J. Sens. Actuator Netw. **2014**, *4*, 297-330; doi:10.3390/jsan3040297

OPEN ACCESS

Journal of Sensor and Actuator Networks

ISSN 2224-2708

www.mdpi.com/journal/jsan/

Article

Towards Long-Term Multi-Hop WSN Deployments for Environmental Monitoring: An Experimental Network Evaluation †

Miguel Navarro [1], Tyler W. Davis [2,3], German Villalba [2], Yimei Li [1], Xiaoyang Zhong [1], Newlyn Erratt [1], Xu Liang [2,*] and Yao Liang [1,*]

[1] Department of Computer and Information Science, Indiana University Purdue University, 723 West Michigan Street, SL 280, Indianapolis, IN 46202, USA; E-Mails: mignavar@cs.iupui.edu (M.N.); liyim@cs.iupui.edu (Y.L.); xiaozhon@cs.iupui.edu (X.Z.); nerratt@umail.iu.edu (N.E.)

[2] Department of Civil and Environmental Engineering, University of Pittsburgh; 3700 O'Hara Street, 728 Benedum Hall, Pittsburgh, PA 15261, USA; E-Mail: gev5@pitt.edu

[3] Department of Life Sciences, Imperial College London, Silwood Park Campus, Ascot, Berkshire SL5 7PY, UK; E-Mail: tyler.davis@imperial.ac.uk

† This article extends our initial work "*A Study of Long-Term WSN Deployment for Environmental Monitoring*", presented at the 2013 IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC).

* Authors to whom correspondence should be addressed; E-Mails: xuliang@pitt.edu (X.L.); yliang@cs.iupui.edu (Y.L.); Tel.: +1-412-624-9872 (X.L.); +1-317-274-9727 (Y.L.)

External Editor: Kirk Martinez

Received: 23 September 2014; in revised form: 13 November 2014 / Accepted: 26 November 2014 / Published: 5 December 2014

Abstract: This paper explores the network performance and costs associated with the deployment, labor, and maintenance of a long-term outdoor multi-hop wireless sensor network (WSN) located at the Audubon Society of Western Pennsylvania (ASWP), which has been in operation for more than four years for environmental data collection. The WSN performance is studied over selected time periods during the network deployment time, based on two different TinyOS-based WSN routing protocols: commercial XMesh and the open-source Collection Tree Protocol (CTP). Empirical results show that the network performance is improved with CTP (*i.e.*, 79% packet reception rate, 96% packet success rate and 0.2% duplicate packets), *versus* using XMesh (*i.e.*, 36% packet reception rate and 46%

packet success rate, with 3%–4% duplicate packets). The deployment cost of the 52-node, 253-sensor WSN is $31,500 with an additional $600 per month in labor and maintenance resulting in a cost of $184 m^{-2} y^{-1} of sensed area. Network maintenance during the first four years of operation was performed on average every 12 days, costing approximately $187 for each field visit.

Keywords: wireless sensor networks; testbed; long-term deployment; network performance; network costs; environmental monitoring

1. Introduction

During the past few years, the development of commercial and research platforms for wireless sensor networks (WSNs) has gained an increasing interest in a broad range of new scientific research and applications. WSN technologies provide high resolution spatial and temporal data at a declining cost per unit area, thus making them an affordable and practical option for many researchers [1]. Additionally, since WSNs are commonly deployed for various scientific applications outside of the computer science and networking fields, researchers require solutions in which they do not have to directly handle the complexity of WSN systems. As a result, off-the-shelf commercial solutions are preferable if collaborations with WSN researchers are not possible.

The adoption of WSNs presents new challenges for scientists and engineers who require high-quality data and optimal network behavior. As an *in situ* mechanism for data collection, WSNs are deployed in multiple scenarios where outdoor locations represent a critical challenge. Indeed, simulation and laboratory methods are unable to capture the complexity of outdoor environments (e.g., forests, oceans, mountains, or glaciers), which significantly affect WSN operations and maintenance. Consequently, experimental deployments are essential to study and analyze WSN performance and its maintenance characteristics under these harsh conditions.

Related experiments have shown unexpected behaviors and observations in outdoor deployments compared to indoor conditions [1–4]. To better understand these situations, previous studies have tested large-scale networks [2,3,5,6]. However, the majority of those large-scale outdoor WSNs had rather short experiment durations, lasting from several days to a few months, mostly due to power constraints.

This paper presents the experimental study of an environmental multi-hop WSN that has been in operation for more than four years. The WSN experiment, named *ASWP testbed*, is deployed in a forested nature reserve of the Audubon Society of Western Pennsylvania (ASWP). One of the initial motivations for this deployment was to explore the feasibility of using WSNs for collecting reliable long-term hydrological data to investigate impacts of vegetation heterogeneity and soil properties on the status and trends of soil moisture and transpiration. Over the course of this study, the ASWP testbed presented various challenges to WSN performance including extreme weather, wildlife, human interactions, and location restrictions for node placement.

Our study is focused on the deployment of a long-term multi-hop WSN testbed that employs both *off-the-shelf commercial* and *research-oriented open source* networking software with TinyOS-based WSN platforms. The main objectives are twofold: first, we analyze the network performance and

operation of the WSN. This analysis is conducted over specific time periods (*i.e.*, one year and six months) during the network deployment time, considering long-term network dynamics (e.g., unstable links, node failures, node relocations, battery replacements) that affect the overall network performance in the outdoor deployment environment. Second, we analyze the network costs, including the deployment, labor, and maintenance costs of the WSN.

Multi-hop WSNs pose additional challenges on their routing protocols, which are responsible for dynamically establishing efficient routes towards the sink node(s). The evaluation and direct comparison of routing protocols in WSNs remains an open research problem, knowing that it is challenging to guarantee the same wireless channel conditions for multiple WSN evaluations [7,8]. Moreover, concurrent implementations of different protocol stacks require more resources from highly constrained WSN motes (e.g., 4 KB of RAM in MicaZ motes [9]). These resources are often limited even for the implementation of a WSN application that uses a single protocol stack. In our work, we hence emphasize on the network evaluation of an environmental multi-hop WSN that uses two different protocol stacks, rather than conducting a direct WSN routing protocol comparison.

To the best of our knowledge, the ASWP testbed represents one of the first known *long-term* multi-hop WSN deployments in an outdoor environment and this study presents the first comprehensive network evaluation of both a commercially available and a state-of-the-art open source networking software for a WSN deployment with those characteristics.

The rest of this paper is organized as follows: Section 2 overviews related works on WSN deployments. Section 3 describes the WSN testbed deployment. Section 4 presents the network performance analysis of our WSN. Section 5 presents the network cost analysis. Section 6 presents our conclusions and future work.

2. Related Works

WSN deployments can be classified into two major categories depending on their application: *periodic sampling* and *object detection/tracking* [3,10]. These two categories have different requirements and thus they are tested in different scenarios. On one side, periodic sampling applications target extensive operational time periods and require low power consumption due to limited energy resources. The second category aims for shorter operational time periods, low latency, and always-on configurations [3]. The ASWP testbed implements a periodic sampling application.

Table 1 summarizes representative multi-hop WSN deployments reported in the past decade, specifying their reported deployment analysis time (*i.e.*, the time period covered by its analyzed dataset), network size in terms of the number of deployed nodes, deployment environment (e.g., indoors, outdoors-open area, and outdoors-forested area), hardware platform, and main application category. The first five deployments listed in Table 1 (*i.e.*, MoteLab [11], Kansei Genie [5], Indriya [12], SensLab [13] and FlockLab [14]) represent indoor experiments and they are classified in a special category as application testing deployments. The main objective in these works is to allow external users to test their algorithms and protocols by providing a WSN infrastructure. These works are critical during early stages of a WSN application design because they allow programmers to test their code in real WSN motes. Nonetheless, indoor environments (e.g., wall-power supply, common interference patterns, and

controlled temperature and humidity) are difficult to generalize for external environments where WSN nodes are directly exposed to harsh conditions.

Table 1. Representative multi-hop WSN deployments from the past decade and their deployment characteristics.

Testbed	Deployment Analysis Time	Size	Environment	Hardware Platform	Application Category
MoteLab [11]	N/A	190 nodes	Indoors	TMote Sky	Application testing
Kansei Genie [5]	N/A	700 nodes	Indoors	XSM, TelosB, Imote2	Application testing
Indriya [12]	N/A	139 nodes	Indoors	TelosB	Application testing
SensLab [13]	N/A	256 × 4 nodes	Indoors	WSN430	Application testing
FlockLab [14]	N/A	30 × 4 nodes	Indoors	TinyNode, Opal, TelosB, IRIS	Application testing
VigilNet [15]	~days	70 nodes	Outdoors (open area)	Mica2	Tracking/ detection
Springbrook [4]	7 days	10 nodes	Outdoors (forested area)	Fleck-3	Periodic sensing
ExScal [3]	15 days	1200 nodes	Outdoors (open area)	Mica2 (XSM)	Tracking/ detection
GreenOrbs [6]	29 days	330 nodes	Outdoors (forest)	TelosB	Periodic sensing
SNF [16]	30 days	57 nodes	Outdoors (forest)	M2135	Periodic sensing
Redwoods [17]	44 days	33 nodes	Outdoors (on a tree)	Mica2Dot	Periodic sensing
SensorScope [18]	2 months	< 100 nodes (16 outdoor)	Outdoors (glacier)	TinyNode	Periodic sensing
Trio [2]	4 months	557 nodes	Outdoors (open area)	Trio Mote	Tracking/ detection
GDI [19]	4 months	98 nodes	Outdoors	Mica2Dot	Periodic sensing
ASWP [20]	1 year + 6 months	42–52 nodes	Outdoors (forested area)	MicaZ, IRIS	Periodic sensing

He *et al.* [15] present VigilNet, a sensor network system designed to support detection and tracking of moving targets. An experiment is carried out using 70 Mica2 motes in an outdoor setting with a maximum expected life of 10, 20, or 48 days, depending on the selected configuration. ExScal [3] represents one of the initial large-scale WSN deployments by using 1200 motes. The deployment was conducted over a 15-day period and it implements an application for intruder detection and tracking. The effect of the environment on the WSN is reported as several motes become non-operational and unexpected faults affect the overall network performance. Trio [2] is an outdoor WSN testbed

deployment that incorporates solar panels to the motes. It is evaluated using an object tracking application in 557 solar-powered motes during a four-month operation period. This long network lifetime is due to the inclusion of an energy-harvesting mechanism; however, not all deployments are appropriate for these alternatives (e.g., limited sun exposure) and WSN motes must rely mainly on batteries as their primary energy source.

The SNF deployment at the Southern Sierra Critical Zone Observatory in [16] presents 57 WSN motes equipped with solar panels. The WSN periodically samples and collects data from snow depth, soil moisture, humidity, temperature, solar radiation, and matric potential sensors. Its initial deployment of 19 motes was analyzed with results below manufacturer specifications (*i.e.*, transmission distances, mote battery lifetime, and transmission reliability). A deployment strategy is proposed and validated with the deployment of the 57 WSN motes. SensorScope [18] is another multi-hop WSN deployment running a periodic sampling application, which also incorporates solar panels to power the WSN motes. Their reported deployment analysis time is two months.

Springbrook [4] presents a multi-hop WSN deployment for long-term monitoring of rainforest ecosystems. Authors evaluate the network performance using 10 WSN motes powered using rechargeable batteries and solar panels. Their results show that motes located in forested areas receive as little as 1% of the solar energy received by motes in open areas. They also provide initial observations regarding drops in link quality and network performance due to rain events and the external environment.

The direct sunlight received at WSN nodes is highly variable and dependent on natural obstacles [4] in addition to weather conditions (*i.e.*, cloudiness) and seasons (*i.e.*, total available sunshine hours). For the ASWP testbed, there are limited available sunshine hours (45% [21,22]), which are further obstructed by natural obstacles (*i.e.*, tree canopy) from reaching the WSN nodes (e.g., see Figure 1).

Figure 1. Examples of two WSN node configurations deployed at the ASWP testbed. Both examples show how natural obstacles obstruct the direct sunlight received at the wireless sensor network (WSN) nodes.

Tolle *et al.* [17] deployed 33 WSN motes to monitor a redwood tree during 44 days. The deployment used battery-powered Mica2Dot motes and the analysis shows a 49% data yield, considering that some

motes start dying after 10 days of operation. In [19], authors present a four-month habitat monitoring deployment consisting of 150 battery-powered motes. Motes were divided into a single-hop network and a multi-hop network, where motes in the multi-hop network achieved average lifetimes of 29 or 60 days, depending on their configuration. These works provide initial observations of the challenges faced by WSNs in outdoor deployments; however, they are based on particular experiments carried during field trips or expeditions, and therefore, they do not consider the challenges of continuous WSN operations and maintenance costs incurred during long-term outdoor WSN deployments.

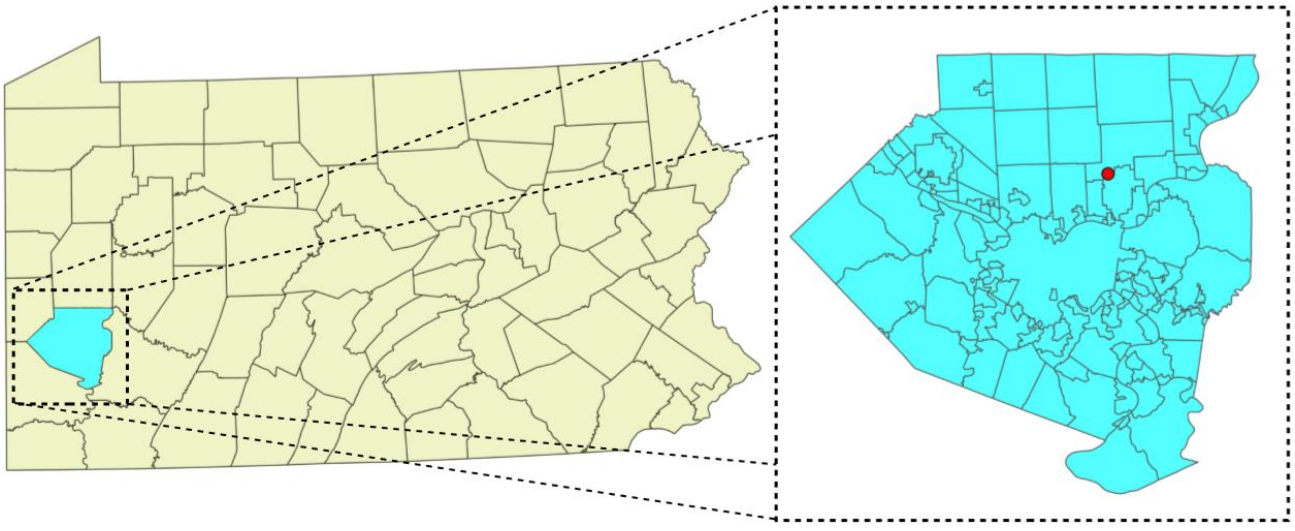
Not all outdoor WSN testbeds undergo the same kind of environmental conditions as those found in heavy forested areas. GreenOrbs [6] is one of the few battery-powered deployments that present similar environmental conditions to the ASWP testbed. In their work, 330 TelosB motes were deployed in a forest for collecting sensor data (*i.e.*, temperature, humidity, illumination, and carbon dioxide). However, their reported deployment analysis time period is still quite short (*i.e.*, from a duration in an order of days). Similarly, WSN deployments have been reported for demonstration and validation purposes, also limiting their deployment durations [23–27].

Single-hop WSN deployments have been reported, such as Life Under Your Feet (LUYF) [28], CrossVit [29] and others [30,31]; however, they do not have any routing considerations in their analysis.

3. Testbed Deployment

Our WSN is deployed at the ASWP's Beechwood Farms Nature Reserve (BFNR), which is located in Fox Chapel in northern Allegheny County, Pennsylvania, USA, as shown in Figure 2. The BFNR is 134 acres of protected land, which is owned by the Western Pennsylvania Conservancy. The reserve facilitates power and Internet needs for the WSN gateway and has an accessible wooded area where nodes may be located. The hiking trails of the reserve are closed from dusk to dawn and attract mostly nature enthusiasts, such that the equipment is relatively well-protected from human interference.

Figure 2. Location of the Audubon Society of Western Pennsylvania (ASWP) testbed (red dot) in Allegheny County (highlighted in cyan and enlarged), Pennsylvania, USA.

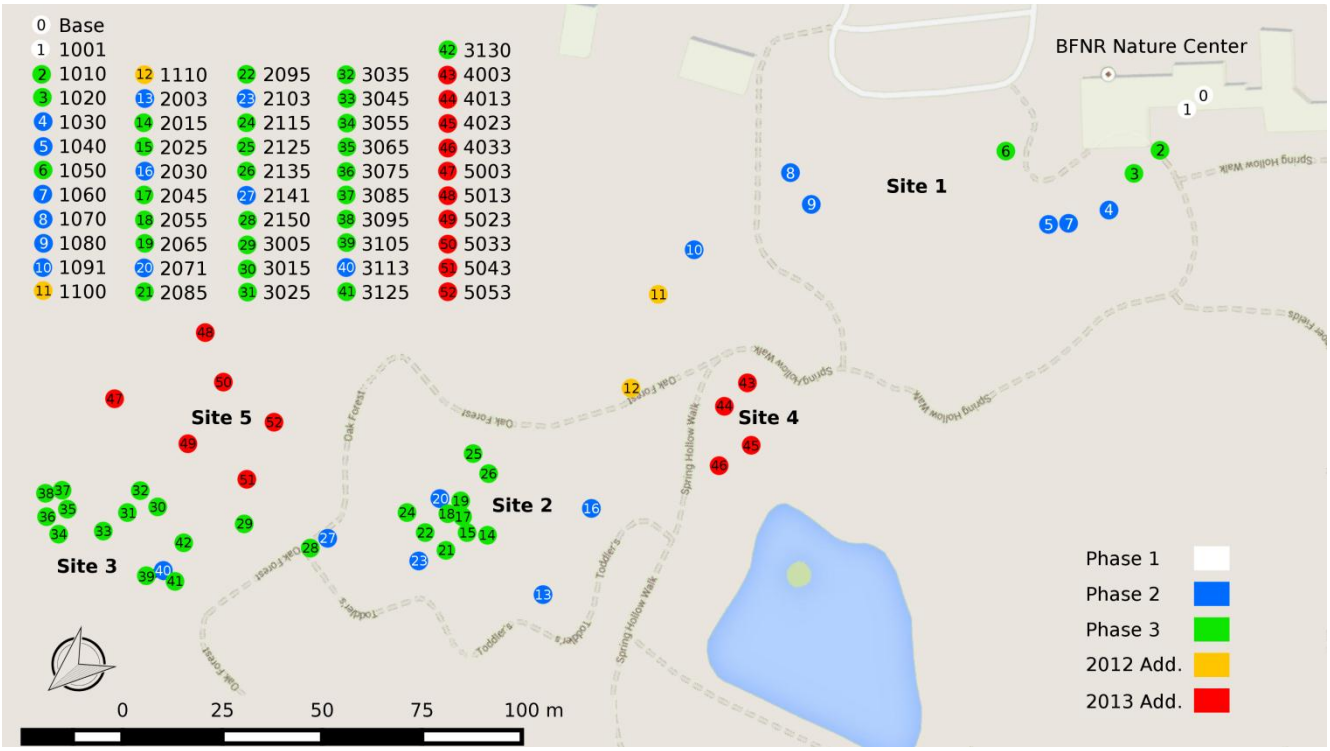


At the time the project started in 2010, the main competitors for WSN technology were Crossbow's MicaZ [9] and MoteIV's Tmote Sky [32] motes. This project invested in Crossbow's MicaZ MPR2400

radio and processor board for the network's base station and wireless motes. For environmental monitoring, the MDA300 data acquisition board [33] was selected because it provides onboard sensors and connections for up to seven external analog sensors. The onboard temperature and humidity sensors on the MDA300 allow for monitoring mote health (e.g., electrical short circuits and water intrusion) and were therefore used on all the wireless motes in the network. In the spring of 2012, MEMSIC (previously Crossbow Inc.) IRIS motes [34] were added to the network. IRIS motes, while compatible with MicaZ networks, provide more memory and stronger transmission power compared to MicaZ motes. Both MicaZ and IRIS mote platforms are powered using rechargeable nickel-metal hydride (NiMH) AA batteries with charge capacity between 2450 and 2700 mAh. An initial analysis of the nodes lifetime at the ASWP testbed is presented in [35].

Based on the desired area for sensor measurements, the study region was divided into five sites. Site 1 corresponds to the area next to the BFNR Nature Center, where the WSN gateway and the base station are located. The purpose of this site is to relay the environmental sensor data from the nodes in other sites to the base station. Sites 2 through 5, which were designated as areas to conduct field sensor measurements, are located in the forested hill-sloped region of the reserve. The five sites, including the node locations, are presented in Figure 3.

Figure 3. Map of the ASWP testbed (April 2014 configuration). Node 0 (*i.e.*, base station) is located within the Beechwood Farms Nature Reserve (BFNR) Nature Center. Nodes are consecutively numbered based on their four-digit node identifier (given in the legend) and colored based on the deployment phase: phase 1 (April 2010, white), phase 2 (June 2010, blue), and phase 3 (July 2010, green). Orange and red colored nodes represent network additions that occurred after phase 3 (2012 and 2013 respectively).



The wireless motes, data acquisition boards, batteries, and necessary environmental sensor circuitry were placed in waterproof polycarbonate enclosures. An antenna (omni-directional with 4.9 dBi gain) was mounted on the outside of the enclosure. To reduce the visibility of the network (for maintaining the aesthetics of the nature reserve), the enclosures were camouflaged and discretely located either hung from tree branches or mounted against tree trunks (see Figure 1). In addition, enclosures were mounted onto PVC-pipe stakes where vegetation was unavailable.

The WSN deployment began in April 2010 via three initial phases. The first phase consisted of testing the connection between the base station, located inside the BFNR Nature Center, and the closest nodes in Site 1. The base station was connected to a gateway that was set on the inside ledge of an office window facing the field where the first nodes were located. Following the success of the first phase, the project moved into the second phase, which consisted of placing additional nodes in Site 1 and building the relays out to Sites 2 and 3. At the end of the second phase, which was finished by late June 2010, there were 15 nodes in place. The third phase consisted of filling Sites 2 and 3 with nodes, which were used for collecting environmental data. By late July of 2010, 25 additional nodes (12 in Site 2, 13 in Site 3) were in place. At this time the network consisted of a total of 40 motes, including both relay nodes and nodes with external sensors.

Following the third phase, network modifications consisted of relay changes, adjusting both the number and location of relays, to increase the network connectivity. In late August 2010, many of the nodes in Site 1 were relocated to accommodate tree removal during a construction project taking place near the BFNR Nature Center.

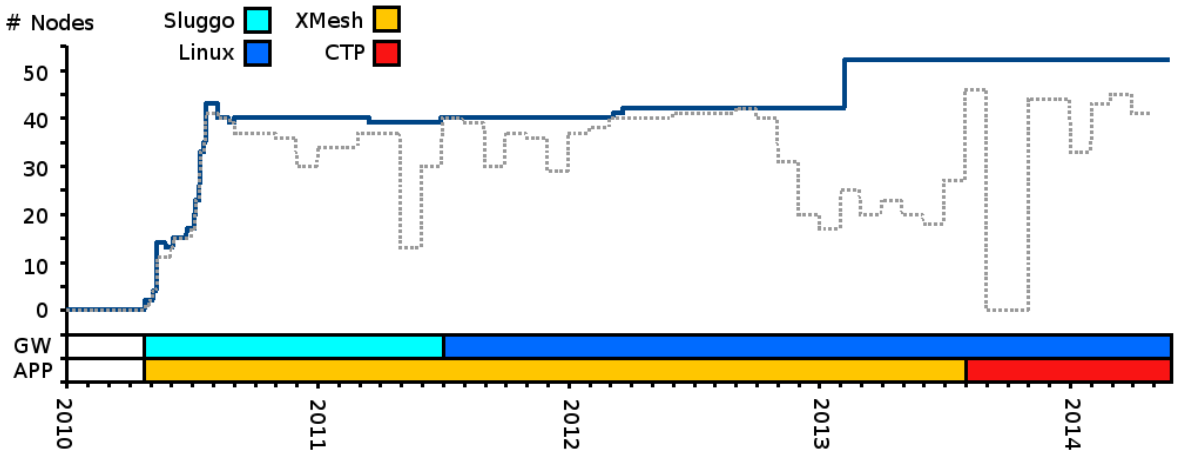
From August 2010 until March 2012 the network consisted of 40 motes, except for the three months in 2011 when there were only 39. In mid-March 2012, the network was increased to 42 motes. These two additional relay nodes were positioned near the boundary of Sites 1 and 2. At the end of March 2012, nodes in Site 1 were relocated once again due to the end of the construction taking place near the BFNR Nature Center. In May 2012, selected nodes, including the two new relays, were replaced with new IRIS motes. The purpose of this upgrade was to increase the connectivity between the sensor beds (*i.e.*, Sites 2 and 3) and the base station.

The WSN continued working with 42 motes until February 2013, when ten additional MicaZ motes were deployed forming Sites 4 and 5, as seen in Figure 3. Site 4 consists of four nodes with environmental sensors located in a copse of trees between Sites 1 and 2. Site 5 consists of six nodes with environmental sensors located south of Site 3.

Figure 4 presents an overview of the network deployment timeline. The top curve shows the total number of nodes deployed in the network over the network's deployment time (solid line) and the monthly maximum number of connected nodes within the network (dotted line). The difference between the number of deployed nodes and connected nodes is due to maintenance-needed events (e.g., hardware failures and battery depletions) and the performance of the routing protocol. Along the bottom are color bars representing the time periods for the two different network gateways (*i.e.*, Sluggo and Linux) and the two different WSN routing protocols (*i.e.*, XMesh and CTP) employed by the WSN application, which are discussed in the following sections.

As of the end of April 2014, the WSN consists of 52 nodes, 253 sensors (including 104 onboard sensors and 149 external sensors) and is running a CTP-based WSN application with a Linux WSN gateway.

Figure 4. Timeline of the ASWP testbed deployment. In the top panel, the solid line shows the number of nodes deployed in the network from April 2010 (phase 1) to April 2014, while the dotted line represents the monthly maximum number of connected nodes within the network. At the bottom, the two bars highlight the time periods of the two network gateways (GW) and the two WSN routing protocols employed by the WSN application (APP).



3.1. Gateway and Data Management

After selecting Crossbow for the WSN technology, their Stargate NetBridge served as the WSN gateway, which is a modified NSLU2 device and is nicknamed the Sluggo gateway. It remained in operation until July 2011 when it had to be replaced with a new Linux-based gateway system (see Figure 4). The need to create a new gateway system stemmed from the shortcomings of the Stargate NetBridge gateway [36,37].

The new Linux gateway was built using an older, untested and unqualified version of the application XServe, provided by Crossbow. This version of XServe was chosen because it is compatible with open-source Linux operating systems running x86 computer architecture. This not only made the gateway more reliable, but also provided the convenience of having the WSN gateway capable of running on a laptop or PC. XServe was successfully integrated with a compatible PostgreSQL database for collecting and storing WSN data. The Linux gateway was also outfitted with TinyOS, which provided the ability to write, compile, and program wireless mote applications. XMesh library files, including Crossbow's applications for wireless motes, were also added to the gateway. The final Linux gateway is operated on an AOpen BB10 mini PC running an Ubuntu 10.04 LTS operating system. A suite of software programs were added to the Linux gateway that perform a variety of tasks including backing up WSN data, tracking IP addresses, and recording internal CPU temperatures of the gateway.

During the time that the Sluggo gateway was in use, remote connectivity was made using a simple web service manager. The Apache AXIS2/C web service was chosen because it was compatible with Sluggo's architecture and had low computational power and memory requirements. The Sluggo gateway operated as the server while a computer located on University grounds, with the client software installed, requested daily data for downloading.

Following the move to the new Linux gateway, Dropbox, a file synchronization and backup service, was used in place of AXIS2/C. Dropbox provided a more sophisticated and user-friendly alternative. In addition, the web-based WSN management system, INDAMS (Integrated Network and Data

Management System for Heterogeneous WSNs) [38], was incorporated into the gateway for data monitoring, providing real-time network status and connectivity information.

3.2. Software Description

The initial WSN deployment operated using XMesh, Crossbow's mesh routing protocol. XMesh provides a self-healing and self-organizing networking service [39]. The application code for XMesh is compiled specifically for a mote architecture (e.g., MicaZ) and sensor board (e.g., MDA300). Arguments for programming the transmission frequency and node/group identifiers are also available. XMesh offers three power modes, which are assigned during the program compilation, including high power (HP), low power (LP), and extended low power (ELP). The ASWP testbed deployment uses the LP mode, where motes power off non-essential electronics when idle. Motes in LP mode can still forward messages from neighboring motes unlike motes programmed in ELP. For MicaZ and IRIS motes, XMesh does not support time synchronization of messages. Therefore, all message transmissions are made asynchronously.

XMesh generates three basic types of application packets, which are transmitted along the network and stored at the WSN gateway:

- *Sensor data*: correspond to the actual sensor readings of the motes and depends on the data acquisition board (MDA300, in this case). This packet type was configured with a sampling interval of 15 min.
- *Node health data*: contain node-level statistics that include the following accumulated counters: node health data packets generated at the node, total number of packets generated at the node (including all three packet types), number of packets forwarded from other nodes, number of retransmissions, number of packets dropped at the node, path cost to the base station (e.g., node cost), and information about the link connecting to the parent node. Counters for node health data packets and node generated packets reflect unique packet identifiers from the point of view of the WSN application; therefore, they do not include packet retransmissions.
- *Neighbor health data*: report the information of up to five neighbor nodes including their link information and path cost values. Neighbor health packets and node health packets are sent alternatively, one type after the other, and they are defined with a single interval named Health Update Interval (HUI). The HUI is set by default to 10 min, thus the effective transmission for each health data type is twice the initial HUI: 20 min.

XMesh's multi-hop routing is based on the Minimum Transmission (MT) cost metric aiming to minimize the total energy consumed to transmit a packet to the base station [39]. In order to send a packet, each node always selects the neighbor with the minimum cost (denoted as parent node). There are two costs defined in XMesh: one associated to a link and one associated to a node. A node computes the link cost to each of its neighbors and also broadcasts its own node cost. As part of an iterative process, started by the base station with node cost equal to zero, each node receives its neighbors' node cost and adds to it the corresponding link cost. Based on these values, the node selects a parent node and updates its own node cost to broadcast it again to its neighbors. From this perspective, it can be seen that XMesh works in a similar way as other mechanisms based on the Estimated

Transmission Number (ETX) given that the node cost, or path cost as referred to in the node health data, is proportional to this value [40]. Node costs and all routing information are exchanged periodically using Route Update (RU) messages and the frequency of the message exchange is defined by a fixed Route Update Interval (RUI). For this deployment, the RUI was initially set to 36 s during the period of the Sluggo gateway and after July 2011 (*i.e.*, the change to the Linux gateway, see Figure 4), it was increased to 128 s for reducing the routing traffic in the network. In terms of quality of service (QoS), XMesh specifies an end-to-end acknowledgement in addition to the data link layer acknowledgement [39]. In this QoS mechanism, the base station sends an acknowledgement back to the origin node after receiving a packet and by default it is only applied to node health packets.

The commercial WSN routing protocol was replaced at the end of July 2013 by an open source approach based on the TinyOS 2.1.2 implementation of the Collection Tree Protocol (CTP) [41,42]. CTP uses the ETX as cost metric and, like XMesh, attempts to build a minimum cost tree within the network, relying on control packets for establishing the network topology. However, since the source code of XMesh is not available, it is not possible to confirm further details about its implementation. Still, a significant difference between these two approaches is that control traffic in XMesh does not adapt to network conditions and thus it always sends routing packets at a fixed rate, while CTP adjusts the transmission of control traffic for a faster response to specific topology changes.

The CTP-based application defines two packet types: *data packets* and *summary packets*. Data packets include all sensor readings and health statistics from each node, such as the total number of generated packets, forwarded packets, retransmissions, and dropped packets. Similar to node health packets in XMesh, the counter of generated packets in CTP reflects unique data packets from the point of view of the WSN application. Summary packets are defined to include further instrumentation information regarding ETX values (link and path ETX) and control traffic.

In addition, the application was configured in two different versions for relay and regular nodes, respectively. Relay nodes do not have external sensors and are flexible in their location. They are mainly deployed for improving network connectivity and providing alternative routes; therefore, all components controlling the ADCs on the MDA300 driver were disabled in these nodes for a more energy-efficient operation. Regular nodes do have external sensors attached through the data acquisition board, and thus, all components in the MDA300 driver are enabled. Moreover, the number of active ADCs can be customized for each WSN mote, according to their predefined configuration (e.g., regular nodes with 3, 5, or 6 external sensors).

The CTP-based WSN application was configured to periodically sample data packets every 15 min and summary packets every 30 min using TinyOS asynchronous low-power listening (LPL). Based on the experience with XMesh, it was noticed that waiting a complete cycle was ineffective for knowing if a mote boots correctly. Therefore, a faster way was required for receiving initial feedback from motes to help identify common problems (e.g., connection errors, battery problems, forgetting to turn the motes on, or defective hardware). Two mechanisms were included in the WSN application for supporting deployment tasks. First, motes were configured to blink their LEDs after booting. This simple mechanism helps to discover several common problems and allows the user to confirm if the WSN application started running in the mote. Verification can be done on-site before closing mote enclosures. After the LEDs blink to confirm their operation, they are automatically disabled to save battery power. The second mechanism uses a faster sampling rate for the first data packets. The initial experiments with

CTP showed that WSN nodes are able join the network in a very short time; therefore, by using a faster sampling rate (e.g., one minute) for the first ten packets, initial feedback (e.g., node parent, battery voltage, and sensor data) can be monitored through the WSN management system's web interface. This helps to solve additional common problems such as using defective batteries or using the wrong version of a WSN application. Table 2 summarizes the parameters configured in the CTP-based WSN application deployed at the ASWP testbed. All other parameters not listed in the table use the default values.

Table 2. Summary of non-default parameters configured in the CTP-based WSN application deployed at the ASWP testbed.

Parameter	Value
Data sampling interval	15 min
Initial data sampling interval	1 min for the first 10 packets
Summary packet interval	30 min
Radio channel	26
Transmission power	Maximum
Low-power-listening (LPL) sleep interval	1 s
Maximum CTP retransmissions	7 attempts
Maximum Trickle timer interval	1 h

4. Network Performance

The mechanisms to evaluate the network performance and inform end-users about the network status at any time are important aspects of WSN deployments, in addition to the objective of the main application. For this purpose, a methodology for network analysis is examined based on one of the main concerns of end users for WSN deployments: data quality.

Data quality is often evaluated based on statistical methods that consider the amount of samples available and the precision of instruments. When WSNs are used as data gathering mechanisms, samples collected by mote sensors are forwarded as packets towards the base station. Major factors that may affect the quality of the data include packet duplications and packet losses, which should be considered before any domain-specific analysis. Most protocol stacks available for WSNs, including XMesh and CTP, provide different mechanisms for addressing, though only partially, these problems.

In long-term deployments, such as the ASWP testbed, all motes will eventually consume out their energy resources and stop working. Therefore, it is necessary to make periodic visits for replacing mote batteries. Additionally, these visits may include replacement of broken motes, node relocations, and other miscellaneous replacements and/or repairs (e.g., external sensors). However, the battery replacement at each node introduces a perturbation in the network for routing to adapt and eventually stabilize, which presents additional tradeoffs for maximizing the network performance and, at the same time, minimizing the frequency of these visits (*i.e.*, maintenance costs).

4.1. XMesh

An analysis of the network behavior is presented, which aims to address the key points previously mentioned regarding the quality of the collected data. For the analysis of the application based on

XMesh, the selected dataset starts on August 2011, after the Linux gateway was deployed, and continues until August 2012, covering one year of operation (see Figure 4). During this year the testbed was exposed to different seasons and weather allowing a comprehensive network evaluation. The dataset contains more than 900,000 packets including sensor data, node health data and neighbor health data, divided into two periods to examine the effect of deploying the two additional IRIS motes in the testbed. Table 3 lists the evaluation periods: period 1 (P1) and period 2 (P2), before and after the additional IRIS motes, respectively. Likewise, shorter time periods of one month of operation were selected for each larger period to account for short-term performance, in which the effect of the network maintenance is reduced. Selected sub-periods correspond to the month with the best performance and highest number of connected nodes. Table 3 also presents the maximum, average, and minimum daily connected nodes in the network for each time period and sub-period.

Table 3. Definitions of the two XMesh evaluation periods and the two sub-periods, including time range, number of deployed nodes, and daily connected nodes (maximum, average, and minimum).

Period		**P1**	**P1a**	**P2**	**P2a**
Range		August 2011–February 2012	15 September 2011–20 October 2011	March 2012–August 2012	1 July 2012–4 August 2012
Description		Before IRIS motes	Sub-period of P1	After IRIS motes	Sub-period of P2
Deployed Nodes		40	40	42	42
Daily Connected Nodes	**Max.**	39	37	41	41
	Avg.	24	22	34	36
	Min.	4	4	4	25

XMesh defines the node health packet counter, which works as an application-layer sequence number for this packet type. This 16-bit counter initially starts at one and increments after every new generated node health packet, allowing for up to 65,535 packets to be identified. In this case, the effective collection rate for each type of health packet (*i.e.*, node health and neighbor health) is 20 min; then, the sequence number would be enough to consider all consecutive packets within a period larger than 900 days, far exceeding the battery life of motes operating without energy-harvesting mechanisms.

Using the node health packet counter, it was found that around 3% to 4% of the received packets corresponded to duplicate packets. These results show the need to include an initial pre-processing stage for identifying and removing these packets from datasets. However, since node health is the only packet type in XMesh that includes a counter field to uniquely identify each packet, it was necessary to devise an algorithm that identifies and removes duplicates for the sensor and neighbor health data.

The main idea behind our devised duplication deletion algorithm is that by comparing the content of two received packets from the same node, it can be identified if one of them was duplicated with high accuracy, given that for each node it is unlikely to obtain all sensor readings with exactly the same values. With this idea, any two packets from the same origin node can be compared and duplicates can be identified.

Additional assumptions were introduced in this context. First, it is assumed that the sampling period, represented as T, is large enough so that each packet is either delivered or dropped before the next packet

from the same node is generated. This assumption limits the interval in which packets could be duplicated and it is denoted as the *effective interval*. Due to the fact that in XMesh there is no synchronization and no global notion of time in the motes, the timestamp of each packet is assigned when they are received at the gateway. Based on this, a delay is defined, denoted as ∂T, which represents the time duration between the moment a packet is generated and the moment the packet is received at the gateway, including processing, queuing, transmission, and propagation delays along the path. This value is considered in the effective interval to avoid any misclassification caused by delays during transit in the network. The procedure is presented in Algorithm 1.

Algorithm 1: **Identifies and Removes Duplicate Packets**

Input: Packets from the same node ordered by time and marked as valid packets

Output: Packets marked either as valid or duplicate

Begin

While $pkt_i = nextValidPacket()$ do *//loop on* pkt_i
  While pkt_i *is valid* AND
  $pkt_j = nextValidPacket()$ do *//loop on* pkt_j
    If $|pkt_i.time - pkt_j.time| < T - \partial T$ then
      // pkt_j *is in the effective interval of* pkt_i
      If $pkt_i.content == pkt_j.content$ then
        // pkt_i *and* pkt_j *have the same content*
        Mark pkt_j as a duplicate of pkt_i
      End
    Else *//* pkt_j *is on the next interval*
      Break loop on pkt_j
    End
  End
  $pkt_i = nextValidPacket()$
End *// end loop on* pkt_i

End

The algorithm validation was performed using the node health data as truth data. Using the node health packet counter, the truth values for duplicate packets received at the gateway were identified. Then, the counter information was removed from the received node health packets and the duplication deletion algorithm was executed. Obtained results indicate that the algorithm does not misclassify any valid packet as a duplicate, giving zero false positives; however, the algorithm may not identify some real duplicates (*i.e.*, false negatives). The percentage of received duplicate packets calculated for both XMesh evaluation periods, based on an experimental ∂T equal to 2 min, are presented in Table 4. Based on the results obtained from this validation using the node health data, we believe that the devised duplication deletion algorithm should achieve similar effectiveness for both the sensor data and neighbor health data packets.

Table 4. Percentage of duplicate packets received for each packet type per time period ($\partial T = 2$ min) during the two XMesh evaluation periods.

Period	Node Health Data Duplicate % (with Seq. Number)	Node Health Data Duplicate % (with Our Algorithm)	Sensor Data Duplicate %	Neighbor Health Data Duplicate %
P1	4.10%	4.04%	3.82%	3.65%
P2	3.16%	3.07%	3.01%	3.08%

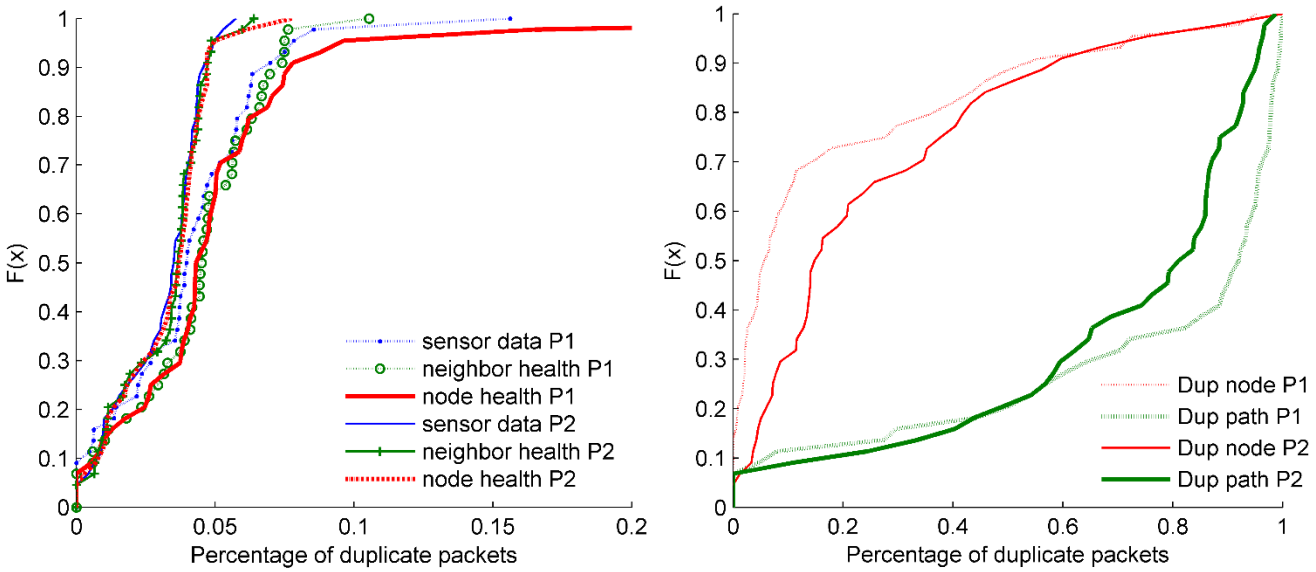
An additional observation, with respect to the duplicate packets received, is that the percentage is higher for node health data, compared to those of the sensor data. This could be explained as an effect of the end-to-end acknowledgement QoS mechanism used in XMesh, which may increment the number of retransmissions for this type of packet. However, with the information available it is not possible to determine the exact number of retransmissions associated to each packet type.

With the information provided by the node health data in XMesh, duplicate packets generated at the origin node and duplicate packets created at forwarding nodes can be distinguished. This classification is possible because if duplicate packets are generated at the origin node, then the retransmission counter is updated before each attempt. Therefore, if a packet is received with the same sequence number (*i.e.*, node health packet counter) and different content due to the retransmission counter increment, then it corresponds to a packet duplicated at the origin. Otherwise, if a duplicate has the same sequence number and the same content, then it corresponds to a packet duplicated by one of its forwarding nodes. The increment in the number of retransmissions of the forwarding nodes will be reflected in their own node health packets.

In Figure 5a, the cumulative distribution function (CDF) for the percentage of duplicate packets received from each node in the three packet types is presented. Around 95% of the nodes present less than 10% of duplicate packets and there are a few outlier nodes that can have up to 20%. It can also be seen that when comparing results for periods P1 and P2, there is a slight difference because a few nodes presented a higher number of duplicate packets during P1, including outlier nodes which were mostly due to hardware and software failures. Figure 5b shows the percentage corresponding to each type of duplicate based on the number of duplicate packets received at the sink: packets duplicated at the origin node or packets duplicated at forwarding nodes along the path. The results obtained reveal that during P1, on average, 95% of the duplicates received from each node correspond to packets that were duplicated along the path, and only the remaining 5% were duplicated at the origin nodes. During P2 the duplicates are reduced compared to P1; however, most of the received duplicate packets, around 85%, are associated to duplications along the path. These results reveal the possibility that duplicates, and therefore the number of retransmissions and dropped packets, may be associated to specific nodes in critical locations. Those critical nodes can be identified as the same nodes with higher percentages of duplicates at the origin node in Figure 5a. This is because the critical nodes may be causing the duplications along the path for other nodes located farther from the base station, when attempting to forward their packets.

Once duplicate packets are removed, the statistics included in the node health data can be used to get a better idea of the network behavior. As mentioned in the previous section, XMesh's node health statistics define counters for node generated packets, forwarded packets, retransmissions, and dropped packets. Based on these counter values, the following indicators were adopted:

Figure 5. (**a**) CDF percentage of duplicate packets received per node for each packet type; (**b**) CDF percentage of each duplicate packet type: duplicates at the origin node and duplicates along the path.



(**a**) (**b**)

Packet Reception Rate (PRR): this value indicates the amount of data collected as the ratio between packets generated at an original sending node and packets received at the sink from that node, as defined in Equation (1). This indicator can also be computed for the entire network by aggregating the packets received and generated from all nodes, as shown in Equation (2), where N is the number of connected nodes in the network.

$$PRR_i = \frac{received_{pkts_i}}{generated_{pkts_i}} \quad (1)$$

$$PRR_{network} = \frac{\sum_i^N received_{pkts_i}}{\sum_i^N generated_{pkts_i}} \quad (2)$$

Packet Success Rate (PSR): this is an indicator to evaluate the probability that a packet has to be successfully transmitted to the parent node at any time, giving an estimate for the quality of the link as defined in Equation (3). Similarly, it can also be computed at the network level by aggregating the values from all nodes as shown in Equation (4).

$$PSR_i = \frac{generated_{pkts_i} + forwarded_{pkts_i} - dropped_{pkts_i}}{generated_{pkts_i} + forwarded_{pkts_i} + retransmitted_{pkts_i}} \quad (3)$$

$$PSR_{network} = \frac{\sum_i^N generated_{pkts_i} + forwarded_{pkts_i} - dropped_{pkts_i}}{\sum_i^N generated_{pkts_i} + forwarded_{pkts_i} + retransmitted_{pkts_i}} \quad (4)$$

The PRR and the PSR indicators provide two complementary measures about the network performance. The PRR reflects an end-to-end behavior and it is directly influenced by the WSN routing protocol; on the other hand, the PSR provides a measure of link quality between the sending node and its parent node, corresponding to a local characteristic. The PSR is influenced by both the routing protocol (*i.e.*, parent selection) and the external environment (*i.e.*, noise and interference causing packet corruptions and retransmissions).

Consolidated results at the network level are presented in Table 5. It shows that there is a slight improvement in the network PRR during period P2 compared to period P1, although P1 has a higher PSR.

Table 5. Network-level performance metrics for the two XMesh evaluation periods and their respective sub-periods, including packet reception rate (PRR) and packet success rate (PSR).

Period	PRR	PSR
P1	35.17%	49.09%
P1a	61.04%	53.92%
P2	36.01%	46.08%
P2a	42.16%	45.33%

The results for sub-periods, P1a and P2a, illustrate the impact of factors that arise from the long operational time periods. P1a reached the highest network PRR at 61.04%, a 74% increment compared to that of the full period P1. On the other hand, P2a only reached 42.16% network PRR, a 16% improvement compared to that of the entire period P2. This smaller difference in P2 indicates that during this period the network topology presented some additional problems that could be associated to increments in the network traffic. Similarly, the sub-periods show the potential performance of the network for longer time periods.

Relating the above results with field observations, it was noticed that during P1 the network performance was highly impacted by mote failures, resulting in major network partitions disconnecting nodes in Sites 2 and 3 from Site 1. During P2, with the additional two IRIS relay nodes, major network partitions between Site 1 and the remaining testbed were mostly resolved and the network performance was slightly increased. However, during that time the network was suffering some degradation of the link quality, reflected by the reduction of the PSR. As a reference for these results, the indoor experiment presented on [43] obtained 86% packet success rate for MicaZ motes running TinyOS. Although the WSN motes in the ASWP testbed are running a different routing protocol, this significant difference in the PSR reflects the impact of the outdoor environment on XMesh.

The effect of the number of connected nodes in the network is illustrated in Figure 6, where the network PRR is plotted as a function of the number of connected nodes for each month in the time periods P1 and P2. It can be seen that for similar numbers of connected nodes, major changes in the network PRR occur, which are the result of variations in the network topology as different nodes leave and enter the network (e.g., after battery depletions and network maintenance). Examples of these observations are the highest PRRs in the figure, which correspond to 19 and 16 connected nodes, respectively; nevertheless, 20 connected nodes produced the lowest PRR during these time periods. Such high network PRR values occur when only nodes from sites closer to the base station are connected, and the performance is reduced as nodes from farther sites connect to the network. The figure also confirms that the XMesh application at ASWP testbed presented congestion problems, especially when operating under heavier traffic generated from a higher number of connected nodes, as seen for period P2 after the deployment of the additional IRIS motes.

An additional perspective for the performance of the network, and specifically for the XMesh routing protocol, is presented in Figure 7 with the nodes' PRRs, PSRs, and average path costs. First, with respect to the node PRRs, it is possible to see that most nodes in Site 1, which are closer to the base station, were

able to maintain higher percentages, between 50% and 64%, compared to the rest of the nodes in the testbed. The PRRs for most nodes in Site 1 are comparable to the highest network PRR obtained during sub-period P1a. It is observed that there were a few low peaks in the nodes' PSR, indicating that those forwarding nodes across the testbed presented a lower link quality.

Figure 6. Network PRR *versus* number of connected nodes in the network when using XMesh. PRRs are computed monthly and the number of connected nodes is computed as the average of daily connected nodes within the network in the same time period.

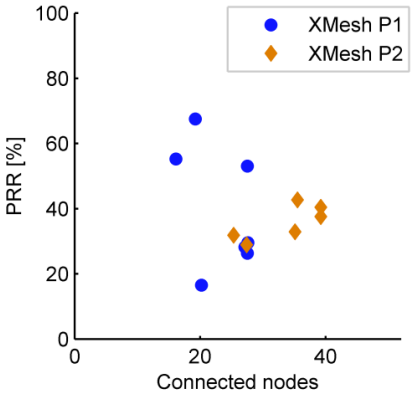
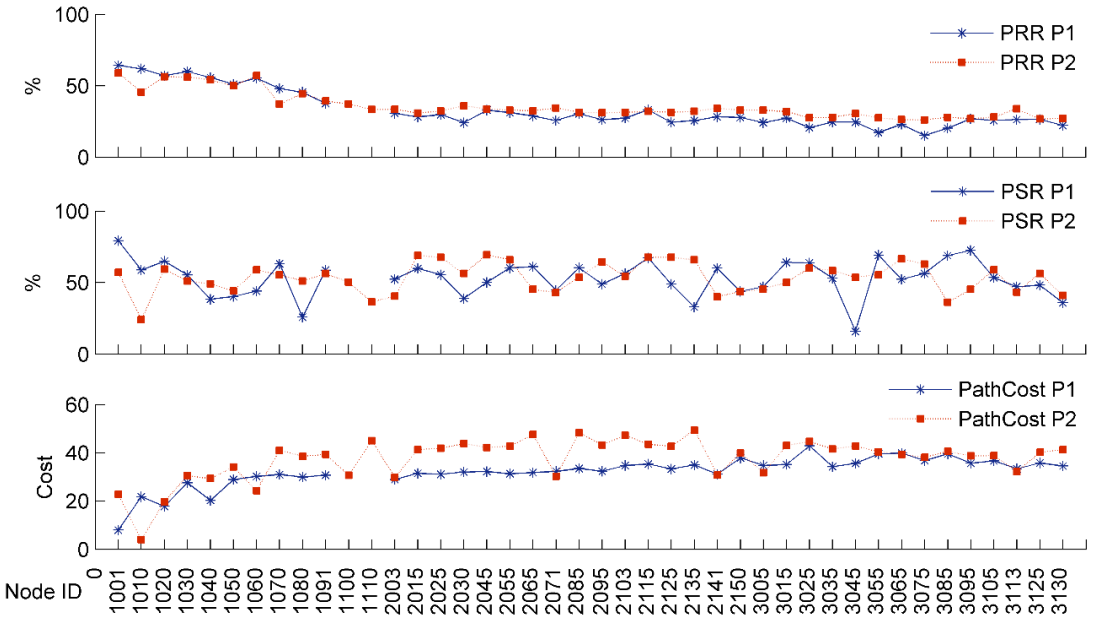


Figure 7. Daily averages of individual node packet reception rate (PRR), packet success rate (PSR), and XMesh path cost during evaluation periods P1 and P2.

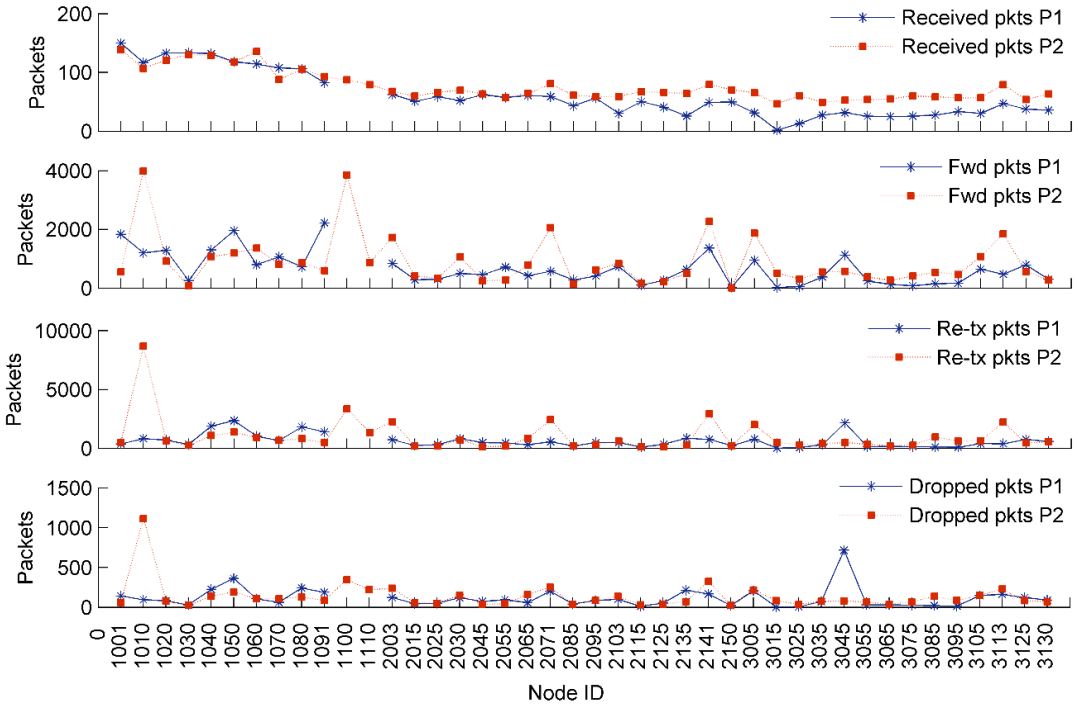


An unexpected result was that several nodes with relatively low PSR (e.g., nodes 1010, 1040, 1060, 2071, 2141, 3045 and 3113) reported lower path costs for routing. For example, node 1010, regardless of having one of the lowest PSRs, kept reporting the lowest path costs during P2 at its critical location close to the base station. Therefore, it was the most likely node to be selected as a parent after the base station.

To further analyze potential causes behind high packet losses, node health statistics were processed at the node level and Figure 8 presents the results for each node in average daily values. Most nodes

located in Site 1 have a higher number of received packets and these values decrease for nodes located in Sites 2 and 3. Comparing the node packets received between P1 and P2, it can be seen that nodes located farther away from the base station consistently had a lower number of received packets, as reflected in the figure by nodes with higher node identifiers. Furthermore, when considering forwarded packets, there are a few nodes (*i.e.*, 1010, 1100, 2071, 2141, 3005, and 3130) which were highly used by their neighbors. These nodes established a highly used path across the network topology (see Figure 3), which at the same time was accountable for most of the packet retransmissions and drops.

Figure 8. Daily average node packets received, packets forwarded, packets retransmitted and packets dropped per node during XMesh evaluation periods P1 and P2.



4.2. CTP

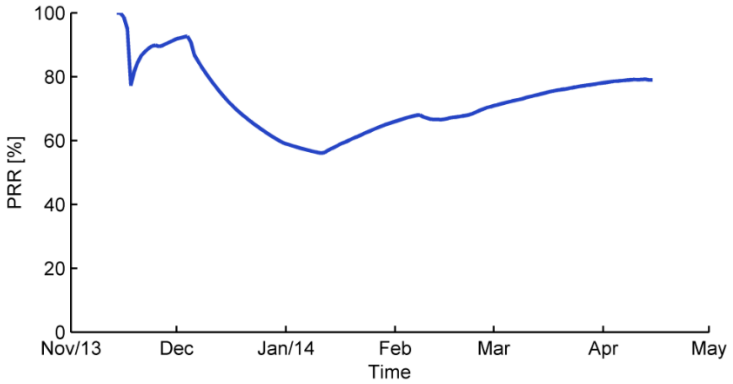
The analysis of the network performance after deploying the CTP-based WSN application is presented for the data collected from November 2013 to April 2014 (see Figure 4). This dataset has more than 475,000 packets, including sensor data packets and summary packets. During this period, the ASWP testbed had 52 motes deployed in Sites 1 through 5 as described in Section 3.

Duplicate packets received at the sink node are identified using the sequence number defined in the CTP header and the additional health information implemented for this version of the WSN application. It was found that only 0.2% of the packets received at the WSN gateway are duplicates, showing that CTP is effective in detecting and removing duplicate packets. This functionality in CTP identifies duplicates in the same collection tree using a small cache and saving the origin node's identifier, the CTP sequence number, and the Time Has Lived (THL) fields from transmitted packets. In this way, the routing protocol only considers 1-hop duplicates and avoids discarding looping packets. Each node tracks the number of duplicates detected and removed, which is reported in the instrumentation information received in summary packets. Based on this information, the 1-hop duplicate rate at the

network level obtained for this time period of six months is 1.5%. Overall, the control of duplicate packets in CTP is effective, especially considering that most duplicates are detected in their first hop and thus unnecessary transmissions are avoided.

A significant improvement is observed in the PRR and PSR during this six-month period, in which CTP achieved 79% PRR and 96% PSR; however, network partitions remain an important challenge. Knowing that nodes may leave and enter the WSN as their batteries are depleted and replaced (or in the event of hardware failures and repairs), there are different situations in which the routing protocol is found not able to reestablish a path to the base station. Figure 9 shows the behavior of the PRR at the network level when using CTP. It can be seen that after December 2013, the PRR has a significant reduction, which was caused by a major network partition when an important relay node stopped working. This situation was solved in early January 2014, by replacing and relocating different relay nodes in Site 1. The high PSR is also consistent with these observations, indicating that overall the WSN does not have problems forwarding data packets and therefore, the reduction in the PRR may be related to routing problems at specific nodes.

Figure 9. Network-level packet reception rate (PRR) during the CTP evaluation period.



For further analyzing the behavior of data traffic, the network-level cost of transmissions was computed according to Equation (5) given below. The intuition behind this indicator is to compute the average number of transmissions required in the network for the successful delivery of one packet to the base station, based on node health statistics. Figure 10 shows the cost of transmissions along time, ranging between 3 and 4 most of the time. The curve shows increments during November/December 2013 and January/February 2014 which correspond to maintenance activities that increased the number of connected nodes in the network. Furthermore, after January 2014, most maintenance activities are focused on nodes located farther than Site 1, introducing a higher number of forwarded packets and retransmissions, thus increasing the cost of transmissions at the network level.

$$Cost\ of\ Tx = \frac{generated_{pkts} + forwarded_{pkts} + reTransmissions}{generated_{pkts}} \quad (5)$$

Control traffic is also instrumented in the CTP-based application. Figure 11 presents the total network-level transmissions and receptions of control packets. It can be observed that the number of control packet receptions is higher than control packet transmissions, reflecting the effect of broadcast control messages received by multiple neighbor nodes. For analyzing the effect of control packets, Figure 12 compares this control traffic with data traffic transmissions in the network. It shows that the

number of transmissions in control packets is higher than data packets, although the behavior of the curves is different. On one side, data packet transmissions are expected to have a linear behavior, sometimes affected by battery depletions, while control packet transmissions tend to stabilize over time. Furthermore, only after four months of operation, the data traffic exceeds control traffic in number of transmissions; however, control packets still consume more energy because broadcast messages use the entire LPL sleep interval.

Figure 10. Network-level cost of transmissions during the CTP evaluation period.

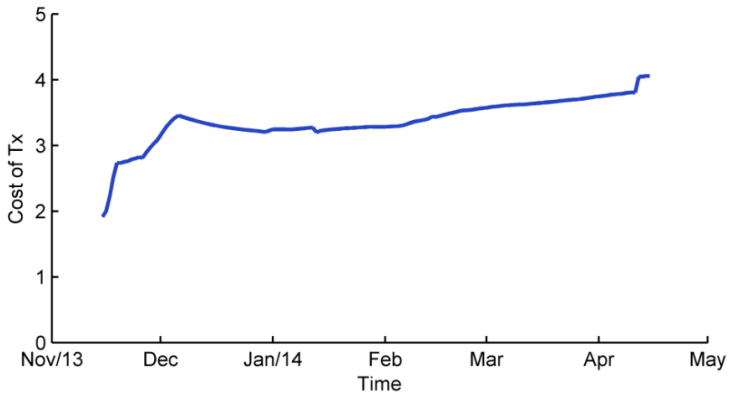


Figure 11. The cumulative number of network-level control packet (Ctrl Pkt) transmissions (Tx) and receptions (Rx) during the CTP evaluation period.

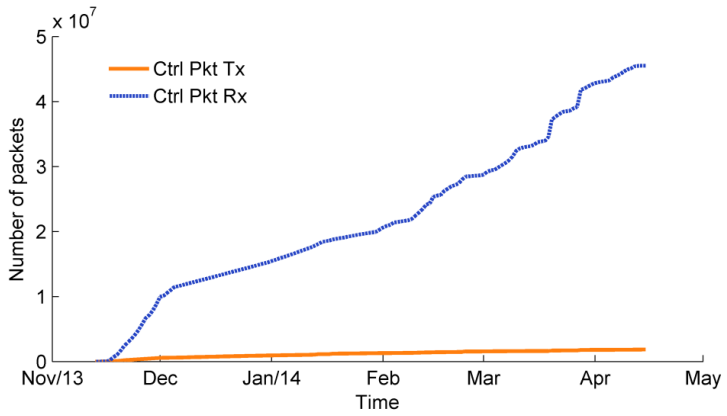


Figure 12. The cumulative number of control packet transmissions and data packet transmissions during the CTP evaluation period in the network.

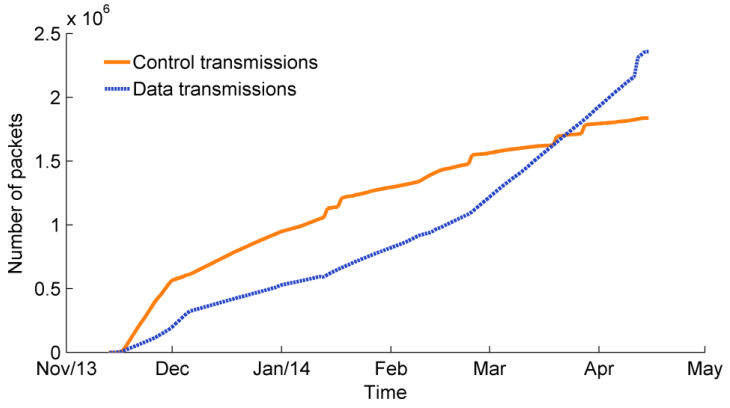


Figure 13 shows the network PRR as a function of the number of connected nodes for each month analyzed for CTP. In this case, higher network PRRs are observed for higher numbers of connected nodes. This indicates that when using CTP, the network improves its throughput and thus, as more nodes are connected, CTP seems to not present problems forwarding the increased generated traffic.

Figure 13. Network PRR *versus* number of connected nodes in the network when using CTP. PRRs are computed monthly and the number of connected nodes is computed as the average of daily connected nodes within the network in the same time period.

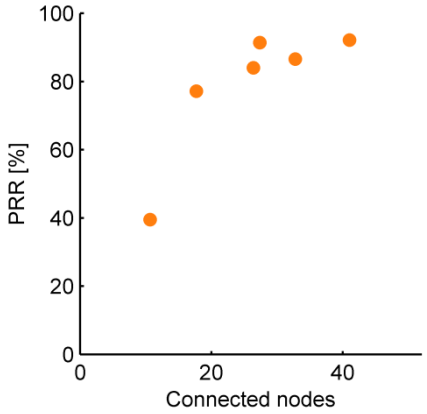
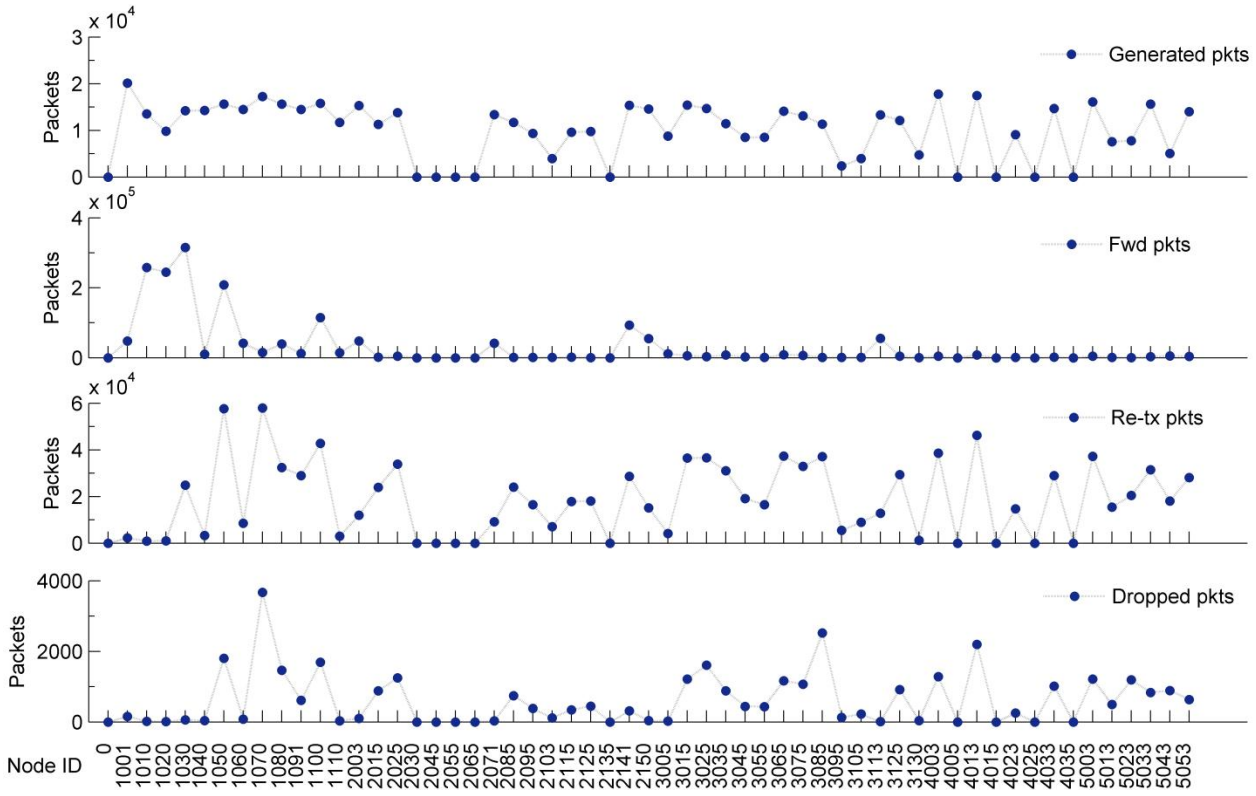


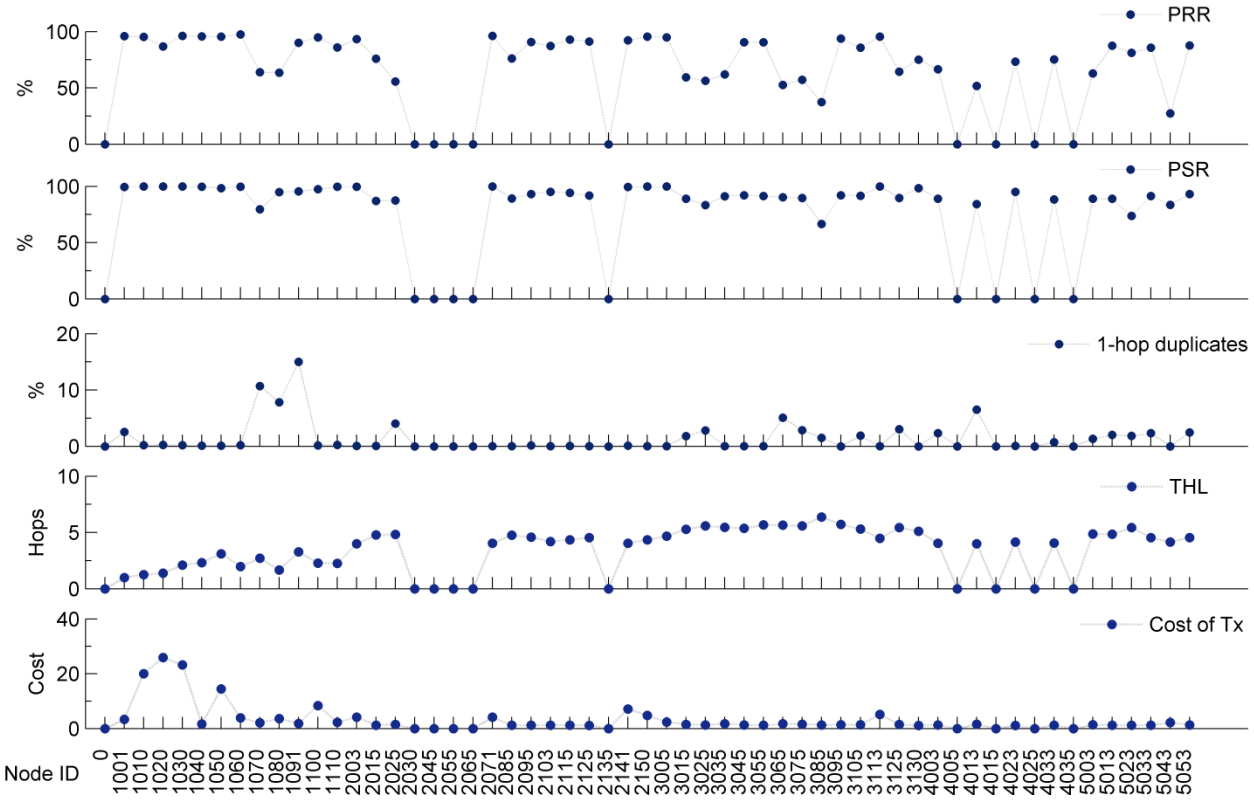
Figure 14. Node-level health information totals for packets generated, forwarded, retransmitted and dropped during the CTP evaluation period.



We further study the performance of the ASWP testbed using the node-level results shown in Figures 14 and 15. Forwarded packets in Figure 14 confirm the existence of highly used nodes

(*i.e.*, 1010, 1020, 1030, 1050, 1100, 2141, 2150 and 3113), which forward most of the traffic in the network. In addition, these nodes do not show a low PRR or PSR, as seen in Figure 15, indicating that they are able to handle these traffic conditions. However, whenever nodes at these hot spots deplete their batteries, network partitions may occur, as experienced during December 2013.

Figure 15. Node-level packet reception rate (PRR), packet success rate (PSR), percent single-hop duplicates, average time has lived (THL) and cost of transmissions during the CTP evaluation period.



5. Network Costs

The network costs include the physical costs of the WSN deployment (e.g., devices and materials), the tangible costs of labor associated with the WSN deployment and operation (e.g., hours worked and distance traveled), and the miscellaneous costs associated with the maintenance of the network (e.g., hardware and battery replacements). Table 6 shows the overall summary of these costs, which are explained in further detail in the following subsections. The labor and maintenance costs are cumulative for the period from May 2010 to the end of April 2014.

Table 6. Summary of network deployment costs and the total labor and maintenance costs for four years of network operation.

Category	Total Cost	%
Deployment Costs	$31,500	52
Labor Costs	$23,900	40
Maintenance Costs	$5000	8
Total	$60,400	100

5.1. Deployment Costs

The deployment costs of a WSN include all the physical components necessary for operation (e.g., hardware, sensors, batteries, and enclosures). Table 7 presents a categorical breakdown of the network's physical costs associated with the network deployment up to May 2014. While growth and change in technology and industry produce fluctuating prices of products, the costs presented in the table are meant to show relative costs of the network rather than an absolute. It can be seen that over half of the physical costs of the network are associated with the WSN hardware, including the network gateway, motes, data acquisition boards, and antennas. The total cost of this network of 52 nodes is approximately $31,500, including the costs of the 149 external environmental sensors. For the network's nodes, the difference between the costs of relay nodes and regular nodes with external environmental sensors is about $330 to $700, respectively.

Table 7. Summary of the ASWP WSN physical costs.

Category	Description	Cost
Hardware	Wireless motes, antennas, gateway, *etc*.	$15,940
External Sensors	Soil moisture and sap flow.	$12,600
Power	Batteries (AA, D, 12 V).	$1500
Enclosures	Waterproof boxes, insulation and desiccants.	$1400
Mounting	PVC pipe, wiring, nuts, bolts and screws.	$60
Total	**Cumulative cost.**	**$31,500**

The sensor costs of a WSN deployment will depend on the nature of the study. In this work, soil moisture and/or sap flow sensors were installed at 35 out of the 52 nodes. The WSN operates on rechargeable NiMH AA batteries, which have a nominal voltage around 1.2 V, such that three batteries in series are used to power the mote. Following about two years of active charging and discharging, the batteries no longer hold appreciable charge and must be replaced. Over 700 batteries were originally purchased (approximately $2.2 each) to maintain over 150 batteries that are used in the motes of the WSN. The power costs are a combination of replacing old batteries as they go out of use and the cost of electricity to charge them. In addition to the batteries required for powering the motes, which also power the external soil moisture sensors via the voltage excitation output on the MDA300, ancillary 12 V batteries were used for powering the external sap flow sensors.

The estimated area covered by Sites 2 through 5 is 5000 m^2 (using GIS polygon coverage). Assuming the "sensed" area for each regular node (*i.e.*, soil moisture and/or sap flow sensors) to be around 6 m^2 (due to the heterogeneous nature of the site), the density of actual measurements to coverage area is about 4% (for 35 regular nodes). Based on the deployment costs, the WSN costs $150 m^{-2} of sensed area. Including the results presented in Table 6, the approximate cost of the sensed area, adjusted for labor and maintenance, is $184 m^{-2} y^{-1}. While these costs may not be uniformly scalable across disciplines or with network size (e.g., larger WSNs may require additional gateways), it serves as a point of reference for comparison with other data collection technologies (e.g., data loggers).

5.2. Labor Costs

The deployment of WSN nodes and their maintenance requires spending time and effort. The labor costs are related to the time preparing for and spent in the field as well as the transportation costs to and from the field. An estimation of the labor costs is presented here by translating the time spent and distance travelled into a dollar cost.

Deployment time includes the time spent checking the network status, changing mote batteries, replacing broken or faulty equipment, adding new nodes to the network, updating the network's gateway, and installing environmental sensors. The time to deploy a new node depends on the node type. A relay node requires less time than a regular node because it does not have additional sensors to set up and install. Once a location is determined, a relay node may be readily switched on and placed in the field to begin operation in the network. A regular node requires additional activities such as burying sensors into the soil and/or attaching sap flow sensors to a tree, which are typically done while the mote is switched off. Following deployment, each node in the network also requires regular maintenance.

By far, the most recurrent maintenance task is the replacement of discharged batteries. Between May 2010 and the end of April 2014, we performed replacement of batteries 128 times out of 154 field visits, as seen in Figure 16. However, not every field visit to change node batteries is successful (e.g., faulty equipment or faulty batteries), requiring multiple successive field visits to restore network connections. The number of field visits during the Sluggo era (see Figure 4) occurred more frequently due, in part, to network expansion (*i.e.*, deployment phases) and node relocations (as described in Section 3) and issues regarding the rechargeable batteries. It was found that the rechargeable AA batteries do not uniformly hold their charge, resulting in varied battery charge levels after recharging. A screening process, where only batteries that maintain adequate charge following a recharging were used in the network, resulted in longer battery life as indicated by fewer dots in Figure 16 from mid-2011 until the end of 2012. Network maintenance was reduced during 2013 after some initial bugs in the CTP application. These problems were solved in November 2013 and regular field visits were resumed as nodes started to deplete their batteries. Based on the battery maintenance schedule in Figure 16, the average time (and standard deviation) between battery changes for each node (about 58 days) is presented in Figure 17. The red line indicates the average time between field visits (*i.e.*, considering all the nodes in the network) to be about 12 days.

Each field visit is recorded in a log where the time spent at the field can be retrieved. The labor costs are obtained by computing the total time spent in the field plus some additional time for preparation before each trip. Preparation time may include charging and sorting batteries, pre-programming motes, preparing mote enclosures, and building and testing environmental sensors. Transportation costs are also included, accounting for the physical distance travelled between the university and the WSN site.

Based on the field log, the average time spent on site is estimated to be about 6 hours per visit. To account for preparation time before field visits and the occasions where there are additional field workers, this time was adjusted by a constant multiplier of 1.6 (*i.e.*, a total of 9.6 hours per visit). A cost of $15/h was assumed (based on graduate and undergraduate students' salary). The transportation cost was computed by multiplying the round trip distance (about 20 miles) by a constant transformation factor of $0.565/mile. Table 8 shows the summary of the cumulative labor costs up through April 2014 (approximately $23,900) and the average cost per visit for the same time period (approximately $155).

Figure 16. Battery changing schedule from initial network deployment until the end of April 2014. For each node in the network, days when a node's batteries were changed are indicated by an orange dot.

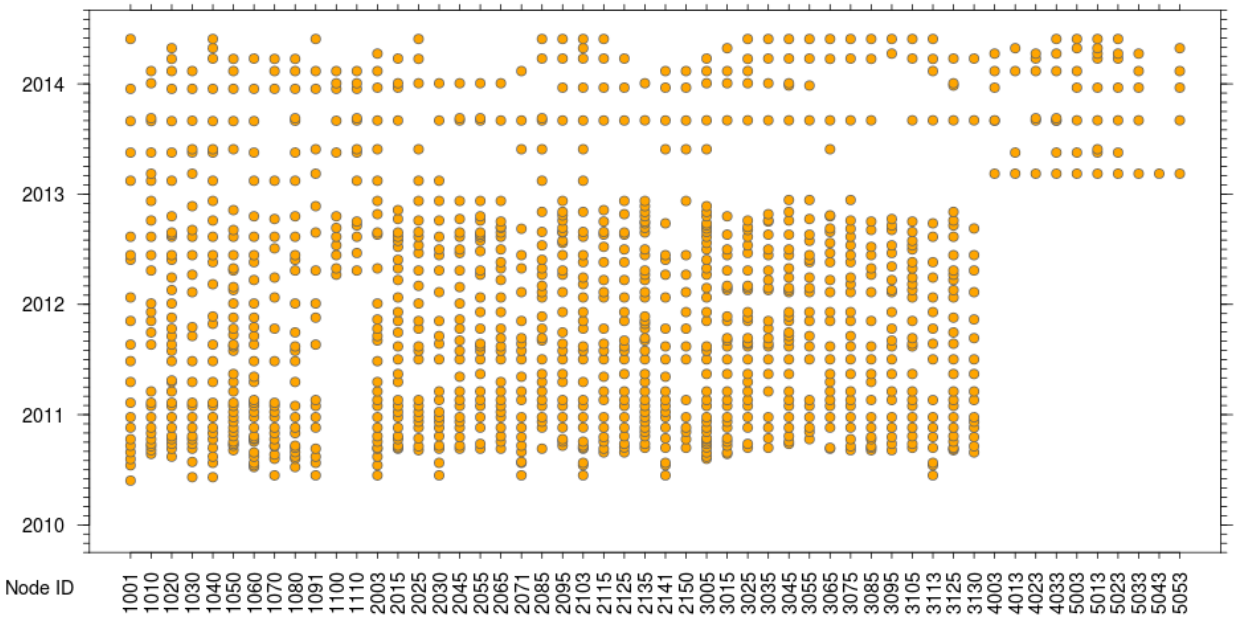


Figure 17. Average and standard deviation of time between battery changes for each node. The red line is the average time between network field visits for battery maintenance.

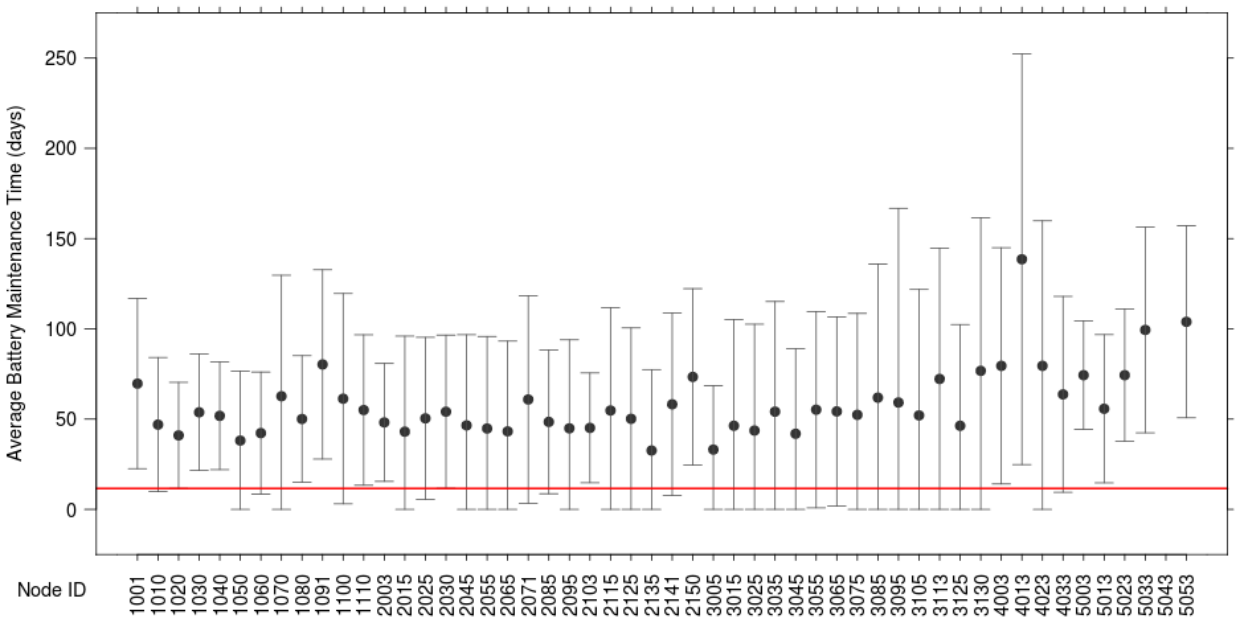


Table 8. Summary of cumulative labor cost and averaged cost per visit.

Category	Total Cost	Per Visit	%
Time Cost	$22,200	$144	93
Transportation	$1700	$11	7
Total	**$23,900**	**$155**	**100**

5.3. Maintenance Costs

The maintenance costs are defined here as the costs of replacing hardware, enclosures, and power (spare batteries). The hardware includes antennas, data acquisition boards, and motes. The antennas are the most vulnerable part of the hardware because they are exposed to the environment. Most of the damage to the antennas is due to animals (e.g., chewing damage by squirrels and chipmunks) and falling tree limbs (e.g., under windy conditions).

The enclosures suffer from mechanical stresses due to the need of frequent access to the mote batteries (e.g., opening and closing of the lid) and thermal stresses due to changes in temperature (e.g., freezing and thawing of water along seems and joints). The enclosures attached to trees (*i.e.*, for sap-flow sensing nodes) undergo additional mechanical stresses caused by the natural growth of the tree and, in some cases, the enclosure is fractured leaving the electronic equipment inside vulnerable to water intrusion.

Water is a leading cause of malfunctions in node hardware. It short-circuits electronics causing batteries to discharge rapidly and potentially damage sensitive circuitry of the mote or data acquisition board. Water also rusts metallic components, deteriorating batteries, wires, and motes. The quality of rechargeable batteries used to power the motes also deteriorates over time.

Table 9 shows that the cumulative cost of maintenance of the WSN is about $5000 and the average cost per visit is about $32.

Table 9. Summary of cumulative maintenance cost and average cost per visit.

Category	Total Cost	Per Visit	%
Hardware and Enclosures	$3700	$24	74
Power	$1300	$8	26
Total	**$5000**	**$32**	**100**

5.4. Unforeseen Costs

For the ASWP WSN, circumstances were encountered that resulted in unexpected overhead of maintenance and labor costs. Three of such circumstances are given here, including: node ID change phenomenon, network outage battery loss, and Internet security.

5.4.1. Node ID Change Phenomenon

Node identifiers (IDs) are the unique numbers configured for each mote in the network. Nodes were assigned four digit numbers that were associated with the node's location (*i.e.*, site number), orientation (PVC mounted, tree mounted, or wire hung from a tree branch) and sensor configuration. Therefore, node identifiers serve a vital role in network monitoring, such that data can be correctly analyzed.

Throughout the deployment time of the network, there have been isolated incidents when a node ID is permanently changed to a different value at runtime (e.g., node restart). The initial impression was that the issue might have been related to the Sluggo gateway, where incidences of data corruption were common. However, the occurrence of node ID changes continued after the adoption of the Linux gateway. It was then suspected that the issue was with XMesh (e.g., unsuspecting bugs in the proprietary software). This hypothesis was also dismissed when node ID changes were found after the switch to the

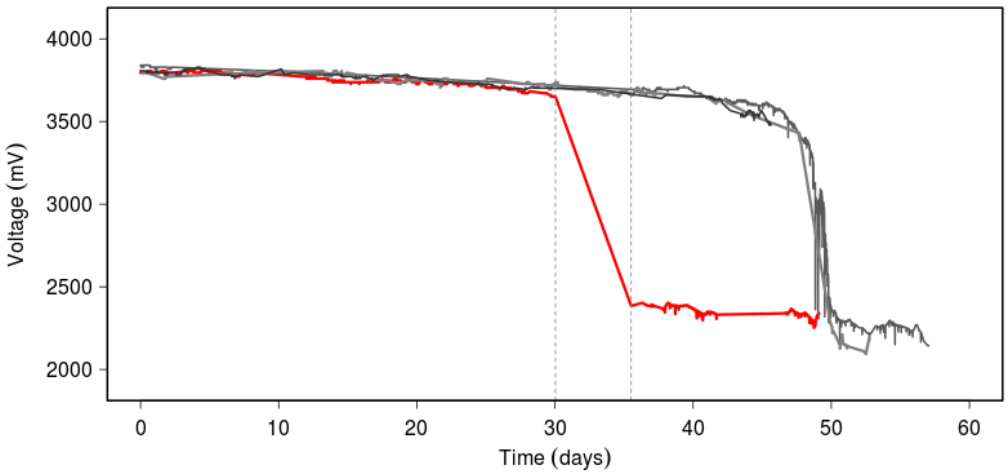
CTP-based application. At least 18 occurrences of node ID changes have been encountered during the first four years of the network deployment. The cause of node ID changes remains an open problem. Still, in most cases, it is possible to determine the original node ID by analyzing features of the data such as mote type (MicaZ/IRIS), type of application (relay/regular node), number of environmental sensors, and neighboring node IDs (e.g., parent and child nodes).

Due to the unpredictable nature of node ID changes, their occurrence is not always noticed until the data are analyzed. Their presence adds maintenance costs to the network in the form of identifying a switched node's original ID and mapping the old and new node IDs for network and environmental data analysis. Currently, node ID changes are logged in a spreadsheet; however, to facilitate data analysis, node ID maps may be incorporated directly into the network database.

5.4.2. Network Outage Battery Loss

The gateway, powered by the general electric grid power in the BFNR Nature Center, is susceptible to building power outages. Such instances are typical during storms when lightning strikes or high winds cause breakages to electrical supply wires. During gateway outages, the base station is offline from the wireless network. Without the base station, there is no root node, thereby causing the path cost to increase throughout the network and looping packets will continuously appear. Moreover, route updates continue to be transmitted amongst the nodes in the network. In the CTP-based application, as routes are continuously lost and updated due to the absence of a root node, the routing update interval will be frequently reset to its minimum value (approximately 120 ms).

Figure 18. Four battery discharge curves for node 2150 (Site 2) representing normal and truncated battery life. The red line depicts the rapid depletion of battery power during a gateway outage (indicated between the two vertical dashed lines).



The shortened route update interval during gateway outages (in the case of the CTP-based application) causes the duty-cycle of the mote's radio to increase significantly, resulting in a dramatic waste of nodes' battery energy, especially for longer outages. An example of this situation is shown in Figure 18 where four battery discharge curves are overlaid for one of the relay nodes in Site 2 (*i.e.*, node 2150, see Figure 3). Three of the four discharge curves overlap representing consistent battery usage. The fourth line (shown in red) represents the battery discharge curve during a period when a gateway outage

occurred (indicated by the sharp decline between the two vertical dashed lines). In this case, the battery voltage had decreased to a near-depleted level by the time the gateway and the network were restored (approximately six days).

This problem compounds the issue of gateway outages where node battery life is unnecessarily depleted while no data packets are being collected. It is important to recognize this problem for network maintenance following a gateway outage. Short-interval power outages can be mitigated by means of uninterrupted power supply (UPS) connected to the gateway.

5.4.3. Internet Security

For the purposes of real-time monitoring of the WSN, remote access to the gateway is granted over the Internet. By allowing external (*i.e.*, outside the local network) Internet access, the gateway is exposed to the general public. While access to the gateway is protected by a username and password, unauthorized users may still attempt to access the system. In the first year of deployment, the WSN gateway received 175 unique unauthorized attempts at accessing the system and in just over two years there were over 700 unique recorded attempts.

The significant number of attempts from outside users presented an unexpected maintenance cost for the network. For the purposes of security, a record is kept of all the addresses of users who made an unwanted attempt to access our system. These records are used to maintain a blacklist to restrict system access from future attempts.

6. Conclusions

This study presents an analysis of our long-term outdoor WSN, with both commercially available and open source networking software for TinyOS-based WSN platforms. This work represents a novel effort for the empirical evaluation of multi-hop real-world environmental monitoring WSNs, focusing on network performance and network costs.

We observed that around 3%–4% of all the packets received at the gateway were duplicates when using XMesh, which indicate a significant number of unnecessary transmissions within the network. This issue is mostly resolved with the use of CTP, where the duplicate packet control is carried at the first transmission hop for each node, avoiding unnecessary transmissions towards the sink node. The network analysis shows that only 0.2% of the packets received using CTP corresponded to duplicates.

Based on the network statistics collected from the ASWP WSN testbed, a highly used path across the network was found in forwarding activities. For XMesh, nodes located closer to the base station created a bottle neck, responsible for most of the packet retransmissions and drops, reducing the network performance. In CTP, nodes along this highly used path are able to handle the network traffic load; however, these nodes consume more energy than their neighbors and network partitions may occur once their batteries are depleted.

Unexpectedly, it was found that nodes with relatively low path costs were associated with poor PSR under XMesh (especially for nodes close to the base station), which resulted in significant retransmissions and packet loss. In contrast, appropriate high transmission costs are assigned to these nodes in CTP, avoiding the unnecessary expenditure of power (due to retransmissions) and improving the success rate of packet reception at the base station.

PRRs at the node level also present important differences between the two analyzed deployment approaches. In XMesh, it was found that nodes deployed closer to the base station are able to maintain PRRs of 50% and above, only up to 61%, while nodes located farther from the base station obtain PRRs fluctuating between 15% and 40%. This behavior changed in CTP, where nodes located both close to and far from the base station could achieve PRRs higher than 90%. However, some specific node locations exhibit lower performance (*i.e.*, nodes 1070, 1080, 3025, 3085, 5043) throughout the deployment field. The PSR was included as an additional indicator of the network performance. When using XMesh, the entire network maintains a PSR between 45% and 53%, while PSR values range from 15% to 79% for individual nodes closer and in direct connection with the base station. These results are lower than those obtained with CTP, which achieved 96% PSR for a six-month period, evidencing critical differences between these two WSN routing protocols and their reaction to ASWP's outdoor conditions.

In summary, the analysis revealed numerous issues pertaining to the XMesh performance (and ultimately the increased maintenance) of the network, including the presence and transmission of duplicate packets, the presence of congestion along highly used paths, the utilization of under-performing nodes for packet forwarding, and network partitioning. For the CTP-based application, packet duplicates, poor forwarder selection, and congestion were no longer an issue; however, network partitioning remains. Network partitions may significantly reduce the network performance as nodes within the highly used path deplete their batteries resulting in entire sections of the WSN unable to reestablish a path towards the sink node. At the ASWP testbed, network partitions are mainly consequences of both maintenance related events (e.g., hardware failures, battery depletions) and the behavior of the routing protocol (the capacity of the protocol to recover the routes when possible. Handling network partitions in an automatic manner is still an open challenge for WSNs, since additional factors need to be considered such as reactive factors (e.g., computing alternative routes, using low quality links at higher costs, stopping data transmissions until feasible routes are available) or proactive factors (e.g., load balancing, topology management). In our WSN testbed, network partitions are handled by site maintenance visits.

The physical cost of the network is currently $31,500 (35 regular nodes with sensors, 17 relay nodes and one base station and gateway) and is deployed over five sites with nodes monitoring an area of 5000 square meters. The physical costs of the network are combined with the regular maintenance required for its upkeep (e.g., mote battery replacements, mote hardware replacements, and node relocations). While individual nodes have batteries replaced on average every 58 days, network visits for battery maintenance occur almost every 12 days. These values appear consistent with other reported studies [17,19]. The maintenance costs of these visits are high, averaging $187 per field visit (including the time, transportation, hardware, and power costs).

Our experimental evaluation of the ASWP testbed shows that long-term WSN deployments and operations have significant impact not only on the network performance, but also on network costs as battery depletions and hardware problems must be addressed as part of regular network maintenance. Further support from the protocol stack to the network performance and maintenance is needed for optimizing the overall network deployments and operations, which will be considered in the future work.

Acknowledgments

This work was supported in part by the U.S. National Science Foundation under CNS-0758372, CNS-1252066, CNS-1320132 and CNS-0721474, CNS-1251995, CNS-1319331 to IUPUI and the University of Pittsburgh, respectively.

The authors would like to thank colleagues (C.-M. Kuo, C. Duffy, D. Salas, and F. Plaza) and students (H. van Hemmen, E. Ferriss, A. Aouni, B. Quinn, T. Hare, B. McGlynn, and B. Ryu) who assisted in the development and deployment of the ASWP testbed.

We are also grateful to the ASWP (especially B. Shema and S. Detwiler) for the opportunity and support of this field research.

Author Contributions

M.N. led the development of the open source WSN application, conducted the analysis of the network performance, designed and performed experiments, and co-wrote the initial manuscript. T.W.D. led the deployment of the ASWP testbed and the development of the XMesh WSN application, designed and performed experiments, conducted the analysis of network costs, and co-wrote the initial manuscript. G.V. led the continued deployment of the ASWP testbed, designed and performed experiments, conducted the analysis of network costs, and co-wrote the initial manuscript. Y. Li and X.Z. performed experiments and contributed to the development of the open-source WSN application and configuration. N.E. led the development of the WSN gateway for the ASWP testbed, contributed to the development of the open-source WSN application, and designed experiments. X.L. and Y. Liang conceived the ASWP testbed, guided the network design, development, deployment, experiments, and analysis, and contributed to writing the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. *Comput. Netw.* **2002**, *38*, 393–422.
2. Dutta, P.; Hui, J.; Jeong, J.; Kim, S.; Sharp, C.; Taneja, J.; Tolle, G.; Whitehouse, K.; Culler, D. Trio: Enabling sustainable and scalable outdoor wireless sensor network deployments. In Proceedings of the 5th International Conference on Information Processing in Sensor Networks, Nashville, TN, USA, 19–21 April 2006; pp. 407–415.
3. Bapat, S.; Kulathumani, V.; Arora, A. Analyzing the yield of exscal, a large-scale wireless sensor network experiment. In Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP 2005), Boston, MA, USA, 6–9 November 2005; p. 10.
4. Wark, T.; Hu, W.; Corke, P.; Hodge, J.; Keto, A.; Mackey, B.; Foley, G.; Sikka, P.; Brunig, M. Springbrook: Challenges in developing a long-term, rainforest wireless sensor network. In Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2008), Sydney, Australia, 15–18 December 2008; pp. 599–604.

5. Ertin, E.; Arora, A.; Ramnath, R.; Naik, V.; Bapat, S.; Kulathumani, V.; Sridharan, M.; Zhang, H.; Cao, H.; Nesterenko, M. Kansei: A testbed for sensing at scale. In Proceedings of the 5th International Conference on Information Processing in Sensor Networks, Nashville, TN, USA, 19–21 April 2006; pp. 399–406.
6. Liu, Y.; He, Y.; Li, M.; Wang, J.; Liu, K.; Li, X. Does wireless sensor network scale? A measurement study on greenorbs. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 1983–1993.
7. Gnawali, O.; Guibas, L.; Levis, P. A case for evaluating sensor network protocols concurrently. In Proceedings of the 5th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, Chicago, IL, USA, 20–24 September 2010; pp. 47–54.
8. Puccinelli, D.; Gnawali, O.; Yoon, S.; Santini, S.; Colesanti, U.; Giordano, S.; Guibas, L. The impact of network topology on collection performance. In *Wireless Sensor Networks*; Springer: Bonn, Germany, 2011; pp. 17–32.
9. MEMSIC. Micaz, wireless measurement system. Available online: http://www.memsic.com/userfiles/files/Datasheets/WSN/6020-0060-04-B_MICAz.pdf (accessed on 27 November 2014).
10. Al-Karaki, J.N.; Kamal, A.E. Routing techniques in wireless sensor networks: A survey. *IEEE Wirel. Commun.* **2004**, *11*, 6–28.
11. Werner-Allen, G.; Swieskowski, P.; Welsh, M. Motelab: A wireless sensor network testbed. In Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, Los Angeles, CA, USA, 25–27 April 2005; p. 68.
12. Doddavenkatappa, M.; Chan, M.C.; Ananda, A.L. Indriya: A low-cost, 3D wireless sensor network testbed. In *Testbeds and Research Infrastructure. Development of Networks and Communities*; Springer: Shanghai, China, 2012; pp. 302–316.
13. Des Rosiers, C.B.; Chelius, G.; Fleury, E.; Fraboulet, A.; Gallais, A.; Mitton, N.; Noël, T. Senslab very large scale open wireless sensor network testbed. In Proceedings of the 7th International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCOM), Shanghai, China, 17–19 April 2011.
14. Lim, R.; Ferrari, F.; Zimmerling, M.; Walser, C.; Sommer, P.; Beutel, J. Flocklab: A testbed for distributed, synchronized tracing and profiling of wireless embedded systems. In Proceedings of the 12th International Conference on Information Processing in Sensor Networks, Philadelphia, PA, USA, 8–11 April 2013; pp. 153–166.
15. He, T.; Krishnamurthy, S.; Luo, L.; Yan, T.; Gu, L.; Stoleru, R.; Zhou, G.; Cao, Q.; Vicaire, P.; Stankovic, J.A. Vigilnet: An integrated sensor network system for energy-efficient surveillance. *ACM Trans. Sens. Netw. (TOSN)* **2006**, *2*, 1–38.
16. Kerkez, B.; Glaser, S.D.; Bales, R.C.; Meadows, M.W. Design and performance of a wireless sensor network for catchment-scale snow and soil moisture measurements. *Water Resour. Res.* **2012**, *48*, doi:10.1029/2011WR011214.
17. Tolle, G.; Polastre, J.; Szewczyk, R.; Culler, D.; Turner, N.; Tu, K.; Burgess, S.; Dawson, T.; Buonadonna, P.; Gay, D. A macroscope in the redwoods. In Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, San Diego, CA, USA, 2–4 November 2005; pp. 51–63.

18. Barrenetxea, G.; Ingelrest, F.; Schaefer, G.; Vetterli, M.; Couach, O.; Parlange, M. Sensorscope: Out-of-the-box environmental monitoring. In Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN'08), St. Louis, MI, USA, 22–24 April 2008; pp. 332–343.
19. Szewczyk, R.; Mainwaring, A.; Polastre, J.; Anderson, J.; Culler, D. An analysis of a large scale habitat monitoring application. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 3–5 November 2004; pp. 214–226.
20. Navarro, M.; Davis, T.W.; Liang, Y.; Liang, X. A study of long-term wsn deployment for environmental monitoring. In Proceedings of the 2013 IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London, UK, 8–11 September 2013; pp. 2093–2097.
21. NOAA National Climatic Data Center. Ranking of cities based on percentage annual possible sunshine. Available online: http://www1.ncdc.noaa.gov/pub/data/ccd-data/pctposrank.txt (accessed on 9 September 2014).
22. Northeast Regional Climate Center (NRCC). Percent possible sunshine. Available online: http://www.nrcc.cornell.edu/ccd/pctpos.html (accessed on 9 September 2014).
23. Cerpa, A.; Elson, J.; Estrin, D.; Girod, L.; Hamilton, M.; Zhao, J. Habitat monitoring: Application driver for wireless communications technology. *ACM SIGCOMM Comput. Commun. Rev.* **2001**, *31*, 20–41.
24. Liu, T.; Sadler, C.M.; Zhang, P.; Martonosi, M. Implementing software on resource-constrained mobile sensors: Experiences with impala and zebranet. In Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, Boston, MA, USA, 6–9 June 2004; pp. 256–269.
25. Arora, A.; Dutta, P.; Bapat, S.; Kulathumani, V.; Zhang, H.; Naik, V.; Mittal, V.; Cao, H.; Demirbas, M.; Gouda, M. A line in the sand: A wireless sensor network for target detection, classification, and tracking. *Comput. Netw.* **2004**, *46*, 605–634.
26. Trubilowicz, J.; Cai, K.; Weiler, M. Viability of motes for hydrological measurement. *Water Resour. Res.* **2009**, *45*, doi:10.1029/2008WR007046.
27. Peres, E.; Fernandes, M.A.; Morais, R.; Cunha, C.R.; López, J.A.; Matos, S.R.; Ferreira, P.; Reis, M. An autonomous intelligent gateway infrastructure for in-field processing in precision viticulture. *Comput. Electron. Agric.* **2011**, *78*, 176–187.
28. Musaloiu-e, R.; Terzis, A.; Szlavecz, K.; Szalay, A.; Cogan, J.; Gray, J. Life under your feet: A wireless soil ecology sensor network. In Proceedings of the 3rd Workshop on Embedded Networked Sensors (EmNets 2006), Cambridge, MA, USA, 30–31 May 2006.
29. Matese, A.; Vaccari, F.P.; Tomasi, D.; Di Gennaro, S.F.; Primicerio, J.; Sabatini, F.; Guidoni, S. Crossvit: Enhancing canopy monitoring management practices in viticulture. *Sensors* **2013**, *13*, 7652–7667.
30. Vellidis, G.; Tucker, M.; Perry, C.; Kvien, C.; Bednarz, C. A real-time wireless smart sensor array for scheduling irrigation. *Comput. Electron. Agric.* **2008**, *61*, 44–50.
31. Szewczyk, R.; Polastre, J.; Mainwaring, A.; Culler, D. Lessons from a sensor network expedition. In *Wireless Sensor Networks*; Springer: Berlin, Germany, 2004; pp. 307–322.

32. Moteiv Corporation. *Tmote sky: Low Power Wireless Sensor Module*; Technical Report, Moteiv Corporation: Redwood, CA, USA, June 2006.
33. MEMSIC. Mda300 data acquisition board. Available online: http://www.memsic.com/userfiles/files/Datasheets/WSN/6020-0052-04_a_mda300-t.pdf (accessed on 27 November 2014).
34. MEMSIC. Iris, wireless measurement system. Available online: http://www.memsic.com/userfiles/files/Datasheets/WSN/6020-0124-01_B_IRIS.pdf (accessed on 27 November 2014).
35. Navarro, M.; Li, Y.; Liang, Y. Energy profile for environmental monitoring wireless sensor networks. In Proceedings of the 2014 IEEE Colombian Conference on Communications and Computing (COLCOM), Bogotá, Columbia, 4–6 June 2014; pp. 1–6.
36. Stajano, F.; Cvrcek, D.; Lewis, M. Steel, cast iron and concrete: Security engineering for real world wireless sensor networks. In *Applied Cryptography and Network Security*; Springer: Berlin, Germany, 2008; pp. 460–478.
37. Davis, T.W.; Liang, X.; Navarro, M.; Bhatnagar, D.; Liang, Y. An experimental study of wsn power efficiency: Micaz networks with xmesh. *Int. J. Dis. Sens. Netw.* **2012**, *2012*, doi:10.1155/2012/358238.
38. Navarro, M.; Bhatnagar, D.; Liang, Y. An integrated network and data management system for heterogeneous wsns. In Proceedings of the 2011 IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS), Valencia, Spain, 17–22 October 2011; pp. 819–824.
39. MEMSIC. Xmesh user manual. Revision A. Available online: http://www.memsic.com/userfiles/files/User-Manuals/xmesh-user-manual-7430-0108-02_a-t.pdf (accessed on 27 November 2014).
40. MEMSIC. Moteview user manual. Revision D. Available online: http://www.memsic.com/userfiles/files/User-Manuals/moteview-users-manual.pdf (accessed on 27 November 2014).
41. Gnawali, O.; Fonseca, R.; Jamieson, K.; Moss, D.; Levis, P. Collection tree protocol. In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, Berkeley, CA, USA, 4–6 November 2009; pp. 1–14.
42. Gnawali, O.; Fonseca, R.; Jamieson, K.; Kazandjieva, M.; Moss, D.; Levis, P. Ctp: An efficient, robust, and reliable collection tree protocol for wireless sensor networks. *ACM Trans. Sens. Netw. (TOSN)* **2013**, *10*, doi: 10.1145/2529988.
43. Ganti, R.K.; Jayachandran, P.; Luo, H.; Abdelzaher, T.F. Datalink streaming in wireless sensor networks. In Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, Boulder, CO, USA, 31 October–3 November 2006; pp. 209–222.