An Experimental Evaluation of Network Reliability in a Secure Internet of Things Deployment

Elias Z. Tragos
Insight Centre for Data Analytics,
NUI Galway and FORTH-ICS
elias.tragos@insight-centre.org

Antonio Lignan
Relayr GmbH
antonio.lignan@relayr.io

Alexandros Fragkiadakis
FORTH-ICS
alfrag@ics.forth.gr

Marc Fabregas
Zolertia
mfabregas@zolertia.com

Abstract

The technological advances of the Internet of Things (IoT) have matured enough the last few years and real-world deployments in smart city and building environments have emerged. The IoT promises significant improvements in the everyday life of people, but its performance in real deployments has not been studied thoroughly, especially due to the fact that IoT devices, although constrained, are supposed to provide multiple concurrent services. This raises concerns for the performance of the IoT network, especially since IoT devices are mostly constrained and sensor networks cannot support high traffic. Additionally, when IoT devices are equipped with extra security mechanisms, their network performance might be downgraded, because the secure data transmissions require extra signalling, such as for encryption or integrity protection. This work discusses the network reliability of real IoT deployments, taking as example a deployment in Heraklion, Greece. The evaluation results follows also a discussion section with lessons learned.

Categories and Subject Descriptors

C.2.5 [**Computer Systems Organisation**]: Computer-Communication Networks—*Local and Wide-Area Networks*; B.8.1 [**Hardware**]: Performance and reliability—*Reliability, Testing and Fault-Tolerance*

General Terms

Performance, Reliability, Security, Experimentation

Keywords

Internet of Things, Smart Cities, Network reliability, Secure deployment

International Conference on Embedded Wireless Systems and Networks (EWSN) 2018
14–16 February, Madrid, Spain

ISBN: 978-0-9949886-2-1

1 Introduction

More than 60% of the earth population will be living in cities by the year 2025 and there will be more than 30 cities with population above 10 million people. The increasing number of people living in urban areas has called for radical changes in the way that cities are organised and the type of services they provide to their citizens [9]. Smart cities have emerged as a promising concept for providing advanced public services, improving among others the quality of life of citizens. The Information and Communication Technologies (ICT) and especially the Internet of Things (IoT) are considered as the main drivers for boosting the deployment and provisioning of smart city applications and services.

In the last decade, the developments in the IoT domain have become very mature and this facilitated the installation of IoT systems in many cities around the world. Within Europe, smart city deployments exist nowadays in many cities, for example in Santander [11], Amsterdam [4], Barcelona [3], London, Copenhagen, etc[1]. These deployments are realized with the installation of hundreds or thousands of sensors in outdoor and indoor environments, enabling the provision of various applications: environmental monitoring, building energy consumption, indoor comfort quality monitoring, traffic and waste management.

The deployment of sensors in city areas is not a trivial thing. Both in indoor and outdoor city areas, installations of WiFi access points are very common for providing free Internet access to the citizens. In smart city deployments, installed sensors should coexist with WiFi access points in a harmonized way for providing applications of a standard quality. However, as it has been proved in the literature, when there is coexistence of IEEE 802.15.4 and IEEE 802.11, the performance of IEEE 802.15.4 degrades severely. This can cause significant increase in the packet losses due to interference [13, 6, 17]. Hence, it is evident that the existence of WiFi access points must be taken into account when deploying sensors and gateways in municipal areas. Additionally, the existence of buildings and walls is also affecting the performance of wireless networks, because

[1] https://www.fastcompany.com/3024721/the-10-smartest-cities-in-europe

the signal degrades as it passes through concrete walls.

In this work, we describe the experience with respect to network reliability of IoT smart city installations, by providing and analysing link quality measurements in a secure IoT deployment in the city of Heraklion in Greece that was built through RERUM [16]. The measurements were gathered during extended experiments performed in the evaluation of the RERUM project and used within WiVi-2020 [2] for assessing the interference between IoT devices. The structure of the paper is as follows: Section 2 provides a brief overview of the experimental testbed deployed in the city of Heraklion and used for the evaluation of the network reliability. Section 3 provides the background on the link quality indicators and the method followed for the evaluation. Section 4 provides the measurements and the analysis of the network reliability, as well as the availability and timeliness of the devices. Section 5 provides a discussion and best practices.

2 Heraklion Smart City Deployment

2.1 Deployment Description

As part of the activities of EU projects, we have installed and deployed a smart city IoT-based testbed in the city of Heraklion, Greece. The IoT system targeted initially four main applications, in outdoor and indoor deployments: (i) indoor applications for building energy monitoring and for comfort quality monitoring and (ii) outdoor applications for environmental monitoring and traffic management.

The basic physical components of the IoT deployment are: (i) the IoT Devices, (ii) the IoT Gateways, (iii) the Application Server, (iv) the Security Center and (v) the IoT Middleware. All deployments were connected to the same secure IoT middleware, which was developed within RERUM [8] as an extension of the OpenIoT middleware [15]. For the rest of this work, we consider only the devices and the gateways, since the focus is on evaluating the network reliability of the deployments. The measurements were gathered by the devices and extracted by log files on the gateways. However, since the network measurements were exposed as services by the middleware, one could also get the measurements directly from the middleware.

The deployment includes several indoor and outdoor devices that are exposing services, sending data to the middleware through the RERUM gateways. The devices used in the deployments were based on the Zolertia RE-Mote device [3]. The RE-Mote is based on the CC2538 ARM Cortex-M3 system on chip with an onboard IEEE 802.15.4 2.4GHz interface, but is also capable to use the subGHz bands at 868MHz for long distance communications with the CC1200 chip that also has onboard. The RE-Mote has 32KB of RAM nd low energy consumption. For the RERUM system the software was built based on the Contiki Operating System [5].

Due to the different nature of the physical environments in indoor and outdoor communications, and to avoid interference between the gateways, different frequencies and protocols were used. For the indoor communications, the devices use the channel 26 at the 2.4GHz band of the IEEE 802.15.4, while the outdoor devices are configured to use the subGHz band at the 868MHz, to ensure the communication at longer distances. The use of subGHz in the indoor deployments is avoided because of the concerns of the employees of the municipality although it would possibly have better network performance. Moreover, the devices use 6LoWPAN and RPL for routing. The route between the devices and the gateways is being handled by the RPL and it is not always single-hop. For some devices, the route changes over time according to the traffic and the interference. The use of RPL and not static routes was intentional in order to have better performance and avoid dropped links.

The gateways are developed integrating a RaspberryPi [4] and a RE-Mote in order to be able to interconnect the devices to the middleware servers. We remind here that the devices are using IPv6, while the middleware is using IPv4, so network and protocol translation were developed to allow the devices to "talk" to the middleware and the applications. Additionally, the devices are using CoAP to expose resources and services. The middleware sends CoAP [12] OBSERVE requests to get subscribe and get the measurements from the devices. At the gateways, the CoAP californium is used for allowing the communication with the devices using CoAP. The devices have multiple sensors on board, so they are exposing many services occupying a lot of RAM. The RE-Mote has 16KB of RAM retention, which was not enough for exposing all the services that the devices provide, thus radio duty cycling was disabled for allowing the usage of the whole 32KB of RAM.

2.2 Security Impact on Communications

The target of the deployment was to build a smart city IoT system based on the concepts of security, privacy and reliability by design. As a result, there are various security and privacy mechanisms that are employed in the deployment: (i) data minimization on the devices, (ii) DTLS-based communications, (iii) encryption based on Compressive Sensing (CS), (iv) integrity protection based on digital signatures, etc. Although these mechanisms improve the system security, they also affect its performance as shown in [1] because they increase the signaling and the packet sizes. This affects the wireless traffic, which normally has an impact on the network reliability.

As described in [10], there is significant communication overhead added due to the security mechanisms that are embedded on the IoT devices. As measured in these laboratory tests, the Integrity Protection mechanism more than doubles the packet size, with an increase of 171% in the packet size, due to the fact that every packet should carry apart from the actual measurement the signed measurement, which is a much longer string. Similarly, as described in [7], DTLS has an increas of on average 21 bytes per packet, so here with a packet size of 46 bytes, the increase is approximately 45%.

As described in [1], compressive sensing reduces the communication signaling significantly, even by 50% depending on the measurement type, but in this deployment, only a couple of devices were using compressive sensing and only for temperature and humidity, so CS did not have a significant impact on the communications. Finally, it is important

[2] http://wivi-2020.eu

[3] https://zolertia.io/product/re-mote-suite/

[4] https://www.raspberrypi.org/products/raspberry-pi-2-model-b/

to notice that a self-monitoring mechanism was also running on the network, gathering network statistics from the deployed devices every 30 seconds. This creates additional traffic in the network and increases the communication overhead for more than 25% as shown in [10].

From the above, it is obvious that the usage of security mechanisms on the network has a significant impact on the communications, increasing the signalling. The goal of the experiments is to see how much these security mechanisms and the overall deployment affect the network reliability.

3 Network Reliability Indicators

According to [14], network reliability is the ability of a network to perform a designated set of functions under certain conditions and for specified operational times. Reliability is different than availability, which is considered as the ability of a network to perform its functions at any time under certain conditions. Basically, availability is normally a metric used to measure the percentage of time that a network is functioning according to some standards and usually is measured (among others) with the uptime. However, we can say that reliability supersedes the availability and measures also the "quality" of the network.

In this work, we focus on measuring and evaluating the reliability of the wireless links of the smart city deployment, both indoor and outdoor, giving also measurements with respect to the availability and timeliness of the devices.

The link quality can be measured taking into account metrics already available at the wireless interfaces. Normally in sensor networks, the link quality is measured by the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI). RSSI is a common measurement of the link strength and basically is the logarithm of the received signal measured at each packet arriving at the device. LQI depends on the radio transceiver modulation process and is also measured at each packet. Both values are available in Contiki and have been exposed through a COAP resource. RSSI and LQI provide significant information about a given link between two communicating devices and basically the next hop to the gateway [2].

The RSSI value is given by the formula (1) using the Friis free space path loss model. It depends on factors like the distance between devices, the gain of the antennas used by the devices, and the transmission power. A RSSI value close to the receivers sensitivity typically indicates a link susceptible to break down and may be the cause of messages being lost, provoking the network healing processes to be triggered often thus also increasing network traffic and congestion.

$$RSSI = 10 * log(P_{RX}/P_{ref}) \quad (1)$$

where

$$P_{RX} = P_{TX} * G_{RX} * P_{TX} * (\frac{\lambda}{4\pi d})^2 \quad (2)$$

and P_{ref} is the received power of a reference signal.

Table 1 shows the sensitivity of both transceivers onboard the RE-Mote platform. A first approximation to assert a wireless link is to estimate the available link budget, given by the sensitivity of the radio and the transmission power in general (considering the radio transceiver output power and antennas used). Notice that the antenna gain value given in Table 1 is the worst-case scenario, and there is room for improvement if using antennas with higher gain.

Table 1. RE-Mote's radio transceivers and link budget

Radio Transceiver	Sensitivity	TX power	Antenna gain	Link budget
CC2538 (2.4GHz)	-97dBm	7dBm	5dBi	109dB
CC1200 (868MHz)	-109dBm	12dBm	-2dBi	119dB

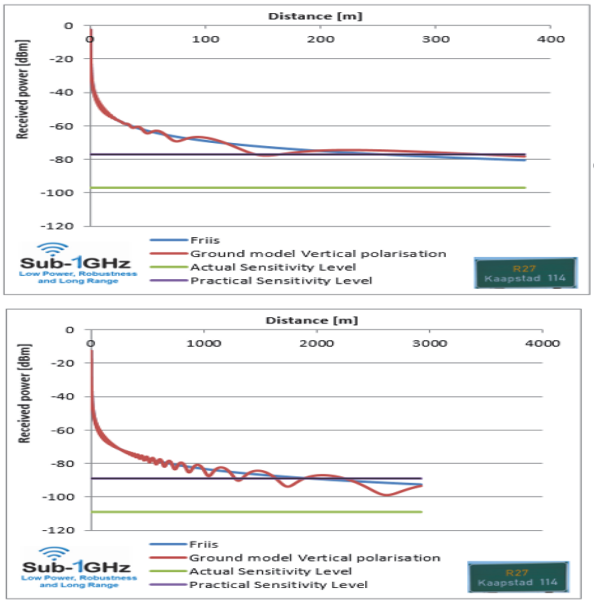

Figure 1. Link budget and Range expectations for (a) 2.4GHz and (b) 868MHz deployments

These values were used in the Texas Instruments range calculator [5] to obtain a practical approximation of the maximum expected range. As shown in Figure 1 , the maximum expected range (without any obstacles and plain line of sight) is about 1.8Km for sub-GHz links and 251mt for devices in the 2.4 GHz band. These results provide a rough estimation on how far the devices may be deployed, and how much margin for external factors like obstacles do we have.

On the contrary with RSSI that is calculated regardless of the interface, the LQI value is specific to the radio transceiver. In both radio interfaces used by the RE-Mote, the LQI indicates how well the signal is demodulated on the receiver side, thus indicating whether the link may be affected by phenomena like interference due to noise or other devices in the network.

In the case of the CC2538 2.4GHz radio transceiver, a correlation value of approximately 110 indicates a maximum-quality frame, whereas a value of approximately 50 is typically the lowest-quality frame detectable by the radio. For

[5] https://e2e.ti.com/support/wireless_connectivity/proprietary_sub_1_ghz_simpliciti/f/156/t/375556

the CC1200 sub-GHz radio the LQI value ranges from 0 to 10, where zero reflects a packet being cleanly demodulated.

The RSSI and LQI provide metrics to evaluate how good the wireless links are, taking into account any problems caused by static obstacles (buildings, trees), or derived from bad installation (antenna orientation or disconnection). The RSSI also determines whether there is enough margin to mitigate the effect of random events such as rain or traffic. Lastly, the RSSI and LQI may be further used to assert whether the network statistics indicators such as packet drops and CRC may be derived from the link conditions.

Apart from RSSI and LQI, the network and link-layer statistics can also be used as metrics to evaluate the reliability of a wireless link. These statistics allow quantizing the required effort to maintain the network topology and to ensure end-to-end communication between the devices and the server. The monitored values are:

- IP packets sent and received
- Received packets with bad CRC
- Failed transmission attempts due to channel congestion.

The network statistic values are gathered by the RPL and link layer modules of Contiki and are exposed through COAP resources. The "uptime" value is also used to accumulate the network statistics values in cases the device has been restarted. The obtained values are then to be correlated to the link quality indicators, to provide a better insight on the devices availability in terms of reliable wireless links.

4 Evaluation of Network Reliability

Figure 2 shows the topology of the indoor deployment. The outdoor devices are deployed in two locations and are around the central square of the city in short distances but with buildings between them and the gateway. The indoor devices are deployed in the same area and they span in two adjacent buildings. The devices send continuously multiple measurements (temperature, humidity, noise, light, weather, gases, etc.) with different periods between 30s and 2 min.

4.1 Outdoor Deployment Network Reliability

The link quality measurements of the outdoor devices are shown in Table 2. The devices use the sub-GHz radio interface with a multiband antenna, and the obtained results are within the RSSI and LQI margins (the deviation is shown in the "RSSI dev" and "LQI dev" columns). The table does not show the link layer errors due to bugs in the CC1200 library. We have to remind here that the RSSI is measured per hop and not between the device and the gateway. Thus, for a multihop link (like the E03) the RSSI measures the signal strength between E05 and E03.

As shown in the table, the RSSI minimum observed value is in most cases on average more than 30dB higher than the transceiver sensitivity, allowing the mitigation of the signal degradation in cases of obstacles and others disturbances. In the worst case of E05 and E07, the lowest RSSI is measured at -93dB, which is still 16dB higher than the sensitivity. At a closer look, the device L02 in the Lions Square scenario is the farthest located with respect to the gateway (100 metres) with two buildings in between. However, the link budget is enough to allow wireless communication, as the minimum

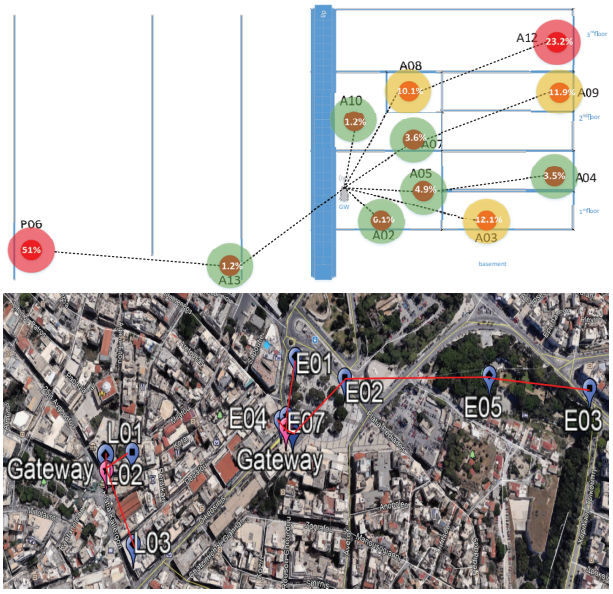

Figure 2. Network topology for (a) indoor and (b) outdoor deployments

RSSI observed value is still 33dB above the transceiver sensitivity. This shows that in outdoor smart city scenarios, the subGHz band works perfectly with respect to the RSSI level.

Figure 3 shows the histogram of the RSSI levels of all the outdoor devices for all the measurements. This shows that most devices have an RSSI between -52dB to -77dB, while there is also one device that has a much higher RSSI (since it is very close to the gateway). This figure helps to show that the outdoor links are quite good and there shouldn't be network outages due to bad connections.

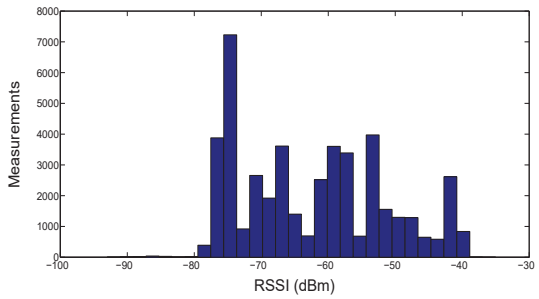

Figure 3. Histogram of the RSSI of outdoor devices

The RSSI and LQI metrics do not really show the whole picture with respect to the network reliability. One device might have very high values in these metrics, however due to collisions, errors or interference, it might be unresponsive and unable to send data correctly. Another metric used to evaluate the reliability of the wireless links is the "data timeliness" metric. This metric can be calculated by assessing the timeliness of the information exchanged, in order to identify lost packets or excessive delays compared to the expected delivery time of the packets. The "Data Timeliness" (DTi) can be calculated as a percentage of the actual interarrival time of the data compared to the scheduled frequency of the

Table 2. Outdoor deployment measurements

Device	RSSI (dBm)	RSSI_dev (dBm)	RSSI_min (dBm)	LQI	LQI_dev
L01	-72.1	2.51	-80	6.75	2.29
L02	-75.38	1.14	-80	7.18	2.15
L03	-51.31	6.87	-79	7.27	2.38
E01	-60.22	2.75	-86	6.45	2.24
E02	-66.6	2.18	-87	7.09	2.44
E03	-61.17	2.09	-78	6.58	2.27
E04	-58.34	2.39	-75	6.7	2.21
E05	-73.46	2.94	-93	6.77	2.27
E06	-53.95	1.99	-63	7.06	2.31
E07	-44.09	7.21	-93	7.62	2.48

data transmission. Thus, DTi = $\frac{IA_m - IA_{exp}}{IA_m}$, where IA_m is the measured interarrival time of the data and IA_{exp} is the expected interarrival time. For the outdoor measurements, the CDF of the data timeliness is shown in Figure 4. It is obvious that apart from one set of measurements for one device (noise measurements), almost all other data from all devices have a timeliness of more than 90%, which is very high and shows that the outdoor links are quite reliable.

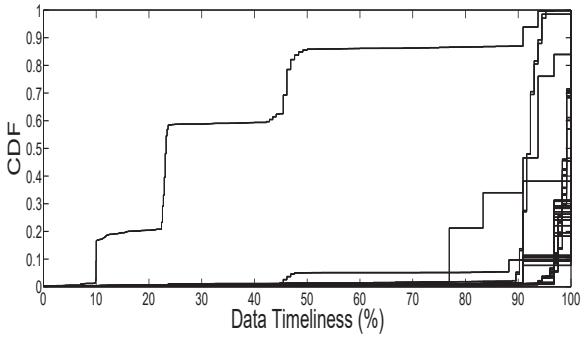

Figure 4. CDF of data timeliness in outdoor deployment

4.2 Indoor Deployment Network Reliability

For the indoor deployments, we considered measurements in two different locations, one (Androgeo) at the central square next to the outdoor deployment and another one at another building (Poleodomia). The link quality measurements of the indoor devices are summarized in Table 3. These devices use the 2.4GHz radio interface with a 5dBi antenna sharing the IEEE 802.15.4 channel 26 but with different PAN IDs between the two buildings.

Overall, all devices show normal link quality indicators considering the topology shown in Figure 2. The devices often change routes and may select new parents depending on the choices of RPL, but due to the location of the devices is safe to assume i.e. device A12 will always perform multihop to reach the GW, since it has to go through two floors,

Table 3. Indoor deployment measurements

Device	RSSI (dBm)	RSSI_dev	RSSI_min	LQI	LQI_dev	RX_lost (%)	TX_cca (%)
A03	-41.99	0.11	-42	107.19	0.47	12.1	0.5
A02	-57.06	0.96	-58	109.78	0.53	6.1	0.5
P06	-74.25	4.04	-92	101.95	13.2	51	2.1
A08	-41.38	0.49	-42	106.97	2.45	10.1	0.4
A05	-66.31	2.96	-73	106.84	4.26	4.9	0.6
A09	-88.6	1.14	-92	106.6	0.73	11.9	3.6
A12	-87.26	0.45	-89	106.67	2.19	23.2	0.5
A13	-88.97	1.57	-99	106.21	2.19	1.2	0.1
A04	-79.16	1.07	-82	106.9	0.75	3.5	0.8
A10	-77.96	1.03	-81	106.87	0.59	1.2	0.3
A07	-81.15	0.44	-81	107	0.41	3.6	0.5

typically via A08 or A07. The values shown for these multihop devices correspond to the link to their parents and not the gateway. The difference in the RSSI values due to obstacles in the line of sight is noticeable, as devices in the same location with the gateway have up to 15-20dB difference with respect to devices in different rooms or floors.

The most critical link is towards A13 as it goes through a thick wall to reach the gateway and also serves as an intermediate node to PO6. The minimum RSSI value of the link is -99dBm, which is 1dB below the radio sensitivity, but still allows the communication to take place. This link is generally stable and not prone to losses due to signal strength, as only a very small percentage of the observed values are within a 10dB margin respect to the maximum sensitivity.

The link quality remarks presented above compared to the network performance values shown in Table 3. The device A13 in overall has a low percentage of lost packets due to failed CRC checks, and as shown in the TX_cca column, it can send packets without having to back-off and retry due to failed CCA (clear channel assessment) checks. However, its child device, PO6 has the second highest percentage of dropped packet due to malformed packets, and per packet transmitted must check the medium and transmit more than two times due to congestion. The same tendency is shown in devices like A12, A09 and A04, having in common being more than one hop away from the gateway.

Figure 5 shows the histogram of the RSSI of the indoor devices. It is obvious that here the RSSI is much worse than in the outdoor deployments. Apart from two devices that are close to the gateway, all other devices have quite low RSSI, in the area of -90dB. This raises concerns with respect to the network reliability, but in order to have an overall picture, one has to see also the packet losses and the data availability and timeliness. The percentage of lost packets is shown in Figure 2 next to the device name. The devices are colored in green if the percentage of lost packets is low, with yellow if the percentage is medium and with red if the percentage

of lost packets is high. It is evident that devices close to the gateway have very good and reliable wireless links, with not many lost packets, even if they are also playing the role of forwarding packets to more distant devices.

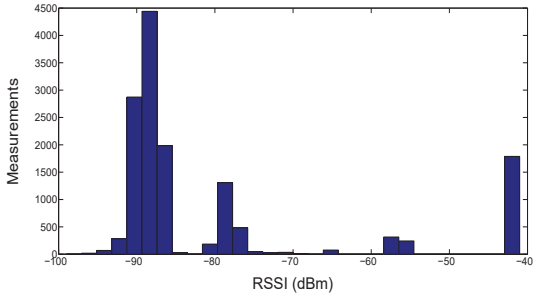

Figure 5. Histogram of the RSSI of indoor devices

Figure 6 shows the data timeliness for the indoor devices. Here, the situation is much different than in the outdoor scenario. Although many devices and data have quite high timeliness percentage (as expected), there are some devices and data that have medium to low timeliness, going down to even 10-20%. We should notice here the light measurements for device A04 are the ones that have very low timeliness, with almost 10% and the PM10 measurements of the same device have a timeliness of 20%. This is quite interesting because the link of A04 is considered (judging by the RSSI, LQI) as quite reliable, but still, although all other metrics are very good, it shows that for these measurements there are either delays in sending the measurements or there are buffer overflows and the measurements are discarded.

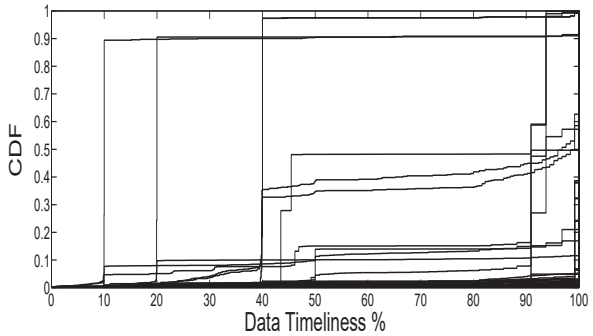

Figure 6. CDF of data timeliness in indoor deployment

5 Conclusions and Lessons Learned

In this work we present an experimental evaluation of the network reliability of a real smart city deployment in the city of Heraklion, Greece. The measurements were extracted during the system trials in the period of two months. The devices were continuously sending application-level data and network statistics and both were considered for the network reliability evaluation. The network reliability was assessed considering metrics for the RSSI, the LQI, the packet losses and the data availability. It is shown that considering only the RSSI or the LQI one cannot estimate the reliability of the wireless links and additional metrics for the interarrival time of the data and the packet losses have to be considered.

The outdoor links behaved very well, with very high RSSI and LQI values, quite low percentages of lost packets and very good data availability in almost all devices and measurements. This is quite interesting, since at some devices, their distance to the gateway is very long, for example the E03 device that has to go through three hops to reach the gateway. This shows also that using the cc1200 and the sub-GHz band for outdoor installations is a perfect choice, since it allows reliable communications even in long distances.

The indoor links behaved on average well enough. Although the RSSI and LQI values in all devices were well above the sensitivity thresholds, the lost packets in some devices were quite high and the data timeliness in some links was quite low. This is explained by the use of the 2.4GHz interface, which does not behave well when there are walls between the devices, degrading the signal and its quality.

6 Acknowledgments

This work has received funding from the EU FP7/2007-2013 under GA no 609094 and from the Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement no 642743.

7 References

[1] V. Angelakis et al. Analysis and evaluation of system performance and scalability. *RERUM D4.3*, 2016.

[2] N. Baccour et al. Radio link quality estimation in wireless sensor networks: A survey. *ACM Transactions on Sensor Networks (TOSN)*, 8(4):34, 2012.

[3] T. Bakıcı, E. Almirall, and J. Wareham. A smart city initiative: the case of barcelona. *Journal of the Knowledge Economy*, 4(2), 2013.

[4] G. Baron. Amsterdam smart city. *Amsterdam Smart City. Retrieved August*, 2:2014, 2010.

[5] A. Dunkels et al. The contiki os: The operating system for the internet of things. *Online], at http://www. contikios. org*, 2011.

[6] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, pages 309–322. ACM, 2010.

[7] J. Mattson. Message size overhead of coap security protocols. *IETF Internet draft, draft-mattsson-core-security-overhead-00*, 2017.

[8] G. Moldovan et al. An iot middleware for enhanced security and privacy: the rerum approach. In *NTMS, 2016 8th IFIP*. IEEE, 2016.

[9] U. Nations. World urbanization prospects: The 2014 revision, highlights. department of economic and social affairs. *Population Division, United Nations*, 2014.

[10] G. Papadopoulos, G. Oikonomou, et al. Laboratory evaluation results. *RERUM D5.3*, 2016.

[11] L. Sanchez et al. Smartsantander: Iot experimentation over a smart city testbed. *Computer Networks*, 61:217–238, 2014.

[12] Z. Shelby, K. Hartke, and C. Bormann. The constrained application protocol (coap). 2014.

[13] S. Y. Shin, H. S. Park, and W. H. Kwon. Mutual interference analysis of ieee 802.15. 4 and ieee 802.11 b. *Computer networks*, 51(12), 2007.

[14] A. P. Snow, U. Varshney, and A. D. Malloy. Reliability and survivability of wireless and mobile networks. *Computer*, 33(7):49–55, 2000.

[15] J. Soldatos et al. Openiot: Open source internet-of-things in the cloud. In *Interoperability and open-source solutions for the internet of things*, pages 13–25. Springer, 2015.

[16] E. Z. Tragos et al. Enabling reliable and secure iot-based smart city applications. In *PERCOM Workshops, 2014 IEEE on*. IEEE, 2014.

[17] E. Z. Tragos, A. Fragkiadakis, I. Askoxylakis, and V. A. Siris. The impact of interference on the performance of a multi-path metropolitan wireless mesh network. In *ISCC, 2011 IEEE*. IEEE, 2011.