Experiences from building an Outdoor Testbed for Community Wireless Networks

Bart Braem, Chris Blondia and Steven Latré
iMinds – University of Antwerp – MOSAIC Research Group
{bart.braem, chris.blondia, steven.latre}@uantwerpen.be

Abstract—**Community Wireless Networks are an emerging networking model, offering people the opportunity to build and manage their own network without being dependent on telecom operators. The strength of this type of networks lies in the involvement of the whole community, as each person benefitting from the community wireless network somehow contributes to the design, deployment and maintenance of the network. This model has resulted in large community wireless networks growing all over the world, connecting people in the local communities to each other and the Internet. Because of the rising popularity and demonstrated success, researchers are also becoming more interested in community networks. This paper presents guidelines and experiences from creating an outdoor testbed targeted at community wireless networks, based on experience and feedback from community network members.**

I. INTRODUCTION

In many regions of the world, getting Internet access is complex due to a variety of reasons. Economical, political and geographical conditions may influence the willingness or possibility of Internet providers to connect a particular location. Being connected to the Internet may not be the biggest concern however; just being connected with other members of the local community can introduce enough benefits to justify the investment. Community Wireless Networks (CWNs) offer a solution to these use cases. They are not owned, deployed or maintained by a single corporation, but by a larger community of individuals who contribute financially (by buying equipment), logistically (by providing locations to place the equipment) or technically (by installing and maintaining the equipment and overall network).

The European FP7 project CONFINE [1] studies and promotes test environments targeted at CWNs. Within the project both large-scale and smaller-scale testbeds are built and interconnected to allow researchers and community network members to perform network experiments Everything is integrated in the Community-Lab platform, which offers intuitive control over the infrastructure.

This paper presents an overview of some good practices and useful tips on how to prepare and execute the deployment of an outdoor CWN testbed. The described techniques are based on experience collected during the deployment of a CONFINE testbed extension at the University of Antwerp in Belgium, based on feedback and suggestions from the local community network Wireless België, currently consisting of six indoor and six outdoor nodes[1]. In what follows we will refer to this with the more generic term "testbed".

In literature, there is plenty of evidence to support the use of testbeds to validate research results in more realistic environments. Langdoen et al. [2] is a perfect illustration of the difference between simulation studies and outdoor networks (in this case sensor networks). In Tan et al. [3] the authors find similar discrepancies, with more recent wireless hardware. Raychaudhuri et al. [4] and Soroush et al. [5] describe outdoor wireless testbeds, not focused on community networks. The key difference lies in the hardware and the node structure, in a community networks a node typically consists of multiple antennas and a router, see section II. In ORBIT and DOME the wireless nodes do not consist of separate router hardware. This convergence of multiple technologies (independent wireless antennas and advanced routing) correlates to the trend described by Blywis et al. [6]. Ishmael et al. describe the deployment of a community network serving a local village [7], based on older hardware with IEEE 802.11b interfaces. A similar article by Allen et. al. also stems from a previous wireless hardware generation [8]. This work considers more recent hardware used in community networks around the world.

The main contribution from this work is practical, hands-on information on building an outdoor testbed for CWNs research, based on knowledge from CWN members. It documents good practices to allow replication of such a testbed in other locations, while avoiding pitfalls commonly known in the CWNs community.

II. TESTBED NODES

In Figure 1, node B of our testbed is depicted. Two Nanostation loco M5 (the two small enclosures at the top) and a GentleBox JE-300 (the large enclosure) can be seen on the mounting pole. Coming from the indoor power supply, there is one Power over Ethernet (PoE) cable entering the GentleBox to provide power and to connect to the control network. Two cables exit the enclosure to provide power and connectivity to the two antennas. A copper wire behind the components conducts lightning impacts to the ground. It is attached to the mounting pole base and to the lightning protection of the building. Four concrete tiles hold the mounting pole upright during windy weather conditions.

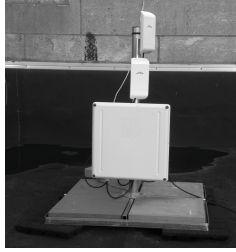[1]See http://wiki.confine-project.eu/testbeds:belgium for more pictures and configuration information.

Fig. 1. A typical node layout, consisting of a central unit and two Nanostation loco M5's

Fig. 2. Plug to be used with cable ties. Source: http://www.frequencydistribution.co.uk

Component	Voltage		Power
	Min (V)	Max (V)	Max (W)
Nanostation loco M5	24	24	5.5
rocket M	24	24	6.5
RouterBOARD 450	14	28	6.5
alix3d2 (board only)	7	20	5

TABLE I. OVERVIEW OF MINIMUM AND MAXIMUM OPERATING VOLTAGE LEVELS AND MAXIMUM POWER CONSUMPTION

Three challenges have to be tackled do deploy a single node, as described below.

An important task in creating a CWN testbed is the correct choice of hardware. In most cases, a single CWN node will be composed of the following components: at least one wireless interface with an antenna, a routing device to connect all individual components, a low-power computer or embedded system used as a local controller for the experiment execution and a power supply.

In Avonts et al. [9], the authors describe results from a questionnaire on different community networks properties. One of the aspects covered by the questionnaire is the hardware used in each of the different CWNs around the world. As this questionnaire indicated many CWNs use hardware from Mikrotik[2] or Ubiquity Networks (UBNT)[3], or OpenWRT compatible hardware. Based on feedback from the local CWN Wireless België, we used the following components for the nodes in the testbed: a airectional UBNT Nanostation loco M5 antennas and omni-directional UBNT rocket M antennas, Mikrotik RouterBOARD 450 routers for outdoor nodes and Mikrotik RouterBOARD 951-2n for indoor nodes and finally aa PC Engines alix3d2 provisioned with two Wistron DNMA92 wireless cards

Indoor equipment can easily be assembled, outdoor nodes however are more challenging. Although the enclosure of the UBNT devices is weather proof, the other components are not and thus have to be installed in a weather proof enclosure. Multiple options are available. Based on feedback from the local CWN, the GentleBOX JE-300 from Jirous[4] was chosen because of its size, flexibility and easy mounting options.

The main challenge with the outdoor nodes is powering all devices, as it is cumbersome to draw both network and (multiple) power cables to each of the outdoor nodes while keeping a flexible setup where components can easily be added or removed. Widely available in low-cost devices used in community wireless networks, passive PoE was chosen to power the testbed. However, before all components can be connected to this power feed, power distribution among the

components in a single node, voltage levels of components in a single node and the power supply itself have to be considered.

Whether the power distribution is a real issue depends on the selected routing hardware. Some routing platforms can power equipment connected to their network ports via PoE. Other routing platforms do not pass the power on their other network ports. For the latter, a passive PoE distribution panel has to be installed inside the node or the routing hardware has to be modified. The two routing boards selected for our testbed can both be modified to enable PoE passthrough on the LAN ports. The RouterBOARD 951-2n was built using non-magnetic RJ45 connectors. The modification of this board therefore consists of connecting pins four and five, respectively seven and eight with each other on each RJ45 connector. When doing the same for the fourth pair, the negative feed is distributed among all ports as well. The RouterBOARD 450 uses magnetic RJ45 connectors, with pair one available on pin four and pair four on pin five. The actual modification therefore consists of connecting all pin fours respectively pin fives from the different connectors.

As it is now possible to power all components via a single PoE feed, a verification whether all individual components operate at the same voltage is needed. Table I lists the operational voltage level of each individual component used in the testbed, as defined by the device vendors. As can be seen, all components can operate safely at 24V, except the alix3d2. The adopted approach in this case consists of feeding each node with 24V and lowering this specifically for the alix3d2. We illustrate this with the selected components, different components will require a similar approach. A transistor cannot be used to bring the voltage level down, as the voltage drop would vary with the load. A better way to reach a safe voltage level to power the alix3d2 is by placing Zener diodes between the global feed and the power lines to the alix3d2. Two parameters are important for the selection of the Zener diodes: the targeted voltage drop (in this case 6V) and the maximum amount of heat generated by the diodes. A Zener diode converts electrical energy into heat, which it needs to dissipate. Therefore a Zener diode which is safe to operate at the maximum expected current passing the diode has to be selected. This maximum can be calculated by looking at the maximum load behind the Zener diode (9.8W in this case), the power consumption of the Alix and its wireless cards. The current through the Zener diode equals 0.54A ($P = U \times I$ with $U = 24V - 6V = 18V$ and $P = 9.8W$), which brings the total dissipated power to 2.7W ($P = U \times I = 5V \times 0.54A$). For the example,

[2]Mikrotik routers: http://www.mikrotik.com/

[3]Ubiquiti networks: http://www.ubnt.com/

[4]http://en.jirous.com/Accessories-complements/je-300

the 1N5340B Zener diode from ON Semiconductor[5] was selected. This diode has a reverse Zener voltage of 6.0V $\pm$ 0.3V and can dissipate up to 5W at 25°C. However, its capability to dissipate heat derates with 40mW/°C above 25°C. Because the testbed nodes are located on a roof in plain sunlight, temperatures of 55°C and above must be taken into account. Therefore two Zener diodes in parallel were included. This will divide the total dissipated power of 2.7W by two.

The configuration described above allows building a fully operational CWN testbed node. As some of the testbed nodes are located outside, the maintenance procedures should also be optimized. To do so, two components can be easily added: basic environmental monitoring and a serial connection between the routing platform and test controller.

The most critical and error-prone component of the testbed node is the controller platform, in this case the ALIX board, as this system actively takes part in the experiments executed on the testbed and might become unreachable. As a consequence, there is a need for an alternative to the wired connection, in this case a serial console. Both the alix3d2 and the RouterBOARD 450 have a serial connection available, which can be connected. However, both the alix3d2 and RouterBOARD 450 are by default configured to act as a serial client. To correct this issue, the console output of the routing device has to be disabled.

The second optimization consists of some basic environmental monitoring, as suggested by the local CWN. Because the alix3d2 has native support for the I²C protocol, an I²C enabled digital temperature sensor such as the LM75A[6] can easily be connected to this board to monitor the temperature.

III. PRACTICAL INSTALLATION GUIDELINES

Compared to indoor nodes, outdoor nodes are more vulnerable to environmental conditions.This section provides suggestions about specific topics that deserve extra attention during the outdoor deployment, to mitigate these threats.

Of course care should be taken to use materials and equipment rated for outdoor usage. This holds both for the wireless equipment, enclosures and network cable and for the mounting poles, screws, cable-ties etc. Outdoor rated equipment not only guarantees water sealed enclosures, it is also more resistant to degradation caused by UV and oxidation. To this end, the CWN members suggested to cover screw and bolt connections with a metal primer, preventing small cracks from becoming a source of oxidation. The use of outdoor-rated components however still requires attention to the equipment suffering any damage from harsh environmental conditions. Special attention should be given to humidity, lightning and windy conditions.

By selecting a well-suited enclosure and using weatherproof cable glands, direct water penetration is avoided. Due to temperature differences between the inside and outside of the enclosure condensation will happen. So, it is important to select an enclosure which is rated for outdoor usage and also designed for housing electronic equipment. These enclosures contain a small outlet at the bottom to let the condensed water out. To keep the node safe, regular checks whether the condensation outlet is still free and not covered by dust, snow or ice are required.

Lightning can damage the installation, either by direct strike or by induced current. When lightning strikes near a node, the area around the impact becomes electrically charged. Due to this induced charge, currents start flowing to drain the differences in electrical potential away. Due to their electrical characteristics, these currents often happen to take place inside electrical cables (including network cables).

To prevent the lightning current from reaching the central power distribution, lightning protectors must be installed directly behind the power distribution. Lightning protectors can be found in two categories, those only protecting from lightning and those offering protection from lightning arrests and surges. In most cases, the former is built using Gas Discharge Tubes (GDTs). The latter contains additional electronic components which react more quickly to a sudden rise in voltage levels, offering better protection. The problem however is that these components have typically more constraints on the load they can handle. In our deployment, lightning and surge protection units were initially installed. During indoor testing all individual components worked fine. Once installed outdoor however the arrestors were reaching temperatures of over 80°C. It turned out that this was caused by the additional UTP cable length used in the outdoor setup (ten times longer than in the indoor tests). This introduced more power loss due to the increased electrical resistance, leading to more current which caused the surge arrestors to start heating to extreme temperatures. So when using both lightning and surge protection, the maximum load the arrestor must withstand should always be calculated.

Strong wind may cause a node to shift or fall, when it is not fixed sufficiently. Precisely calculating the wind force applied to a node is hard, we give an estimation. The force generated by wind on an object is given by formula 1 [10].

$$F = \frac{1}{2}\rho \times c_d \times A \times v^2 \tag{1}$$

F is the force of the wind, ρ the density of the medium (air), c_d the drag coefficient, A the exposed cross-section normal to the wind direction and v the wind velocity. The worst-case value of the drag coefficient of a cube equals 1.05, for a flat plate this is 1.40 to 2.05 depending on its relative size [11]. In this case, 1.40 is a good approximation of the situation. Now the exact wind conditions a node should withstand can be derived. As an example, consider the wind force on the Gentlebox for wind speeds of 110km/h (30.6m/s). This enclosure measures 326mm $\times$ 326mm $\times$ 90mm so the maximum exposed cross section is $(0.326m)^2 = 0.106m^2$. The air density equals $1.23\frac{kg}{m^3}$. Substituting these values in equation 1, the total wind force equals $F_{je-300} = \frac{1}{2}1.23\frac{kg}{m^3} \times 1.40 \times 0.106m^2 \times (30.6\frac{m}{s})^2 = 85.5N$.
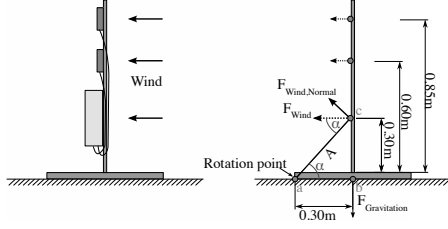
Fig. 3. Schematic overview of the forces impacting a node.

This wind force value can now be used to calculate the moment around the base point of the mounting stand, to determine the contra weight needed to keep the node in place during high wind speeds. Figure 3 shows the different forces on a node. On the left side, a typical node layout is displayed. In a worst case scenario the wind blows perpendicular on the back of the devices. To prevent the node from tilting, the moment caused by the gravitational force should be greater than the sum of the moments caused by the wind force on the devices on the pole.

As an example, consider the calculation of the moment on the central unit M_{je-300}. It is calculated by multiplying the length of the lever arm A and the value of the applied force normal to this lever arm, $F_{Wind,Normal}$.

$$\begin{aligned} M_{je-300} &= |A| \times |F_{Wind,Normal}| \\ &= |A| \times |F_{Wind}| \times sin(\alpha) \\ &= |ac| \times |F_{Wind}| \times \frac{|bc|}{|ac|} \\ &= 25.65 Nm \end{aligned}$$

To compensate for this value, the gravitational force F_G must be greater than $85.5N$. Indeed, The torque M_G caused by the gravitational force F_G can be written as $M_G = |ab| \times |F_G|$. So to counter the wind effect on the central unit alone, a weight of $8.72kg$ has to be placed equally distributed on the base stand as $F_G = g \times w$ with w being the mass of the counter weight and $g = 9.81\frac{m}{s^2}$.

The testbed equipment can also cause damage to its surroundings such as rooftops or walls. To minimize these risks, the location should be carefully prospected before the actual installation, paying special attention to minimize impact on the surroundings. In our testbed two additional tricks limit impact of these hazards. First, cables are prevented from obstructing pathways. As recommended by the local CWN, special plugs designed for use in combination with cable-ties (as shown in figure 2) are used to fix cables. Push the plug in a hole drilled in a simple brick and use cable-ties to secure the cables. Under normal circumstances, using one such brick every three meters should be sufficient to safely guide a UTP cable between the power distribution panel and a node. Damage to the roof is prevented by using non-penetrating base stands designed for satellite dishes. These can easily be moved, making it possible to adapt the configuration of the testbed. Rubber mats underneath the edges of the base stand prevent damage to the roof.

IV. Conclusion

This paper outlined steps taken and the underlying motivation when building an outdoor testbed for CWNs. Special attention was given to the selection of hardware and the technology powering the nodes. In addition some practical safe deployment guidelines were given.

During the installation of our testbed, we felt that there was a lack of documentation covering practical guidelines to deploy an outdoor testbed. After talking to the local CWN, we were able to compose this list of guidelines. Depending on the location, environmental conditions and previous experience, community members and researchers should adapt the mechanisms. In true CWN spirit, we encourage them to share their experiences with the deployment of CWNs or testbeds targeted at these network types.

References

[1] B. Braem, C. Blondia, C. Barz, H. Rogge, F. Freitag, and L. Navarro, "A case for research with and on community networks," *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 3, pp. 68–73, jul 2013.

[2] K. Langendoen, A. Baggio, and O. Visser, "Murphy loves potatoes: Experiences from a pilot sensor network deployment in precision agriculture," in *Proceedings of the 20th International Conference on Parallel and Distributed Processing*, ser. IPDPS'06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 174–174.

[3] K. Tan, D. Wu, A. J. Chan, and P. Mohapatra, "Comparing simulation tools and experimental testbeds for wireless mesh networks," *Pervasive and Mobile Computing*, vol. 7, no. 4, pp. 434 – 448, 2011.

[4] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, and M. Singh, "Overview of the orbit radio grid testbed for evaluation of next-generation wireless network protocols," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 3. IEEE, 2005, pp. 1664–1669.

[5] H. Soroush, N. Banerjee, A. Balasubramanian, M. D. Corner, B. N. Levine, and B. Lynn, "Dome: A diverse outdoor mobile testbed," in *Proceedings of the 1st ACM International Workshop on Hot Topics of Planet-Scale Mobility Measurements*, ser. HotPlanet '09. New York, NY, USA: ACM, 2009, pp. 2:1–2:6.

[6] B. Blywis, M. Guenes, F. Juraschek, and J. Schiller, "Trends, advances, and challenges in testbed-based wireless mesh network research," *Mobile Networks and Applications*, vol. 15, no. 3, 2010.

[7] J. Ishmael, S. Bury, D. Pezaros, and N. Race, "Deploying rural community wireless mesh networks," *Internet Computing, IEEE*, vol. 12, no. 4, pp. 22–29, 2008.

[8] W. Allen, A. Martin, and A. Rangarajan, "Designing and deploying a rural ad-hoc community mesh network testbed," in *Proceedings of the The IEEE Conference on Local Computer Networks 30th Anniversary*, ser. LCN '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 740–743.

[9] J. Avonts, B. Braem, and C. Blondia, "A questionnaire based examination of community networks," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, no. 8. IEEE, oct 2013, pp. 8–15.

[10] R. Blevins, *Applied Fluid Dynamics*. Krieger Publishing, 2003.

[11] S. M., *Aircraft Performance Analysis*. VDM Verlag, 2009.