i=1}^{n} E_{Ri} + \sum_{j=1}^{m} E_{Aj}$$

For a node running m applications and n routing instances where

E_{Aj} is the expected energy consumption for the node for application j,

E_{Ri} is the expected energy consumption for the node for routing instance i and

E is the expected total energy of the node which can be estimated based on battery capacity, radio consumption for transmission and reception and mcu, peripheral and sensors consumption.

It must be noted that the impact of routing instance energy consumption is greater if requests with long-term or permanent characteristics are issued from VITRO users.

The ***Bandwidth evaluator*** will permit the creation of the new RPL instance only if the sum of the current links utilization monitored for 1-hop neighbors at each VGM and the bandwidth demands of the new routing request does not exceed the maximum bandwidth of the link. The traffic amount contributed to the new routing instance can be considered negligible since after the initialization phase a DIO message is broadcasted every several seconds.

The ***Trust Manager*** is responsible for the evaluation of the trust requirements of the user request and the module should reject requests of certain trust level if trust is not supported from the underlying WSI.

The final stage of the Routing Classifier is the ***Objective Function Selector*** where the user request information is used to determine the metrics/constraints that will be included in the OF used by the new RPL instance. The repository of RPL instances will be consulted for active RPL instances and updated for every new RPL instance. At the end of this procedure, the sink node will be informed from VGM to start advertising the new RPL instance through the use of DIO messages.

IV. ROUTING METRICS USAGE IN VSN CONSTRUCTION

In RPL specification, a large space for metrics/constraints has been left to meet different objectives and QoS routing policies. A first distinction in RPL metrics is between node and link metrics, with node metrics including node state and attributes (e.g. cryptography support), node energy and Hop Count and link metrics including throughput, latency, Link Reliability and link Color. Moreover, to enrich RPL with

security features, we have defined a trust-related metric named Packet Forwarding Indication (PFI).

To assess the impact of adopting different routing metrics on the achieved performance as well as combinations among them, we have developed a simulation model based on the JSIM open simulation platform. This model [9] allows for flexibly configuring nodes attributes as well as link dynamics. It also supports the creation of multiple instances over the same LLN.

Based on the extensive simulation scenarios carried out we concluded that each routing metric used on its own (i.e. not combined with each other) can lead to different performance aspect optimization as described in table I.

TABLE I. ROUTING METRICS AND AFFECTED PEROFRMANCE ASPECTS

Primary routing metric	Routing operation	Main Performance characteristic
HC	Shortest path	Low latency
ETX	More reliable link with respect to layer 2 performance	Low packet loss - Low latency
RSSI	More reliable link with respect to signal strength (does not take into account congestion for example)	Increased reliability with respect to transmissions successfully received by neighbours, high latency
PFI	More reliable neighbor	Efficient detection of misbehaving nodes, low packet loss due to misbehaviours
RE	Avoids systematically using the same neighbors for forwarding exhausting their energy	Network lifetime elongation

To evaluate the impact of different metric on the achieved performance, we have run multiple scenario sets. As our aim in this paper is to prove that it is possible to optimize different performance aspects using the same routing protocol adopting different routing metric, we indicatively include here the scenario set which focused on the comparison between the ETX metric capturing link layer losses and the PFI metric capturing the effect of routing layer losses caused by misbehaving nodes. The results in terms of routing layer losses as a function of misbehaving nodes are shown in figure 3.

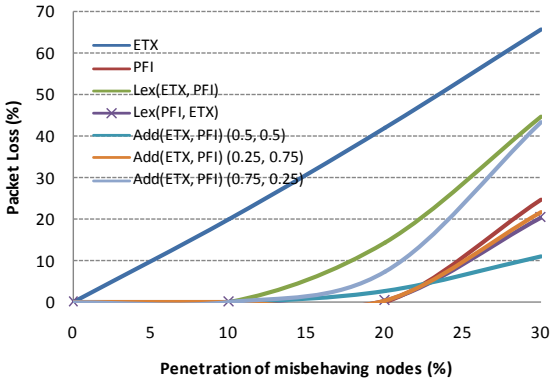

Figure 3. Packet loss vs. penetration of misbehaving nodes for different combinations of ETX and PFI routing metrics

It is evident that the packet loss observed for the case where only ETX is taken into account is the highest, since such a routing metric does not take into account any misbehaving node behavior. In other words, if a node acknowledges the reception of frames, even if this node does not actually forward this packet, the source node will continue to co-operate with it. Any other objective function taking into account PFI succeeds in detecting these misbehaving nodes and avoids them. Although performance differences exist among them, the difference from the ETX case is evident.

V. CONCLUSIONS

Given the wide proliferation of wireless sensor networks, the next challenge that these systems have to face is the virtualization of resources so that they can support repurposing and service multiple application run concurrently. In this paper, we have focused on the requirements that the virtualization concept imposes on the routing procedure. We have proposed the use of RPL protocol as a tool to efficiently support resource virtualization and Quality of service differentiation over WSNs. We have defined the functionality that has to be executed in the sensor network nodes in order to support virtualization and exploit the features offered by RPL. Finally we provided guidelines on the selection of routing metrics to optimize performance aspects.

ACKNOWLEDGMENT

The work presented in this paper was partially supported by the EU-funded FP7 ICT-257245 VITRO project.

REFERENCES

[1] Lambros Sarakis, Theodore Zahariadis, Helen-Catherine Leligou and Mischa Dohler, «A Framework for Service Provisioning in Virtual Sensor Networks», EURASIP Journal on Wireless Communications and Networking, April 2012, doi:10.1186/1687-1499-2012-135.

[2] T. Winter, et. Al. "RPL: IPv6 Routing Protocol for Low power and Lossy Networks ", March 13, 2011, available at: https://svn.tools.ietf.org/html/draft‐ietf‐roll‐rpl‐19

[3] N. M. Chowdhary, M. R. Rahman and R. Boutaba, "Virtual network embedding with coordinated node and link mapping", In Proceedings of IEEE INFOCOM, 2009

[4] 4WARD Project, HTUhttp://www.4ward‐project.euUTH

[5] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas, "Energy efficiency and implementation cost of trust-aware routing solutions in WSNs", 14th Panhellenic Conference on Informatics (PCI 2010), 10-12 September 2010, Tripoli, Greece

[6] Theodore Zahariadis, Helen Leligou, Panagiotis Trakadas, Stamatis Voliotis, "Trust management in Wireless sensor Networks" European Transaction on Telecommunications, Vol. 21, Issue 4, June 2010, pp: 386-395 (DOI 10.1002/ett.1413).

[7] JP. Vasseur, et. Al."Routing Metrics used for Path Calculation in Low Power and Lossy Networks", March 1, 2011, available at http://tools.ietf.org/pdf/draft-ietf-roll-routing-metrics-19.pdf

[8] P. Thubert, "RPL Objective Function Zero", September 5, 2011, available at http://tools.ietf.org/html/draft-ietf-roll-of0-20

[9] P. Karkazis, P. Trakadas, T. Zahariadis, A. Hatziefremidis, H. C. Leligou, "RPL Modeling in J-Sim Platform", in 9th International Conference on Networked Sensing Systems, Antwerp, Belgum, June 11-14, 2012