A framework for Wireless Sensor Networks performance monitoring

Vasco Pereira, Jorge Sá Silva, Edmundo Monteiro
Laboratory of Communications and Telematics, DEI / CISUC - University of Coimbra
Coimbra, Portugal
e-mail: {vasco, sasilva, edmundo} @dei.uc.pt

Abstract— **A new generation of Wireless Sensor Networks (WSNs) is expanding to performance critical environments. In these new scenarios, performance must be monitored and effectively measured, in order to guarantee that the network fulfills initial expectations. However, measuring performance in WSN has not the same requirements as measuring performance in traditional networks. While new specific WSN metrics have been proposed to cope with the new specific needs of these networks, a global performance framework for evaluating WSN does not yet exist. In this paper, WSN specific communication performance needs are analyzed and, to measure them, an initial approach to a global framework of WSN performance metrics is proposed. These metrics are intended to evaluate the real-time performance of a WSN, providing the necessary measurements to indicate if the QoS expectations are being met.**

Keywords- Wireless Sensor Networks, Performance evaluation, Quality of Service, Taxonomy

I. INTRODUCTION

Until recently, Wireless Sensor Networks (WSN) were used without controlled performance, in non-critical environments. The aim to extend the flexibility and unique characteristics of these networks to a broader set of applications and scenarios, where Quality of Service (QoS) is essential, poses new challenges that must be met by a new approach. Performance controlled WSNs imply not only that the network must assure a pre-determined QoS level, to provide for application specific demands, but also that the QoS must be maintained over time. As an example, WSNs that run critical industrial applications belong to this group.

However, QoS in WSN is much more challenging than in traditional networks [1], not only by the obvious hardware and software restrictions, but also because it is heavily dependent on the application used, with different applications demanding different performance (eg. delay, loss, coverage, energy waste, response time). To worsen this scenario, there is no standardized framework for measuring performance in WSN, being difficult to understand if a network complies with the necessities of a new application to deploy, or to compare different networks.

In this paper, a global WSN performance framework is proposed and a new set of performance metrics, related to the transmission of packets in WSN is defined. This framework is derived from the Communication Performance branch of a previously presented WSN requirements taxonomy [2]. The goal is to be able to have a common WSN performance framework with which performance between different networks may be compared and application needs may be confronted.

The remainder of the paper is structured as follows. Section II presents some of the previous work done in IP networks performance metrics and presents work done in specific WSN metrics. Section III addresses QoS in WSNs and introduces a taxonomy of WSN with QoS requirements. The fourth section details WSN performance needs in industrial environments, as an example of controlled performance WSNs, and presents our proposed WSN communication performance taxonomy. Section V presents our proposed WSN metrics framework. Finally, last section presents the conclusions.

II. RELATED WORK

The issue of performance in computer networks has been deeply investigated. In IP networks, IETF's IP Performance Metrics Working Group (IPPM) of the Transport Area, proposed a Framework for IP performance evaluation (RFC2330) [3]. The motivation to develop IP Performance metrics was to give users and providers of Internet service a common understanding and framework for measuring the performance offered and obtained. The metrics are designed for use of network operators, independent testing groups, or end users, and represent an unbiased quantitative measure of performance. The metrics can be divided in two main groups. The first group contains the basic metrics to measure IP performance and is constituted by the IPPM Metrics for Measuring Connectivity (RFC2678) [4], One-way Delay Metrics (RFC2679) [5], One-way Packet Loss Metrics (RFC2680) [6] and Round-trip Delay Metrics (RFC2681) [7]. The second group deals with specific Internet behavior and specifies new concepts of performance. It is constituted by One-way Loss Pattern Sample Metrics (RFC3357) [8] (introducing the concepts of Loss Distance and Loss Period), IP Packet Delay Variation Metric (RFC3393) [9], IPPM Metrics for periodic streams (RFC3432) [10], Packet Reordering Metrics (RFC4737) [11], Network Bulk Transport Capacity Metrics (RFC3148) [12], Network Link Capacity Metrics (RFC5136) [13] and One-Way Packet Duplication Metric (RFC5560) [14]. Additionally, the composition, decomposition and aggregation of individual metrics over time and space are also presented (RFC2330, RFC5835) [3][15].

QoS requirements in WSNs are analyzed in [1] using application and network perspectives. Collective QoS parameters are introduced as a response to the specificities of the measurement of QoS in WSNs. Namely it defines collective latency, collective packet loss, collective bandwidth and information throughput.

978-1-4673-1239-4/12/$31.00 ©2012 IEEE

Some guidelines to WSN performance benchmarking, in search for a common methodology to collect, compare and evaluate different optimization methods, are proposed in [16]. It also proposes metrics such as energy consumption, network lifetime, average delivery ratio, average packet delay, average overhead, total data aggregation, standard deviation of remaining energy in nodes, throughput, average packet journey length, response time and sampling frequency.

Specific studies focusing on particular aspects of WSN performance were also presented. As examples, [17] deals with fault tolerance, introducing a new concept of region-based connectivity, [18] analyses WSNs tracking systems using estimation of the tracking error (distance between the predicted and the actual location of the target) and computation time as metrics, and [19] uses different metrics to create a new definition of network lifetime that also indicates the performance degradation of the WSN.

The analysis of performance using nodes local storage and computation capabilities, instead of sending all information to the sink, is discussed in [20].

A taxonomy for the QoS requirements of WSNs in real-time environments is presented in [2]. It aims to create a reference model to characterize and measure QoS in WSN. Each of the requirements should be mapped into usable metrics that define completely (or as completely as possible) the QoS provided by the WSNs. It also classifies the application scenarios of WSNs.

However, till this moment, and in our best knowledge, most of the evaluation of the performance of WSNs continues to rely on traditional wired metrics such as simple throughput, one-way delay, one-way loss and connectivity. Also, most of the current research on WSN performance mostly targets specific aspects and not a global framework, which does not permit a global view and perception of the global performance provided by the WSN.

III. QoS in WSN

Many techniques have been proposed to enable QoS in traditional networks. However, to evaluate it, most of the parameters measured are the typical delay, delay variation, available bandwidth and packet loss, measured end-to-end. Additional metrics were defined to characterize the behavior of the network, but rely on the same basic metrics [3].

WSN, on the other hand, present a new range of applications and scenarios, which imply that a typical WSN must have to deal with new QoS demands and parameters. A WSN that targets precision agriculture will have in its QoS parameters the accuracy and precision of the measurements. An industrial plant will demand strict time restrictions, reliability and security as some of its QoS needs. A biodiversity mapping WSN will most certainly have coverage among its essential QoS necessities. Also, WSN present severe hardware restrictions such as processing power, energy, storage, communication capabilities, bandwidth, dynamic topology, non-uniform traffic, scalability, or multiple sinks, raising the challenge of enabling these networks with QoS.

While it is difficult to have a WSN that fulfills all the QoS requirements of all the possible applications, a framework that allows for the full characterization and evaluation of QoS parameters can be used to estimate and control the final behavior of a particular application in a specific WSN. As a first approach to the problem of QoS in WSN, a general taxonomy of its requirements will be used. This taxonomy was presented in [2] and classifies these networks in communication and information perspectives. By using specific metrics to measure each of the requirements identified, a framework for evaluating WSN (with QoS) can be achieved.

In this paper, the focus will be in the Communication Processing group, specifically in its Performance branch, that includes all the necessary requirements that influence the speed, quality and efficiency of the packets travelling in the network. This branch will be characterized and provided with the necessary metrics for its full evaluation.

IV. Communication Performance in WSN

The Performance branch of the Communication Processing group, presented in the previous section, deals with every aspect of WSN that targets the transmission of packets in the network. Although one might considerer other aspects of performance, in a broader notion of the term, only performance dealing with the communication aspects of WSN requirements will be discussed in this paper.

While performance metrics may be applied to all kinds of WSN, using any type of application, they are most needed in WSN with controlled performance. In this specific type of WSN, QoS and its specific performance targets must be assured, as are essential to fulfill the expected behavior of the applications used. Among the most demanding scenarios for WSN with controlled performance are industrial plants.

To provide WSN with performance assurances in industry, several studies were made, resulting in new standards and WSN architectures targeting wireless industrial communications, namely the ISA100.11a [21], WirelessHart [22] and GINSENG [23]. These studies proposed specific algorithms and protocols, together with specific architectures, providing for reliability, monitoring, alerting, open and closed-loop control, and low latencies.

GINSENG – Performance Control in Wireless Sensor Networks, for which the authors of this paper have contributed, gave the necessary insight for the performance issues faced by industrial scenarios. Its testbed, the Petrogal oil refinery in Sines, Portugal, uses different subsystems for the monitoring and control of the plant, each of them with different time and reliability boundaries. As all industrial plants have similar requirements, it should be possible to generalize the solutions and extend them to any other controlled performance scenario. After analyzing all the scenarios critical requirements, two levels of priorities were established [24]. The first concerns message delay and message delivery reliability, while the second includes fault tolerance and energy efficiency. These requirements were translated into a list of generic GINSENG metrics: energy consumption, end-to-end data delivery delay, end-to-end data delivery reliability, and other specific metrics for each of the

GINSENG components. GINSENG proposed metrics and corresponding evaluation are detailed in [25] and [26]. GINSENG also proposed the use of a Management Information Base (MIB), located at each node, where aggregated node and neighbor info are saved. This MIB includes parameters such as total packets sent/received, number of retransmissions, average RSSI, uptime, radio listen and transmission time, and is periodically sent to the sink or retrieved by query. The needs that were found by analyzing GINSENG, and the metrics that were used, will now be expanded to create a global framework.

A. Performance taxonomy

After evaluating the needs of WSN performance in industrial environments and according to what was learned in GINSENG, a set of seven requirements for the communication performance branch of the taxonomy ([2]) were chosen, based on those that were found to be necessary for the full specification of the communication performance requirements of a WSN:

1. Delay Tolerance – specifies time bounds for the delivery delay of packets in the network;
2. Loss Tolerance – specifies loss bounds for data delivery in the network;
3. Capacity – measures the overall capacity of the network to the transmission of data as measured in the link layer (L2);
4. Reliability – minimum assurances by the network that the sent packets reach destination without errors;
5. Energy Efficiency – specifies the amount of work per energy wasted;
6. Criticality – specifies how the network deals with traffic priorities;
7. Fault Tolerance – specifies the tolerance of the network to permanent or temporary nodes failure;

Overall, the use of a complete framework for monitoring WSN performance can be divided in three distinct phases: Deployment, Operation and Debug&Recovery. These phases correspond to the different lifecycle phases of a network. In Deployment, the Framework will provide the guidelines for the specification and planning of the network, by stating the performance goals to achieve. Also, during Deployment, the QoS targets defined in the network project will be compared against the initial network tests, and the necessary corrections will be made, before the network starts its normal operation. After deployment, during operation, the continuous monitoring of the network will assure that the required QoS is under control and fulfills the initial expectations. The last phase is Recovery where, after a malfunction has been detected, the procedures to repair the network are accomplished.

V. WSN Performance Metrics

The former requirements resulting from the taxonomic analysis will now be mapped into usable metrics that define as completely as possible the performance of WSNs.

A. Approach

In selecting metrics for WSN, the restrictions of the network must be taken into account. Therefore, the metrics to be used should avoid unnecessary computation or wireless transmission at nodes, to save energy. The goal is to calculate most of the metrics at the sink and to infer as many metrics as possible from the existing traffic, avoiding unnecessary performance control data. If needed, some metrics may be calculated in the node - the execution of several instructions has a lower cost than the cost of communication [27]. Also, simple metrics provide for a real-time calculation of the performance of the network.

Metrics can be calculated using two different approaches. Data received at the sink node may contain metrics directly obtained from nodes or metrics can be calculated in the sink node indirectly. To distinguish these two scenarios, metrics can be divided in explicit and inferred. Explicit metrics are obtained directly from the nodes (e.g. energy level) and sent to the sink/gateway node that may further treat them. Inferred metrics are obtained at the sink node indirectly, by analyzing or calculating other data received (e.g. live nodes may be detected on receiving data collected by those nodes). Also, the parameters to be measured can be either individual or collective, in order to enable an accurate view of the entire network performance.

Collective parameters are a new type of parameter that results from the fact that its calculation involves the use of values from more than one node, considering the same event [1]. As an example, in a data-gathering application, collective packet loss would be the sum of individual packet losses from all the sensing nodes that sent data related to a specific event, and collective delay the difference between the time the data was obtained and the time when the last packet concerning the event, from all targeted nodes, arrived at the sink. This definition proposed in [1] can be extended considering the aggregation of parameters obtained from all (or a specific group of) network nodes, instead of a specific event and the nodes involved. Considering this context, we propose to divide Collective parameters in Collective Event parameters and Collective Network parameters. In the latter definition, and using the same examples, in a data-gathering application, collective network packet loss would be the sum of individual packet losses from all the sensing nodes that sent data in a specified time frame, and collective network delay the average delay considering all the packets sent from all or a group of nodes, in a specified time frame. Collective measurements are interesting when analyzing networks with redundant or very similar readings of the environment, or to understand the global behavior of the network. However, these new metrics cannot substitute the individual measurements in cases where each sensor has a specific sensing role.

After being calculated, metrics may be aggregated in space and time such as proposed in [15]. Spatial aggregation of a metric implies that the value of the metric along a path P is related and can be calculated by obtaining the value of the same metric in all of the sub-paths that compose P. Temporal aggregation of a metric implies that the value of the metric along a path in a time interval T is related and can be obtained if the values of the same metric in all the sub-intervals of T are known. Also, aggregated or composed metrics might themselves be subject to further steps of composition or aggregation, in higher-order compositions.

B. Performance metrics proposal

It is not the aim of this paper to present all the available and identified WSN performance metrics. Instead, our focus will be to include the best generic, application independent metrics that were found necessary to characterize the network in order to respond to the taxonomy tree of requirements. Also, metrics should be easy to calculate. These metrics will be later categorized in three groups according to the situation where they are mostly used: Deployment, Operation and Debug & Recovery. Deployment metrics will aid the network designer to establish the target performance before building the network and to certify it when the deployment is done. Operation metrics are the minimum set of metrics that are required to be measured in order to detect malfunctions in the network and assure that the initial requirements are being met. The last group includes all the additional metrics that can be used in the debug and recovery of the network.

To use collective event metrics, events have to be identifiable individually and/or by event type, and this information must be sent in the data packets.

For each of the groups of the performance taxonomy presented before, a set of metrics will now be proposed. Each metric will be specified together with its process of evaluation and units used.

1) Delay tolerance: The delay in a packet switching network expresses the time a packet spends travelling from the original sender to its destination, including propagation and transmission time. A packet delay is measured by subtracting the destination timestamp from the original sent timestamp. In the case of packets sent from nodes to sink or from sink to node (i.e. end-to-end) the term ‘delivery delay’ will be used. The clocks between sender and destination must be synchronized. The unit used is the second.

Proposed metrics:

- One-way (individual) node delivery delay: time spent by the packet from the sender to the sink (end-to-end).
- One-way (individual) sink delivery delay: time spent by a packet from the sink to a node. The calculated value must be sent to the sink in other packet.
- Round-Trip (individual) delivery delay: time spent by a packet from the sink to a node together with the response from the node to the sink.
- Actuation delivery delay: time spent by sending a packet from a node to the sink, followed by the response of the sink to the node. The calculated value must be sent to the sink in other packet.
- Collective event delivery delay: difference between the time the data was first obtained in any node and the time when the last packet concerning the event, from all targeted nodes, arrived to the sink.
- (Individual) node delivery delay variation: difference between the delays of two consecutive packets arriving from the same node to the sink (may be positive,0 or negative).
- Delay per hop: individual delays of packets measured between single hops. Reports must be periodically sent to the sink with this information. To avoid a high number of packets and to minimize the memory wasted, average values should be recorded and then periodically sent to the sink.

2) Loss tolerance: In a packet switching network the loss expresses the number of packets lost (or arriving after a pre-defined time) during the communication of two hosts in a specified time interval. The packet loss is measured by subtracting the number of packets sent to the number of packets that arrive destination in a specified time interval. To be able to calculate the lost at the destination node the packets must have sequential identifiers or the source node must periodically send a packet specifying the number of packets sent to date. The unit used is the number of packets lost during the period, as measured in sink.

Proposed metrics:

- One-way (individual) node loss: number of lost packets from the sender node to the sink in a specified time interval (end-to-end).
- One-way (individual) sink loss: number of lost packets from the sink to a node in a specified time interval. The value must then be sent to the sink in other packet.
- Collective event loss: total number of lost packets considering all the packets sent by all the source nodes, and related to the same event, to the sink, in a specified time interval.
- Collective network loss: total number of lost packets considering all the packets sent by all the source nodes to the sink, in a specified time interval.
- Loss per hop: loss of packets measured between single hops. Reports must be periodically sent to the sink with this information. To avoid a high number of packets and to minimize the memory wasted, total values should be recorded in nodes and then periodically sent to the sink.
- Loss length per node: counts the number of consecutive lost packets from a specific node, and is an indicator of the burstiness.
- Loss distance per node: counts the number of packets between two lost packets sent by the same node. It indicates the frequency of the loss.

3) Capacity: Measuring the capacity of a link is no easy task to do or even to define, while measuring the capacity of a network is even more difficult. Capacity varies with the protocol layer, with type of packets, with the conditions of the link. For the purpose of the WSN communication performance metrics capacity is going to be defined as the maximum sustainable throughput of L2 unique data (excluding retransmissions) that is received by the sink, and is measured in bytes/sec. The available capacity end-to-end will be the minimum capacity of each segment of the network. It is measured in bytes per second or, in some cases, as a percentage.

Proposed metrics:

- Capacity per node: maximum amount of sustainable throughput (bytes/sec), excluding retransmissions, of a node. It is calculated by counting the number of bytes, in unique L2 packets, received from a specific node, by the sink.
- Collective network capacity: maximum amount of sustainable throughput (bytes/sec), excluding retransmissions. It is calculated by calculating the total number of bytes received from the network, in unique L2 packets, by the sink.
- Capacity use per node: percentage of capacity of a node that is being used - is obtained by dividing the current node throughput by its previously measured capacity.
- Collective network capacity use: percentage of capacity that is being used - is obtained by dividing the current throughput by the previously measured capacity.

4) Reliability: The reliability of a network expresses its capacity of delivering packets to destination without errors and in a previously defined timeframe. In order to assess for the reliability, sent and received packets must be counted. Reliability will be presented as a percentage of delivered packets. If a sequence number is assumed, the receiving node has to track the received packets and to detect the missing packets. If the sequence numbers do not exist, periodically each node must report the number of packets sent. When considering end-to-end transmissions the term 'delivery reliability' will be used. To calculate the reliability of a WSN the proposed metrics derive from the Packet Delivery Rate, measured as follows:

Pkt Deliv Rate (%) = (Pkts received)/(Pkts sent)*100

Proposed metrics:

- Node delivery reliability: reliability of the connection from a node to the sink, considering the packets it sends and those received from the sink in a period of time.
- Sink delivery reliability: reliability of the connection from the sink to a node, considering the packets it sends and receives from the node in a period of time. The measurement must then be sent to the sink in a packet.
- Reliability per hop: reliability of the connection between nodes measured between single hops. Reports must be periodically sent to the sink with this information. To avoid a high number of packets and to minimize the memory wasted, average values should be recorded and then periodically sent to the sink.
- Collective event reliability: reliability of all nodes of the network that participate in the same event. It is calculated using the sum of all packets received by the sink and those sent by nodes, relating to a specific event.
- Collective network reliability: reliability of all nodes of the network when considered together. It is calculated using the sum of all packets received by the sink and those that were sent in a period of time.

5) Energy efficiency: Measuring the energy in WSN is crucial as nodes run on batteries. Also, it is important to know how efficient nodes are when using the available energy. The energy is measured in Volts or Watts and the energy efficiency is the amount of work done (number of operations) per Watt.

Proposed metrics:

- Data messages sent by watt per node: measures the number of messages that a node is capable of sending by Watt of energy wasted.
- Energy level per node: total energy that is available in the node.

6) Criticality: In a network where different traffic may be present, where the resources are scarce and where urgent messages may have to be delivered with strict time bounds, it is necessary to measure how critical traffic is supported. These critical packets may arise, for example, from pre-defined triggers that measure values in nodes or from messages from the sink to actuators. To measure how critical traffic is supported in the network, its performance will be compared to normal traffic. It is not needed to know, for the purpose of performance evaluation, the exact mechanisms used to raise the priority of critical messages, but to assure that they work.

Proposed metrics:

- Critical packets node delivery delay: measures the delay of a critical message from a node to the sink.
- Critical packets sink delivery delay: measures the delay of a critical message from sink to the destination node.

7) Fault tolerance: Fault tolerance in a WSN is the ability of the network to tolerate faults that lead to service failures. It is an aspect of the resilience of the network.

Proposed metrics:

- Number of active nodes: presents the number of active nodes in the network. If all nodes are active there is no fault. An adjustable time limit must be defined in order to distinguish between faults and temporary faults (automatically adapted to the maximum times of disruption of each node).

C. Metrics by network life phase

Although every metric can be used at any time, specific metrics target a specific phase in the life of the network. In Table 1, the performance metrics presented before are categorized by the phase in which they are most necessary.

Additionally, in italic, some aggregations based on the previously proposed metrics are included.

D. Basic information for metric calculation

The metrics presented assume that a small amount of information is saved in the Management Information Base (MIB) of each node (Table 2). As nodes have restrictions in the memory available, this information should not exceed the minimum necessary. Nodes that need to report periodically to the sink, should adapt the cadence to the traffic conditions of the network.

E. Application to GINSENG

In this section, some of the metrics defined before are applied to the GINSENG setup in laboratory (Fig. 1).

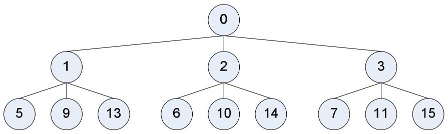


Fig. 1 – GINSENG lab network topology

The GINSENG setup network has a tree topology with 13 nodes, 9 leaves, 3 intermediate nodes and 1 sink (Node 0), and is running GINSENG software [26]. Each node sends a packet every 3 seconds and GINSENG uses TDMA with an epoch of 1 second. Additionally, some interference was provided using another network in the same channel. The data collected corresponds to a period of 15 hours.

The aim of this experiment was not to fully test the proposed framework, as it surpasses the objectives and extension of this paper, but to apply some metrics, chosen from Operation phase, to get an overview of the network performance. Collective event metrics and critical packets are not presently possible to be used in GINSENG and so were not tested. Charts in Fig. 2 present some of the collected metrics evolution by time (for clarity not all individual nodes are shown), using 10 minutes time periods. By analyzing the results (not all shown in the graphics presented), a problem in Node 3 was detected, as it achieved the highest average data delivery delay during all the experiment (111% above the average of all other nodes – 660 ms vs 312ms). All other nodes were around the mean (Fig. 2 a)). Node 15, which communicates with the sink through Node 3, had a maximum Loss Length of 127 packets (in all other nodes it was 1), and was responsible for almost all the lost packets in the network (Fig. 2 b)). By monitoring the number of active nodes, using the packets received at the sink, it was found that at beginning one of the nodes (node 11) ceased transmitting. The average node delivery delay variation was kept in a range of [-5,5]ms for each 10 minutes period (Fig. 2 c)) during almost all experience. Overall the network presented a very high reliability (Fig. 2 d)).

VI. Conclusion

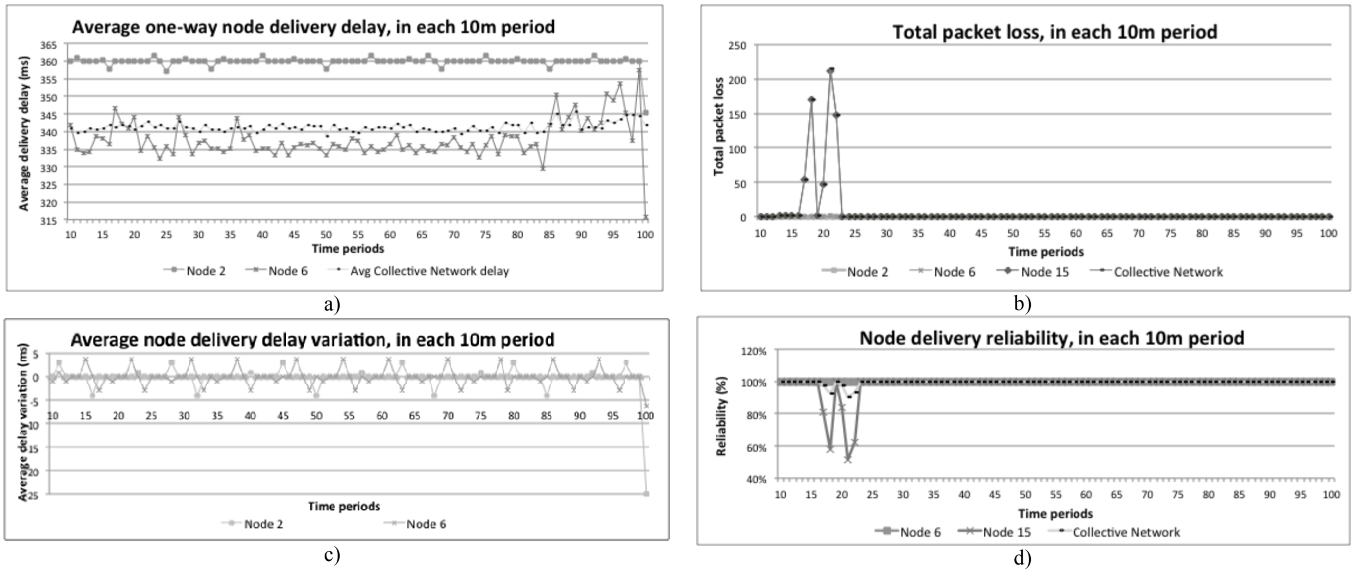
Extending the applicability of WSNs, with their unique characteristics and advantages, to controlled performance scenarios, with strict QoS demands, requires constant evaluation of performance. In this paper, a first step to a global framework of performance metrics applied to WSNs is proposed, starting with communication performance. By providing a deeper and real-time knowledge of the performance of the network, it is possible to assure that the initial QoS demands are being met or to act if they are not, enabling those networks with controlled QoS to their users and applications. Furthermore, by using a common framework, it will be possible to create a systematic methodology to compare WSN performance. Future work will include extending the framework presented to the other branches of the general taxonomy in [2], in order to achieve a global evaluation framework for WSN.

TABLE 1. Communication Performance metrics by phase

	Deployment	**Operation**	**Debug & Recovery**
Delay Tolerance	*Avg delay per node;*	One-way node delivery delay; One-way sink delivery delay; Round-trip delivery delay; Actuation delivery delay; Collective event delivery delay; *Avg node delivery delay variance;*	Delay per hop; Node delivery delay variation;
Loss Tolerance	*Avg loss per node;*	One-way node loss; On-way sink loss; Collective event loss; Collective network loss; Loss length per node; Loss distance per node;	Loss per hop; *Number of retransmissions by node;*
Capacity	Capacity per node; Collective network capacity;	Collective network capacity use;	Capacity use per node;
Reliability	*Avg node delivery reliability; Avg sink delivery reliability; Avg collective event reliability; Avg collective network reliability;*	Node delivery reliability; Sink delivery reliability; Reliability per hop; Collective event reliability; Collective network reliability;	*Total packets sent by node; Total packets received by the sink; RSSI Avg per node;*
Energy Efficiency	Data messages sent by watt per node; *Avg energy wasted by transmitted bit; Avg energy wasted by transmitted data bit;*	Energy level per node;	*Total energy wasted per node; Transmission time per node; Activity-time per node; Idle-time per node; Listen time per node; Duty cycle per node;*
Criticality	*Avg critical packet node delivery delay; Avg critical packet sink delivery delay;*	Critical packets node delivery delay; Critical packets sink delivery delay;	*Average speedup of critical messages by node;*
Fault Tolerance	*Avg time to detect node failure;*	Number of active nodes;	*Avg time to recover; Avg down time per node;*

TABLE 2. NECESSARY FIELDS FOR THE MIB OF THE NODE.

• Total energy wasted in the node;	• Idle time;	• Number of received packets;
• Energy remaining in the node;	• Uptime;	• Avg RSSI from received packets;
• Total listening time;	• Number of packets sent;	• Avg RSSI from received packets from a specific node;
• Total transmitting time;	• Number of forwarded packets;	• RSSI measured in the last packet received;
• CPU time;	• Number of packets retransmissions;	• Response time delay average;



a)

b)

c)

d)

Fig. 2.- Metrics evaluated in GINSENG testbed

ACKNOWLEDGMENT

The work presented was partially financed by the IST FP7 0384239 Ginseng.

REFERENCES

[1] D. Chen and P. K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey", Proc. of the 2004 International Conference on Wireless Networks, 2004.

[2] V. Pereira et al, “A Taxonomy of WSN with QoS”, NTMS'2011 Wireless Sensor Network workshop, February 2011.

[3] V. Paxson, G. Almes, J. Mahdavi, J. and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998.

[4] J. Mahdavi and V. Paxson , "IPPM Metrics for Measuring Connectivity", RFC 2678, September 1999.

[5] G. Almes, S. Kalidindi and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[6] G. Almes, S. Kalidindi and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[7] G. Almes, S. Kalidindi and M. Zekauskas, "A Round-trip Delay Metric for IPPM", RFC 2681, September 1999.

[8] R. Koodli, R. Ravikanth, “One-way Loss Pattern Sample Metrics”, RFC3357, August 2002.

[9] C. Demichelis, P. Chimento, “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)”, RFC 3393, November 2002.

[10] V. Raisanen, G. Grotefeld, A. Morton, “Network performance measurement with periodic streams”, RFC3432, November 2002.

[11] A. Morton, L. Ciavattone, G. Ramachandran, S. Shalunov, J. Perser, “Packet Reordering Metrics”, RFC4737, November 2006.

[12] M. Mathis, M. Allman, “A Framework for Defining Empirical Bulk Transfer Capacity Metrics”, RFC3148, July 2001.

[13] P. Chimento, J. Ishac, “Defining Network Capacity”, RFC5136, February 2008.

[14] H. Uijterwaal, “A One-Way Packet Duplication Metric“, RFC5560, May 2009.

[15] A. Morton, S. Van den Berghe, “Framework for Metric Composition”, RFC5835, April 2010.

[16] G. Martinovic et al, "A Cross-Layer Approach and Performance Benchmarking in Wireless Sensor Networks", WSEAS, 2009.

[17] A. Sen, B. H. Shen, L. Zhou, B. Hao, “Fault-Tolerance in Sensor Networks: A New Evaluation Metric”, Proc. of INFOCOM’06, 2006

[18] N.Ahmed et al, "Performance evaluation of a wireless sensor network based tracking system," Mobile Ad Hoc and Sensor Systems, 2008.

[19] I. Dietrich and F. Dressler, “On the lifetime of wireless sensor networks,” ACM Transactions on Sensor Networks, vol. 5, issue 1, pp. 5:1 – 5:39, 2009.

[20] T. O'Donovan, N. Tsiftes, Z. He, T. Voigt, C. Sreenan, “Detailed diagnosis of performance anomalies in sensornets”, Proc. of the 6th Workshop on Hot Topics in Embedded Networked Sensors ,2010.

[21] ISA-100, http://www.isa100wci.org/, accessed in Dec/2011.

[22] WirelessHART, http://www.hartcomm.org/, accessed in Dec/2011.

[23] IST FP7 0384239 Ginseng - Performance Control in Wireless Sensor Networks, http://www.ict-ginseng.eu/, accessed in Dec/2011.

[24] D1.3 Deliverable, “Final GINSENG Architecture, Scenarios and Quality of Service Measures”, FP7 GINSENG, October 2010.

[25] D4.5 Deliverable, “Second Software Integration and Preliminary Evaluation”, FP7 GINSENG, March 2011.

[26] W-B. Pottner et all, "WSN evaluation in industrial environments first results and lessons learned," Distributed Computing in Sensor Systems and Workshops (DCOSS), June 2011

[27] S.Tilak, N.B.Abu-Ghazaleh, W.Heinzelman, “A taxonomy of Wireless Micro-Sensor Network Models,” ACM Mobile Computing and Communications Review, Volume 6, Issue 2, pp.28-36, 2002.