Cyber Physical System based Proactive Collaborative Maintenance

D1.2 Consolidated State-of-the-Art of Sensor-based Proactive Maintenance Appendix 7: Wireless communication

Work Package	WP1 - Service platform architecture requirement definition. Scenarios and use cases descriptions
Version	1.0
Contractual Date of Delivery	30/04/2016
Actual Date of Delivery	03/06/2016
Dissemination Level	Public
Responsible	Erkki Jantunen
Contributors	Lidia Godoy (ACCIONA), Rafael Socorro (ACCIONA), Raquel Garc□a (ACCIONA)

The MANTIS consortium consists of:

Num.	Short Name	Legal Name	Role	Country
1	MGEP	Mondragon Goi Eskola Politeknikoa J.M.A. S.Coop.	CO	ES
2	MONDRAGON	Mondragon Corporacion Cooperativa S.Coop.	BEN	ES
3	IKERLAN	Ikerlan S.Coop.	BEN	ES
4	TEKNIKER	Fundacion Tekniker	BEN	ES
5	FARR	Fagor Arrasate S.Coop.	BEN	ES
5.1	KONIKER	Koniker S.Coop.	TP	ES
6	GOIZPER	Goizper S.Coop.	BEN	ES
7	ACCIONA	Acciona Infraestructuras S.A.	BEN	ES
8	MSI	Mondragon Sistemas De Informacion S.Coop.	BEN	ES
9	VTT	Teknologian Tutkimuskeskus VTT Oy	BEN	FI
10	LUAS	Lapin Ammattikorkeakoulu Oy	BEN	FI
11	NOME	Nome Oy	BEN	FI
12	FORTUM	Fortum Power And Heat Oy	BEN	FI
13	SQ	Solteq Oyj	BEN	FI
14	WAPICE	Wapice Oy	BEN	FI
15	AAU	Aalborg Universitet	BEN	DK
16	DANFOSS	Danfoss A/S	BEN	DK
17	UNIV	Universal Foundation A/S	BEN	DK
18	HGE	Hg Electric A/S	BEN	DK
19	VESTAS	Vestas Wind Systems A/S	BEN	DK
20	SIRRIS	Sirris Het Collectief Centrum Van De Technologische Industrie	BEN	BE
21	ILIAS	Ilias Solutions Nv	BEN	BE
22	ATLAS	Atlas Copco Airpower Nv	BEN	BE
23	3E	3e Nv	BEN	BE
24	PCL	Philips Consumer Lifestyle B.V.	BEN	NL
25	PHC	Philips Medical Systems Nederland B.V.	BEN	NL
26	PHILIPS	Philips Electronics Nederland B.V.	BEN	NL
27	S&T	Science and Technology B.V.	BEN	NL
28	TU/E	Technische Universiteit Eindhoven	BEN	NL
29	RUG	Rijksuniversiteit Groningen	BEN	NL
30	UNINOVA	UNINOVA - Instituto de Desenvolvimento de Novas Tecnologias	BEN	PT
31	ISEP	Instituto Superior de Engenharia do Porto	BEN	PT
32	INESC	Instituto de Engenharia de Sistemas e Computadores do Porto	BEN	PT
33	ADIRA	ADIRA - Metal Forming Solutions S.A.	BEN	PT
34	ASTS	Ansaldo STS S.p.A.	BEN	IT
35	CINI	Consorzio Interuniversitario Nazionale per l'Informatica	BEN	IT
36	AIT	Austrial Institute of Technology GmbH	BEN	AT
37	HBM	Hottinger Baldwni Messtechnik GmbH	BEN	AT
38	INNOTEC	Innovative Technology and Science Limited	BEN	UK
39	AITIA	AITIA International Inc.	BEN	HU
40	BME	Budaperst University of Technology and Economics	BEN	HU
41	JSI	Josef Stefan Institute	BEN	SI
42	XLAB	XLAB d.o.o.	BEN	SI
43	FHG	Fraunhofer Institute for Experimental Software Engineering IESE	BEN	DE
44	M2X	M2Xpert GmbH & Co KG	BEN	DE
45	STILL	STILL GMBH	BEN	DE
46	BOSCH	Robert Bosch GMbH	BEN	DE
47	LIEBHERR	Liebherr-Hydraulikbagger GmbH	BEN	DE

Document Revisions & Quality Assurance

Revisions:

Version	Date	By	Overview
0.1	24.8.2015	Lidia Godoy (ACCIONA)	First draft
0.2	4.9.2015	Aitzol Iturrospe	Added Wireless Sensors in Machine-Tools Systems
0.3	9.9.2015	Lidia Godoy	Added Abstract and Conclusions
0.4	6.10.2015	Riku Salokangas	Added contractual date of delivery etc. and formatting issues
0.5	19.04.2016	Lidia Godoy	Added topologies network and security issues
1.0	02/06/2016	Mikel Muxika (MGEP)	Format correction Deliverable info update

Abstract

This appendix provides an overview of Wireless Communication focussing on wireless sensor network based on standards, the possibility that it offers and benefits of using this type of communication.

Table of Contents

1 Wireless Sensor Network

A Wireless Sensor Network could be defined as a group of several spatially dispersed sensing nodes, dedicated to monitoring different parameters (temperature, pressure, tilt, acceleration, etc.), which are then collected at a central location and from there sent to a server.

Within a wireless sensor network there are three types of devices:

Coordinator: It is the most complete device. There exist only one in a network and it is the responsible of control the routes and network administration

Router: It is the responsible to interfacing devices through routing and addressing techniques

End device: It is a passive network element which responds to requests of superior devices (coordinator or router)

Data transmission between nodes could be done through four different wireless network **topologies**:

- Pair: It is composed by two nodes. One of them must be a coordinator and another one can be a router or an end device.
- Star: Each node is connected directly to the coordinator
- Cluster tree: The routers form a backbone with the end devices which are grouped around routers
- Mesh: It is not needed to have nodes dedicated exclusively to data transmission, because any sensing node can act as transmitter and receiver. Each node has a list of its "neighbor" nodes. This list is sorted: the first node in the list is the best option to send data and the last is the worst.

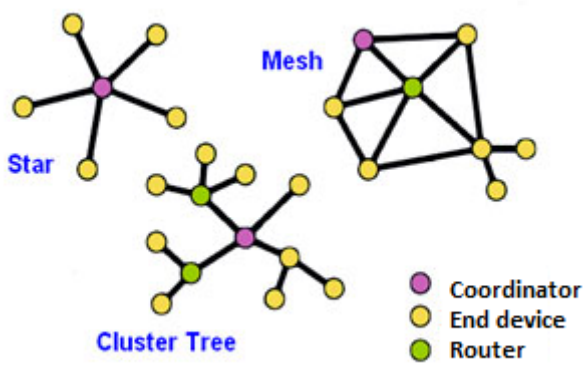

Figure 1. Wireless network topologies

A mesh topology provide great reliability, when a data packet is ready to be sent or arrives from another sensor, each node send data packets to the "best neighbor" option, until the packet arrives to a central point where data is collected (also called "root node") and sent to a storage point.

In a mesh network topology sensor nodes build themselves their own communications infrastructure, and this has three main advantages:

- No additional communication infrastructure is needed
- When any node is broken down, the remaining nodes which were communicating with it can recalculate routes and send data to another working node; therefore the communications

network is more robust compared to others (e.g. star, tree topologies) in the case that any node stops working properly

- The network can be easily scaled up in large areas just with the addition of new sensing nodes.

Many **standards** have been proposed to meet the requirement of WSN applications as evidenced IEEE 802 subgroups facing these issues (see figure below). The most interesting for these applications are part of the IEEE 802.15, which focus their efforts on developing Personal area networks (WPAN) or short distance networks area Personal or Short Distance Wireless Networks area (approximately 10 meters)

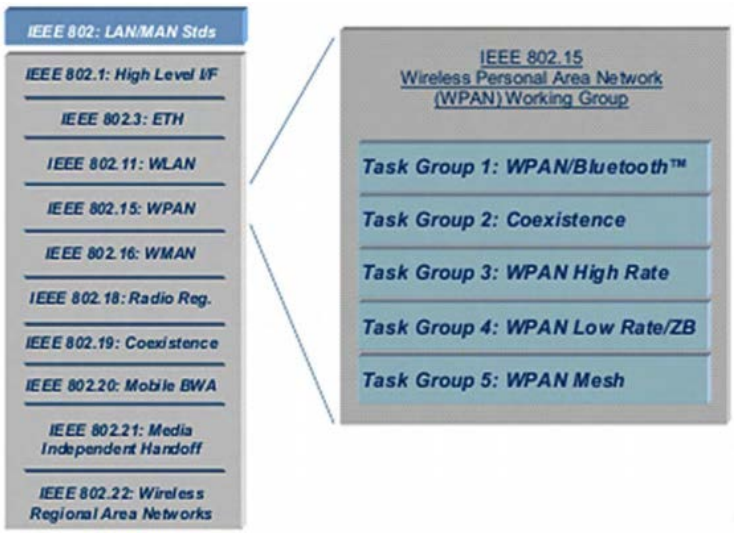

Figure 2. Standards IEE 802.X Sensors Networks. Source: Omar Am□rico, 2011. Thesis Sensor Networks

A wireless solution based on standards allow to the wireless network works without interruptions with the existing LAN system integrated in the subjected scenario to analyze.

1.1 Wireless Sensors in Machine-Tools Systems

Machine-tools systems operate under very demanding conditions so that their environment is particularly harsh, having to sustain temperature and pressure variations and high levels of acceleration. Although the monitoring of different physical parameters is extremely important, these environmental conditions, as well as the presence of rotating parts and limited access to areas of interest makes the integration of sensors a particularly complicated task. Therefore, the problem that arises is demanding in many ways:

- limited space,
- rotating elements,
- withstand harsh environmental conditions,
- properly mounting in the components,
- power-supply and
- communications in metallic environments.

Wireless sensors solve the problems related to the rotating elements and the limited space available. Therefore they appear to be a good choice for monitoring in this type of environment. Wireless sensors must be selected to withstand environmental conditions and to measure in the required ranges. In addition we need some way to fix them in the elements to be measured, provide power and communicate with the outside. Sensors must withstand the environment, need power supply and must support local communication modules.

2 Wireless Communication Benefits

- **Less/no wired**

In many environments, it is very difficult, expensive or even impossible to install a wired monitoring system. Examples of these environments are very long distances between the points of measurement (e.g. monitoring applications in large outdoor areas), already built complex buildings where the installation of wires is tedious and needs a lot of time and material, or areas where the installation of wires is not allowed. In this situation wireless systems are an ideal option to be used.

- **Robust infrastructure**

The use of a mesh network topology allows data to continuously arrive to the Gateway even if any sensor node in the network is broken down. In addition, the Gateway stores locally a backup of the collected information, so that when the internet connection to the remote central storage is not available, data is not lost.

- **Platform versatility**

It is possible to integrate into the platform different types of sensors (temperature, power meters, light, tilt, humidity, etc.), different types of energy sources (batteries, connection to the grid, solar energy), using different PCs and operating systems for hosting the Gateway module, and any type of Internet connection like DSL, mobile broadband, etc. can be used.

- **Upgradeability and scalability**

Due to the modular structure of the platform, it is easy to replace or upgrade any part of the system without interfering with the other modules. It is also very straightforward to include additional measurement points in an already working installation because no modifications or special configurations are needed in the system: it is just enough to install new nodes with the appropriate sensors in the additional measurement points.

- **Different power options**

Power consumption of wireless nodes is very low, so it is possible to feed these devices with batteries, grid or solar panels. Depending on the place where the node is going to be installed.

- **Easy of deployment**

Without the need for wires, the installation of the system is much simpler: in every point of measurement, a wireless node with the appropriate sensors is installed, using the most suitable mounting option (e.g. DIN rail, adhesive tape, etc.). The Gateway with the root node can be installed in any part of the building or monitored area from where the wireless nodes are accessible for the root node. Only power supply and an internet connection are needed for the Gateway.

- **Security**

Continued progress in standards and protocols have made to wireless networks can be as secure as wired networks. A wireless network offers robust security features such as data encryption to protect information traveling over the network; user authentication and safe access for visitors and temporary users. Although, the access to a wireless network medium is the air transmission meaning that is susceptible to further attacks.

3 Network security

Security of the information is an important issue that concern to companies. For that reason must be ensure data confidentiality and data authentication when implementing wireless networks. Fortunately, user knowledge about security and solution offered are improving.

There are actions to can help to protect a wireless network:

- Data protection during transmission through encrypted: It consists on an encryption algorithm which modify the message with a bits string known as security key. The original message can only be recovered by the final recipient.

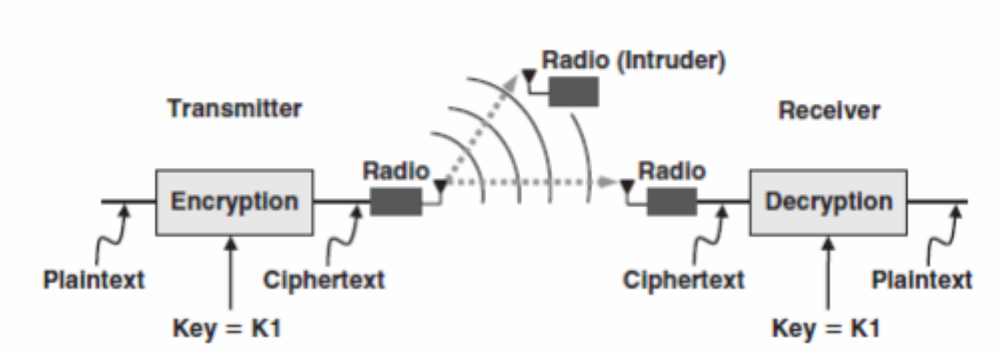

Figure 3. Example of radio intrusion. Source: Ant□n Girod, 2012

- Data authentication: In cryptography, a message authentication code (MAC) is a portion of information used for authenticate a message through hash functions (is a way to generate MACs) accepts as input a secret key and a message to be authenticated and outputs a MAC. That allow to verifiers (who also possess the secret key) to detect any changes to the message content.
- Remove uncertain access points: There are tools that can help to check uncertain access points using a management tool which collects data from access points

4 Conclusions

Wireless networks are connected by an unguided (wireless) mode transmission, so they have at anytime and anywhere communication ability, providing the advantage of mobility and quick installation. For example, wireless sensors solve many problems related to the rotating elements and the limited space available to take into account in the different scenarios. Many of the devices are suited for wireless connectivity which is based on standards and protocols allowing interoperability with other products. Nevertheless, also some inconvenient can occur, such as interferences, speed and security.

Ultimately, wireless networks are emerging as one of the most promising technologies in the coming years. Although progress has been made greatly over the past decade and there are moves important in the consolidation of communications wireless, this technology is currently in a phase of constant development and investigation.

References

Omar Am□rico, 2011. Graduation Thesis Sensor network

Jes□s Ram□rez y Jos□ Vicente D□az. □Las redes inal□mbricas m□s ventajas que desventajas□ http://www.uv.mx/iiesca/files/2012/12/redes2008-2.pdf

Ant□n Girod, 2012. Desarrollo e implementaci□n de una red de sensores Zigbee mediante el dispositivo Xbee de Digi