On the Relevance of Using Interference and Service Differentiation Routing in the Internet-of-Things

Antoine Bagula[1] Djamel Djenouri [2] Elmouatezbillah Karbab [2]

1. Department of Computer Science, University of Cape Town, South Africa.
2. CERIST Research Center, Algiers, Algeria.
`bagula@cs.uct.ac.za, ddjenouri@mail.cerist.dz,`
`m.karbab@mail.cerist.dz`

Abstract. Next generation sensor networks are predicted to be deployed in the *Internet-of-the-Things (IoT)* with a high level of heterogeneity. They will be using sensor motes which are equipped with different sensing and communication devices and tasked to deliver different services leading to different energy consumption patterns. The application of traditional wireless sensor routing algorithms designed for sensor motes expanding the same energy to such heterogeneous networks may lead to energy unbalance and subsequent short-lived sensor networks resulting from routing the sensor readings over the most overworked sensor nodes while leaving the least used nodes idle. Building upon path interference awareness and sensor devices service identification, this paper assess the relevance of using a routing protocol that combines these two key features to achieve efficient traffic engineering in IoT settings and its relative efficiency compared to traditional sensor routing. Performance evaluation with simulation reveals clear improvement of the proposed protocol vs. state of the art solutions in terms of load balancing, notably for critical nodes that cover more services. Results show that the proposed protocol considerably reduce the number of packets routed by critical nodes, where the difference with the compared protocol becomes more and more important as the number of nodes increases. Results also reveal clear reduction in the average energy consumption.

1 Introduction

1.1 Motivations

The recent advances in Radio Frequency Identification (RFID) and Wireless Sensor/Actuator Networks (WSANs) have led to a new information technology (IT) era where devices built around these technologies are deployed in our daily living environments to provide services that range from the most common, such as weather forecasting, to most unusual such as body area monitoring. While RFID systems are used in such environments to accurately identify objects in a number of applications such as asset tracking, telemetry-based remote monitoring, and real time supply chain management, they usually fail short to accurately locate these objects and sense what is happening in their surrounding. On the other hand, while being good in the localization and recognition of the physical parameters of the environment in applications such as precision agriculture, fire detection, weather and pollution monitoring and many others, sensor devices are unable to identify objects. The integration of both technologies into hybrid sensor devices capable of both sensing and identifying objects present a great advantage compared to using a single technology or deploying these technologies separately. When deployed in a hospital setting, for example, to monitor babies in a maternity ward, hybrid sensors can both localize the movement of each baby during daily care, e.g., what treatment stations he baby has been through, and report on the environmental conditions he has been exposed to, e.g, temperature, humidity, light exposure, etc. Separate deployment of these technologies may lead to a duplication of resources both hardware and software, complex and costly system management and difficult software trouble shooting and maintenance. The relevance of using hybrid sensors compared to single or separate technology deployment can be demonstrated in underground mine monitoring where the placement of such devices in different locations of a mine may enable both localization of miners and identification of the environmental parameters they are exposed to in order to enable early warning in case of high exposure to high levels of gazes and danger of explosion.

Ubiquitous Sensor Networks (USNs) [1] are emerging as a family of networks that build upon the integration and networking of RFID, WSAN and hybrid devices into a common communication platform capable of identifying the objects in our living environment and sense what is happening in such environment to provide different services to different users in a multi-technology, multi-protocol environment. It will enable ubiquitous access to the information carried by a multitude of user applications and produced by a multitude of objects that surround us. When endowed with an IP address (or any global ID), USN devices may transform the objects and things we use in our daily environment into *”smart objects”* capable of using the Internet and web services to communicate among themselves, and with humans in an extended last-mile of the Internet connectivity referred to as the *”Internet-of-the-Things (IoT)”* [2]. Born between 2008 and 2009 when the number of objects/things connected to the Internet exceeded the number of people connected, the IoT is raising a great interest by both the research and practitioner’s communities as a network of the future that is predicted to connect by 2020 billions of objects outfitted with sensor, actuator and RFID devices to provide access to the information not only *any time* and *any where*, but also *by anyone* and using *anything* with projected high impact in the development of innovative technologies that will lead the near future. Based on their scientific, economic and engineering benefits, these technologies are opening tremendous opportunities for a large number of novel applications that promise to revolutionize and improve the quality of our lives.

Traditional WSN routing protocols have been designed on a routing model that route sensor readings from nodes to a gateway by assuming that the sensor nodes are of the same fabric and assumed to deliver the same service. The application of these routing protocols in the heterogeneous IoT settings may lead to performance degradation as different nodes might exhibit different levels of service heterogeneity: e.g some nodes might be assumed to sense their environment and use their GPRS modem to send SMSs in fire-fighting applications, other nodes might be tasked to achieve both sensing and identification as illustrated by the underground mining example above while in traditional settings, all the nodes might be endowed with similar sensing capabilities and assumed to provide similar levels of service: sensing and forwarding the sensor readings.

1.2 Related Work

Integration of sensors and RFID devices have been largely investigated in the literature [3–6]. In [3] for example, a two-tiered RFID sensor network where readers collect data from tags and forward it to the base station is proposed. The authors identified energy imbalance in the network caused by an increase in the amount of traffic as the distance to the base station gets shorter. Consequently, readers closer to the base station die quicker. To solve the problem, they propose a scheme that balances load among readers by adding more readers in areas near the base station. The results obtained from the simulation show that the network lifetime increases as the number of readers close to the base station increases. The solution is very expensive considering the current cost of RFID readers. Furthermore, an increase in the number of reader nodes may lead to an increase in the number of collisions in the network.

In [4–6], different techniques for integrating sensor nodes with RFIDs are discussed. The objective of the different integrations is to achieve an ad-hoc network similar to WSNs. The integrated readers collect data from the environment and share the data among themselves. This type of integrated network has similar energy limitations to WSNs because all the nodes have the same properties. In order to save energy in the network, the authors in [4] decreased energy consumption of the network by proposing an on-demand wakeup capability that eliminates idle listening. This approach saves power, but it is a Medium Access Control (MAC) protocol and not a routing protocol. Another category of multi-objective routing in WSN include geographic routing such as [7] [8], but the service differentiation in these protocols is with respect to the traffic classes and requirements and they assume a homogeneous environment and the ”m-to-1” model, while in the proposed solution the differentiation is related to the delivered services of the router nodes in a heterogeneous environment.

Data collection protocols such as collection tree protocol (CTP) [9] and TinyOS beaconing (TOB) [10] are the most related to the solution proposed in this paper. They are designed around a collection tree structure where minimum-cost trees for nodes that advertise themselves as tree roots are built and maintained to forward the sensor readings from nodes to the base-station. *Collection tree* and *adaptive beaconing* are two features implemented in both the CTP and the RPL protocol using the trickle algorithm to enable data traffic to quickly discover and fix routing inconsistencies. As implemented in the trickle algorithm, these two features are used to reduce route repair latency and beacon messages. It has been credited to the *TinyOS Beaconing (TOB)* protocol the attractive feature of node simplicity and the advantage of not having to maintain large routing tables or other complicated data structures. However, this attractive feature has to be weighted against some of the inefficiencies of the beaconing protocol, such as 1) the lack of resilience to node failures, leading to an entire sub-tree being cut off from the base-station during the current epoch when a parent node fails, 2) the tree-like m-to-1 sensor readings dissemination model leading to uneven power consumption across network nodes as the nodes surrounding the base-station tasked to forward packets from all the nodes in their sub-tree consume a lot of power, whereas the leaf nodes in the spanning tree, which do not perform any forwarding, consume least power. These shortcomings are addressed in this paper.

1.3 Contributions Overview

This paper tackles the issue of energy efficiency for USNs to evaluate the impact of using role-based service differentiation on USN efficiency in IoT settings. We propose the LIBP protocol that combines path selection with role-aware service differentiation to enable USN devices of different predefined roles to receive different treatments in order to provide different routing services and thus avoid to overstretch the most overworked sensor nodes. Our simulation results obtained using TOSSIM [11] reveal the relative scalability and efficiency of the traffic engineering scheme resulting from LIBP compared to state of the art collection protocols TOB and CTP. The remainder of this paper is organized as follows: Section 2 presents the proposed model and protocol. The experimental results obtained through comparative simulation study are presented in Section 3, and finally Section 4 draws the conclusions.

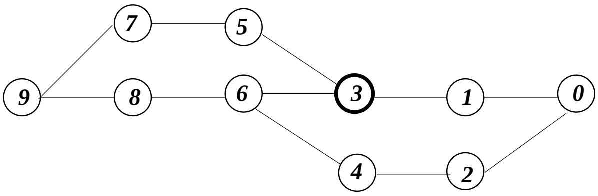
2 Proposed Solution

2.1 Path Finding Scenario

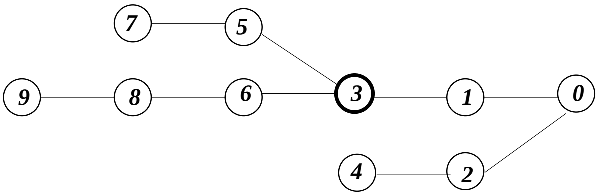
Fig 1 (a) depicts a USN as a trap topology graph with the sink located at node 0 and the edges showing potential wireless links that can be used to route the sensor readings from nodes to sink. The application of any of collection protocol to the USN illustrated by Fig 1 (a) may lead to two sensor network routing configurations, depending on how the parent nodes are selected at each epoch: A path multiplexing configuration illustrated by Figure Fig 1 (b) and a path separated configuration revealed by Fig 1 (c). The path separation configuration is a load balanced configuration which can be useful in 1) interference-aware routing schemes to minimize traffic flows interference on nodes with the expectation of reducing energy usage as each node will route less traffic and protecting the network against the impact of node failures by having less branches cut from the network upon failure 2) service-aware routing schemes to protect critical nodes from being overworked by the routing process while leaving the less critical nodes idle and 3) heterogeneous routing situations combining both schemes which we predict to be common in the IoT. The *"least interference beaconing (LIB)"* model proposed in this paper is a scheme where a weighted combination of interference and service-aware routing is piggy-backed on the beaconing process applied to collection protocols to achieve efficient and scalable USN management. Load balancing can 1) protect node 3 in interference-aware routing from becoming a single point of interference consuming high energy and leading to the high traffic loss under failure and 2) protect node 3 in service-aware routing from being overworked while less critical nodes are idle.

2.2 Network Model

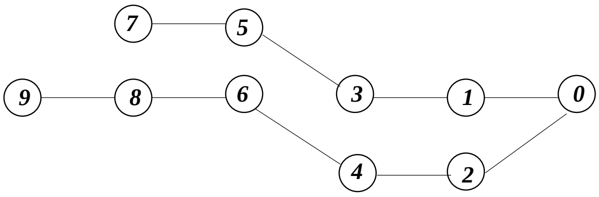
The routing in USNs can be formulated as a zero-one linear problem consisting of finding for each node $n,$ the subset $\mathbf{N}_0 \subseteq \mathbf{N}[n]$ of its neighbours that solves the following



(a) Network Topology Connectivity



(b) Path Multiplexing Configuration



(c) Path Separated Configuration

Fig. 1. *Path Discovery*

zero-one linear problem

$$\begin{array}{ll} \min & \sum_{\jmath\in\mathbf{N}[n]} x_\jmath \quad (1) \\ subject \text{ to} & \end{array}$$

$$\begin{cases} w(n) & = \alpha w_i(n) + \beta w_s(n) \qquad\qquad (2) \\ parent(\jmath) & = n \mid w(n) = \min_{x\in\mathcal{N}(\jmath)}\{w(x)\} \ (3) \\ x_\jmath & = \ 0 \text{ or } 1\ , \forall \jmath \in \mathbf{N}[n] \qquad\quad (4) \end{cases}$$

where $\beta = 1-\alpha$ while $parent(\jmath)$ is a function that returns the preferred parent for a given node n. $w(n)$ is the weight associated with the node expressing its interference in the number of children that it is carrying $w_i(n)$ and the penalty related to the role played by the node in the network $w_s(n)$. Note that as expressed above, the problem formulation does not contain any explicit formulation of the energy efficiency or dependability constraints. It only expresses the path interference minimization and role-based differentiation of services and how they are mapped into i) *a routing metric/cost* expressed by equation (2), ii) *a parent selection* expressed by equation (3) and iii) *the zero-one linearity model* expressed by equation (4). As formulated above, the routing problem is a local optimization problem that may be solved using a heuristic solution as described in subsection 2.3, and thzn implemented as a protocol. The β value and consequently

$\alpha = 1 - \beta$ is an important parameter that defines the routing model used by the USN as expressed below

$$\beta = \begin{cases} 0 & \text{Interference-aware routing} \\ 1 & \text{Service-aware routing} \\ x \in]0 \ldots 1[& \text{Hybrid routing.} \end{cases}$$

It expresses the network administration preference for a given routing model.

2.3 New Protocol

Least Interference Beaconing Algorithm (LIBA) is an algorithmic solution to the routing problem formulated above. It uses a time-bound by "epoch" breadth-first search model to find the routing paths for the traffic flows carrying the sensor readings from nodes to the sink. A high-level description of the LIBA is presented in Figure 2 (a), where T_e is the duration of an epoch while "mod" is the modulo operation. It is used in our case to compute the beginning of a new epoch.

As presented in Figure 2 (a), LIBA provides a heuristic solution to the least interference routing problem expressed by (1) by using a similar scheme to TinyOS beaconing, but with a slight modification to the beaconing process in order to meet the routing constraints (2), (3) and (4) as follows:

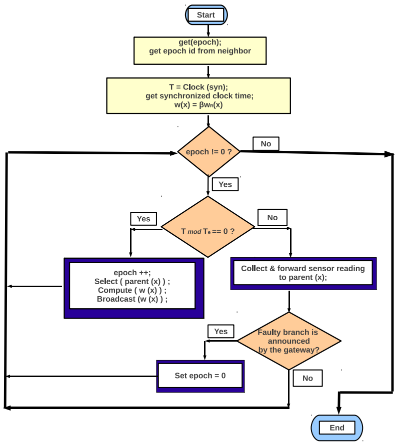
- When broadcasting the beacon after the initial step, the parent computes its weight specifying a weighted average of the number of children it is supporting (interference) and the role played by the node (service delivery) as expressed by the routing constraint (2). It then includes the calculated weight in the beacon that is being broadcasted in the leftmost blue box.
- Upon reception of the beacons from potential parents, the children nodes select their preferences for the least weighted parent and update their forwarding tables based on the expression of the routing constraint (3).
- The zero-one linearity routing constraint (4) can also be expressed by

$$x_\jmath = \begin{cases} 1 & \text{parent}(\jmath) = \imath \\ 0 & \text{otherwise.} \end{cases}$$

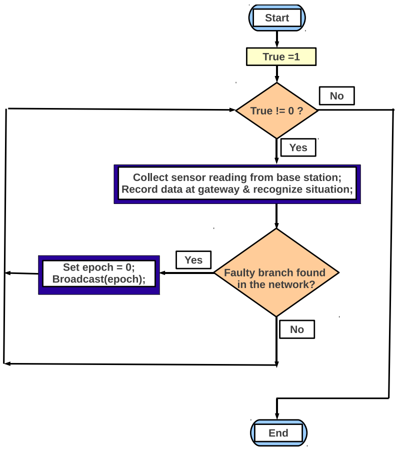
  It suggests the creation of a breadth-first spanning tree rooted at the sink through recursive broadcasting of routing update beacon messages and recording of parents.

Figure 2 (b) presents a high level description of the algorithm implemented by the sensor gateway. It involves a situation recognition process that triggers recovery mechanisms, by reinitializing the epoch counter, $epoch = 0$, upon failure. However, in this paper situation recognition has been limited to ensuring that as a protocol implementation of the zero-one linear formulation, LIBP protocol leads to a connected network. The study of the recovery processes under failure conditions are beyond the scope of this current work.

It should be noted that the LIBA algorithm depicted in Fig 2 (a) might (i) lead to a path multiplexing configuration such as illustrated in Fig 1 (b) during an epoch where



(a) Node Algorithm



(b) Gateway Algorithm

Fig. 2. *Least Interference Beaconing Algorithms*

all weights are equal and (ii) converge to a path separated configuration as depicted in Fig 1 (c) after computation and broadcasting of weights. In the illustration provided in Fig 1, the convergence to a path separated configuration happens after weight allocation and broadcasting in a given epoch where from a path multiplexing, node 3 informs nodes 5 and 6 that it has a $weight = 2$. In this case During the parent selection process that follows the weight allocation and broadcasting, node 5 having only one parent will select node 3 as parent while node 6 will prefer node 4 as parent.

The LIBP protocol is an implementation of the LIBA algorithm that is based on the following key features:

- Use of a simple ad hoc routing protocol, which creates a breadth-first spanning tree rooted at the sink through recursive broadcasting of routing update beacon messages and recording of parents.
- The beacon messages are (1) broadcast periodically at intervals called epochs, (2) propagated progressively to neighbours and (3) received by a few nodes located in the vicinity of the source of the beacon message.
- The transmission of the beacon is built around a source marking progressive propagation to neighbours and rebroadcasting progress, which sets up a breadth-first spanning tree rooted at the sink.
- The least interference paradigm is integrated into the process through selection of a parent node that has the smallest number of children (smallest forwarding table), which is thus a point of least traffic interference.
- While the LIBP protocol leads to the same number of messages exchanged as TOB, it implements a different parent selection model where instead of selecting the first parent node they heard from, the sensor nodes hear from a set of neighbours and select the least burdened (in number of children) as the parent node.

LIBP builds upon an ad hoc routing protocol similar to TOB in terms of simplicity, and to the emerging RPL protocol [12] in terms of structure. Its main messages are beacon and acknowledgement while its main operations are weight updating and broadcasting, parent selection. (i) beacon messages carrying the sender's identity and weight are broadcast to potential children by senders, (ii) parent selection is performed at reception of the beacon messages but acknowledged to only the selected parents and (iii) the selected parents increase their weights only after receiving the acknowledgement message. We note that by piggy-backing the parent identification into the beacon broadcasting process and adding parent identification to the packet header, our model may avoid the signalling overheads related to the addition of an acknowledgement into the routing process. However, as LIBP acknowledgements are sent to only the selected parents, they are bound by the maximum number of nodes in the network, thus reducing tremendously the signalling overheads during an epoch.

3 Simulation Study

To evaluate the performance of the proposed protocol and compare it with CTP [9] and TinyOs Beaconing (TOB) [10], extensive simulations have been conducted with TOSSIM [11]. The number of nodes have been varied from 20 to 200, and β, from 0.2 to 1. In each scenario, 10% of nodes where set to be critical (hybrid) nodes whose energy resource management is of high importance due to the high loads they are required to perform. These node should route as few packets as possible to ensure a long network lifetime. The number of packets forwarded by these nodes is thus the key performance metric that should be optimized (minimized) in this hybrid environment. Table 1 sketches the most relevant simulation parameters. Each point of the plots is the average of several runs, and results are presented with 99% confidence interval. The number of packets forwarded by critical nodes has been measured. Fig. 3 depicts the number of packets forwarded by critical nodes in LIBP vs. β. The plots show averaged values of the minimum number, the maximum number, and the mean number of the forwarded packets by the 10 critical nodes in the 100 nodes scenario. We can see that there is a sharp decrease from $\beta = 0$ to $\beta = 0.4$, then all the numbers become more or less stable with some but insignificant fluctuation. We conclude that setting β to 0.4 is sufficient enough– in the simulated scenarios– to enable relaxing routing load at critical nodes . β is thus fixed to 0.4 for LIBP in what follows. The number forwarded by critical nodes is presented in Fig. 4. Fig. 4 a) depicts the mean values of packets forwarded by critical nodes for both LIBP and TOB vs. the number of nodes. CTP has also been simulated, but its mean values are very fluctuating with very high error bars. It has been removed to make the figure legible. It is clear from the figure that LIBP reduces the routing load on critical nodes compared to TOB. The inevitable increase vs. the number of nodes is much smother for LIBP, and the difference between the protocol becomes more important as the number of nodes rises. This is justified by the fact that the more nodes are n the network, the more choices will be available to permit routing around critical nodes.

Fig. 4 b) shows the interval of the number of forwarded packets by critical nodes (the minimum/maximum dispersal), where CTP is also depicted. Here, it is clear how the difference between the minimum and the maximum values is huge for CTP that does not apply any load balancing, and that the CTP tree construction strategy resulted in some bottleneck nodes amongst the critical ones. On contrary, LIBP demonstrated the best performance owing to its strategic load balancing. Finally, Fig. 5 a) and b) plot the total instantaneous number of data packets received by the sink and those sent by the nodes, respectively, vs. time in 100 nodes scenario. From these plots, it can be seen that CTP implementation results in higher latency owing to the spanning tree construction that takes a long time compared to the other protocols. This explains non-transmission (and accordingly no reception) of packets at the beginning, and peaks in a later stage of the experimentation. Using Avrora, we measured the average energy consumption of all nodes in the network for the tree protocols. Fig. 6 depicts the obtained results vs. the number of nodes. It is clear from the figure taht CTP leads to a drastic rise of energy consumption when the number of nodes reaches 70, while both TOB and LIBP scale with the increase in the number of nodes. LIBP reveals the lowest energy consumption with the increase of number of USN nodes.

Table 1. Simulation Setup

Traffic	every node sends a 28-byte packet every 5 sec
Number of nodes	20: 200
Topology	random
Simulation duration	900 sec
beacon interval	20 s

4 Conclusion and Future Work

This paper presents LIBP, a new routing protocol that builds upon routing simplicity, minimization of the interference among competing traffic flows and service differentiation to achieve efficient traffic engineering of the emerging islands of USNs that form

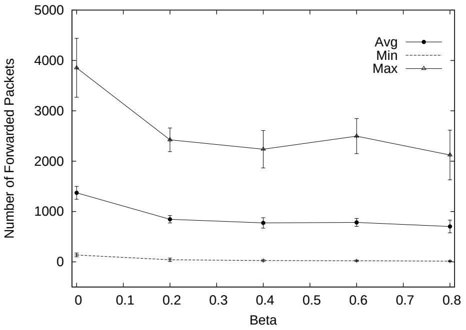
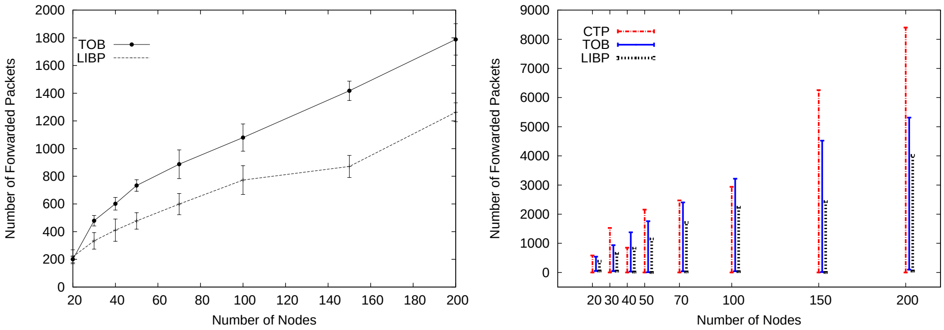


Fig. 3. Impact of β on packet forwarding by critical nodes in LIBP

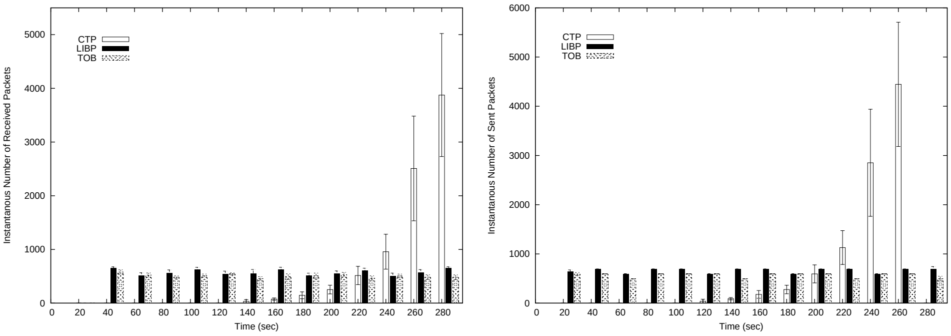


(a) (b)

Fig. 4. Packet forwarding of critical nodes vs. number of nodes a) Average, b) min/max dispersal

the IoT. Preliminary experimental results using TOSSIM reveal the relative efficiency of LIBP compared to CTP and TOB protocols. These results reveal that the "path separation" principle behind the "least interference beaconing" paradigm embedded into LIBP and the "least interference optimization" paradigm proposed in [13, 14] translates into network efficiency.

There is room for further investigation of the LIBP protocol in terms of its fault tolerance capabilities upon failure, its dependability in terms of protection against jamming attacks, and its relative performance compared to recently standardized protocols such as RPL. When deployed to support sensing operations in intermittent power supply environments, a flexible and robust gateway such as proposed in [15] may be augmented with situation recognition capabilities to improve USN security and efficiency. This is another avenue for future research.



(a) (b)

Fig. 5. Instantaneous number of packets a) received, b) sent

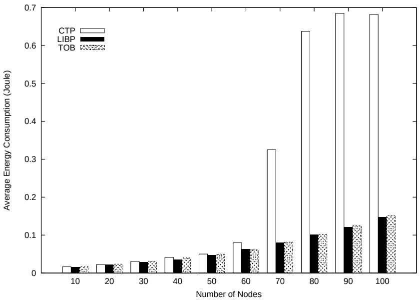


Fig. 6. Average radio energy consumption vs. number of nodes

References

1. A. Bagula et al. “Ubiquitous Sensor Networking for Development (USN4D): An Application to Pollution Monitoring”, in MDPI Sensors, 12(1):391-414, 2012.
2. J. Vasseur & A. Dunkels. “Interconnecting Smart Objects with IP, The Next Internet”, Morgan Kaufmann, ISBN: 9780123751652, July 2010.
3. G. Yang, M. Xiao, and C. Chen,*A simple energy-balancing method in RFID sensor networks*, In Proceedings of 2007 IEEE International Workshop on Anti-Counterfeiting, Security, Identification,Xiamen China, pp. 306-310, April 16-18, 2007.
4. A.G. Ruzzelli, R. Jurdak, and G.M.P. O’Hare, *On the RFID wake-up impulse for multi-hop sensor networks*, In Proceedings of 1st ACM Workshop on Convergence of RFID and Wireless Sensor Networks and their Applications (SenseID) at the 5th ACM Conference on Embedded Networked Sensor Systems (ACM SenSys 2007), Sydney, Australia, November, 2007.
5. Englund, H. Wallin, *RFID in wireless sensor network*, Tech. Report, Dept. of Signals & systems, Chalmers Univ. of Technology, Sweden, 2004, pp 1-69.
6. V. Dyo, S. A. Ellwood, D. W. Macdonald, A. Markham, C. Mascolo, B. Pasztor, S. Scellato, N. Trigoni, R. Wohlers, K. Yousef, *Wildlife and Environmental Monitoring using RFID and WSN Technology*, In Proc. of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys’09), Berkeley CA, USA. Nov. 2009.

7. D.Djenouri, I. Balasingham. Traffic-Differentiation-Based Modular QoS Localized Routing for Wireless Sensor Networks. IEEE Transactions on Mobile Computing, Vol. 10, No. 6, pp 797-809, June 2011.
8. E. Felemban, C.-G. Lee, and E. Ekici, MMSPEED: Multipath Multi-Speed Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks, IEEE Trans. Mobile Computing, vol. 5, no. 6, pp. 738-754, June 2006.
9. O. Gnawali et al. "Collection Tree Protocol", Proc. of ACM SenSys09, Berkeley, CA/USA, November 4-6, 2009.
10. J. Hill et al. "System architecture directions for networked sensors", Proc. of ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS IX), 2000. Oct. 2003.
11. P. Levis, N. Lee, M. Welsh & D. Culler. "TOSSIM: Simulating large wireless sensor networks of tinyos motes", Proc. of ACM SenSys03, pp 126-137, Los Angeles, CA, November 2003.
12. T. Winter et al, "RPL: IPv6 Routing protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.
13. A. Bagula. "Hybrid traffic engineering: the least path interference algorithm", Proc. of ACM annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, pp 89 - 96, 2004.
14. A. Bagula. "On Achieving Bandwidth-aware LSP/LambdaSP Multiplexing/Separation in Multi-layer Networks". IEEE Journal on Selected Areas in Communications (JSAC): Special issue on Traffic Engineering for Multi-Layer Networks, Vol 25, No 5, June 2007.
15. Marco Zennaro & Antoine B. Bagula, "Design of a flexible and robust gateway to collect sensor data in intermittent power environments", in International Journal of Sensor Networks, Vol. 8, Nos. 3/4, 2010.