Ad-hoc & sensor networking for M2M Communications

Threat Landscape and Good Practice Guide

JANUARY 2017

www.enisa.europa.eu

European Union Agency for Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use opsec@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice
Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-207-3, DOI 10.2824/58281

Executive Summary

The term *M2M (Machine-to-Machine) communications* describes any solution or technology that facilitates the wired and wireless communication between networked devices to exchange information, as *ad-hoc networking* is an basic building block for M2M communications. Today, intelligent transportation, cyber-physical systems (CPS) and "Smart <anything>" (e.g. cities, buildings, vehicles, home appliances, phones) technologies have been intensified and attract the attention of the R&D enthusiasts. *Sensor networking* has the lion's share among almost any of the above emerging trends. In this context, it is almost a "condition sine qua non" to define any M2M implementation without including connected sensors in an ad-hoc approach.

All the above contribute in describing the emerging universe of the Internet of Things (IoT), which can be acknowledged as the driver for the evolution of M2M communications. In quantitative terms[1], the IoT connections are expected to exceed 27 billion by 2025 compared to 6 billion in 2015. In respect to the market-share, the revenue opportunity is accounted for 6.8 billion Euros, whereas this amount will increase to 2.7 trillion Euros by 2025. In terms of technology, 71% of all IoT connections are accommodated using a short-range technology (i.e. WiFi, Zigbee, NFC, in-building Programmable Logic Controllers - PLCs).

From the security perspective, the increased attack surface in ad-hoc and sensor networks has urged the development of technology for preventing attack incidents and for tackling system failures. In this vein, the networks acquire greater importance in *critical infrastructures* (i.e. industrial control systems, water and power plants, defence bases) and in *sensitive data exploitation* (i.e. healthcare, banking systems, social networks) for which privacy and ethics issues are likely to arise. Recent incidents proved that any connected device, such as smart TVs and video cameras[2,3], can be compromised to propagate illegitimate network traffic, but can also jeopardize security in a national and governmental level.

Objectives of the report

The ad-hoc and sensor networking Threat Landscape and Good Practice Guide complements the Annual Cyber Security ENISA Threat Landscape (ETL). It provides a deep overview of the current state of security in the ad-hoc and sensor networking for M2M communications. It also aims to support decision makers to comprehend the landscape and take informed decisions regarding cyber-security by incorporating consolidated information from the European Network & Information Security (NIS) threat landscape evolution.

Key findings

By analysing the threats to identified assets of the ad-hoc and sensor networking nomenclature, we focused on Wireless Mesh Networks (WMN), Mobile ad-hoc Networks (MANETs) and Wireless Sensor Networks (WSN). We observed that the current threefold M2M communications architectural model, as considered by the European Telecommunication Standards Institute (ETSI), can be expanded to two additional domains

[1] Machina Research (2016). *IoT Global Forecast & Analysis 2015-25*. [online] Available at: https://machinaresearch.com/report_pdf/428 [Accessed 18 Nov. 2016].

[2] Reuters (2016). Cyber attacks disrupt PayPal, Twitter, other sites. [online] Available at: http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME [Accessed 18 Nov. 2016].

[3] US-CERT (2016). *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets*. [online] Available at: https://www.us-cert.gov/ncas/alerts/TA16-288A [Accessed 18 Nov. 2016].

for addressing the operational challenges as well as the product/business processes. In the same context, we observed that the fusion of sensors, targeting to monitor the physiological vital signs of patients in clinical operations, leads to technical and legal considerations. We also observed that the regulatory frameworks do not explicitly define the obligatory actions that burden the end-users regarding their activities in a health-care environment. These gaps must be bridged to achieve privacy-friendly design of systems and services. Further, security-by-design in sensor networks is found to be inadequate in business processes (e.g. power generation and water distribution). These sensors operate in embedded systems whose preinstalled operating system is susceptible to malicious exploits. The limitation of not modifying these networks components should be eliminated without offending the sensor vendors' copyrights and industrial design rights. Considering that the M2M applications are increasingly based on the cloud computing (CC) paradigm and the respective deployment and service models, we observed that is adequate to only secure the application layer of a service in accordance with legacy environment practices because those service models are mutually dependent for provisioning the end-services.

List of Recommendations

The main recommendations follow; for deeper explanations see section 9.6.

- For developers, M2M applications development in CC environments should be performed by adopting and expanding the application security guidelines of standardization organizations and cover the needs of the M2M architecture.
- For administrators: Identify by whom the sensorial data is accessed. Specific policies should be established about authorising procedures and sharing agreements regarding these data.
- For administrators and service providers: Security by design should be implemented for each layer of the ad-hoc network.
- For service providers, administrators and decision makers: The underlying infrastructure of M2M applications and operations should comply with the security and operations regulatory frameworks regarding the protection of personal data.
- For administrators and networks/service providers: An elastic type of access control mechanism is to be incorporated in ad-hoc and sensor networks
- For administrators and network/service providers: Mobile Edge Cloud Computing (MEC) to be orchestrated so as to develop a perimeter defence and collect/analyse forensic information about the attacks.

Table of Contents

1. Introduction

For 2016, the first ENISA strategic objective foresees: *"To develop and maintain a high level of expertise of EU actors considering evolutions in Network & Information Security (NIS)"*[4]. The current study analyses the threats and the threat landscape for ad-hoc and sensor networks. We perform a comprehensive compilation of the respective threats by analysing collected information, and deliver the respective threat analysis and landscape reports on the application area.

Ad-hoc and sensor networks for smart objects are utilized for the collection of critical, sensitive, massive and other types of data in several points of interest, such as weather stations, healthcare environments, aviation and car fields, baggage and asset tracking, home and industry applications, manufacturing and supply chain analytics and management. Then, the data can be analysed to trigger several corrective/preventive actions; record and analyse system failures, initiate the appropriate remedial changes, apply/revert configuration changes, and provide the quality data reporting and statistical process/control analysis. Today, smart transport, smart finance and loans, smart utilities, smart supply and manufacturing, smart environments, smart energy, smart home, and smart health involve numerous interconnected devices and rely heavily on ad-hoc and sensor networks (Figure 1).

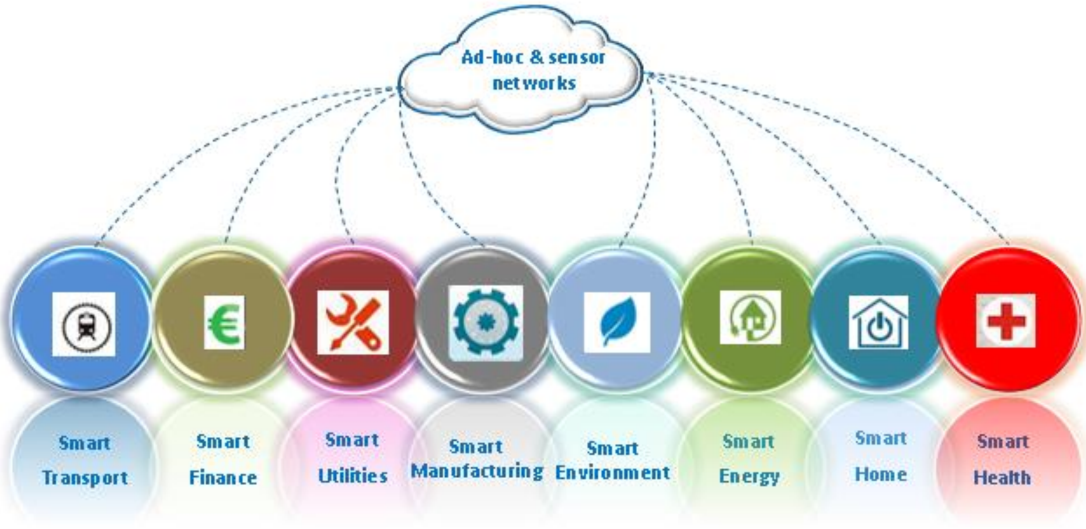


Figure 1 Global ad-hoc and sensor network market space

These pervasive and ubiquitous networks facilitate the processing and collection of data generated by sensors and smart devices. In many cases, the operations, the resiliency, the availability and the performance of these networks are critical, and, thus, we need to protect the secure exchange of the information, and ensure data privacy and integrity. Besides, the reduction of their attack surface is among the predominant issues that thrive during the operation of ad-hoc and sensor networks. Due to the increased attack surface in ad-hoc and sensor networks, we need to prevent security incidents, tackle system failures, and mitigate

[4] European Union Agency for Network and Information Security (ENISA). (2016) *ENISA Work programme 2016* [online] Available at: https://www.enisa.europa.eu/publications/corporate/enisa-work-programme-2016 [Accessed 18 Nov. 2016].

the associated risks. Even more, the necessity to reduce the attack surface acquires greater importance in critical environments (e.g. industrial control systems) and whenever sensitive data are involved (e.g. in healthcare, banking systems and social networks), severe privacy and ethics issues may arise (e.g. compromise of sensitive medical records and patients' data). Inevitably, these networks constitute a strong point of interest for several research teams throughout the world.

1.1 Policy Context

This report aims to analyse the evolving threat environment both from the stakeholder and the EU policy makers' perspective by identifying evolving threats, risks and challenges related to ad-hoc and sensors networks with a special approach to the M2M communication architectural model.

The different challenges appeared during the adoption of new models of communication (such IoT and M2M) suggests to propose a set of recommendations aligned with the EU strategy in research and innovation[5]. A great added value is expected to be created as a result of these technology advancements. The market value of the Internet of Things (IoT) in the EU is expected to exceed one trillion euros in 2020[5]. Within the IoT ecosystem, the major goal is to interconnect networks of sensors and smart objects in a way that they can intelligently interact with humans, and to ensure the secure and seamless sensor and network connectivity. In this context, ENISA expects these sectors to take advantage of the current ad-hoc and sensor network for M2M communications threat landscape and provide added-value services to the IoT and M2M technologies. By enabling a secure, trusted, reliable, and resilient environment, the industry will be more competitive, and the markets within the EU will benefit from numerous innovative use cases. Therefore, it is vital to promote and establish secure ad-hoc and sensor network for M2M communications, and manage efficiently the large volumes of connected devices[6].

The European Commission (EC) supports the evolutionary trends of ad-hoc and sensor networks leading to the integration of sensor appliances in the market through various research and project efforts, such as the *MOBILEMAN* project[7], and the multi-sensor platform *AirSensEUR*[8]. The EC has also acknowledged the emerging trends, identified the need for cross-layer techniques and efficient cooperative protocols, and has implemented and validated the feasibility of the outcome of the *Cooperative transmission and cross-layer techniques for secure wireless sensor networks* (Coolness) project[9].

The current report identifies the ad-hoc and sensor network assets and illustrates the ad-hoc and sensor networking threats by reviewing the current working and environmental practices, assessing the private and public initiatives, and analysing the research information in this area. The report also provides the threat

[5] European Commission, Directorate-General of Communications Networks, Content & Technology. (2014). *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination* [online] Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472 [Accessed 18 Nov. 2016].

[6] European Commission. *Digital Single Market: The Internet of Things* [online] Available at: https://ec.europa.eu/digital-single-market/en/internet-things [Accessed 18 Nov. 2016].

[7] CORDIS: Mobile ad-hoc networks: from theory to reality [online] Available at: http://cordis.europa.eu/result/rcn/85259_en.html [Accessed 18 Nov. 2016].

[8] AirSensEUR: an open-designed multi-sensor platform for air quality monitoring [online] Available at: https://ec.europa.eu/jrc/en/publication/airsenseur-open-designed-multi-sensor-platform-air-quality-monitoring [Accessed 18 Nov. 2016].

[9] Periodic Report Summary - COOLNESS (Cooperative transmission and cross-layer techniques for secure wireless sensor networks) [online] Available at: http://cordis.europa.eu/result/rcn/46005_en.html [Accessed 18 Nov. 2016].

analysis, the risks and vulnerabilities in the EU Global Security Strategy to be more effective in tackling the contemporary challenges in mobility, cyber-attacks, and terrorism, and to manage crises and conflicts[10].

1.2 Target audience

Looking at the activities and the deliverables which are provided by this study and by the ENISA Threat Landscape (ETL), the following target groups can be assorted to:

- **Public Community** to better understand the asset exposure and risks
- **EU Member States** with the aim to understand the protection requirements and develop more cooperative among the member states and industry
- **EU Commission** to provide a closer strategic policy, and enforce more efficient mechanisms (e.g. Network and Information Systems Directive)
- **Business community** to simplify the content of the threat intelligence and improve policy making
- **Industry stakeholders** to develop working good practices and uncover the emerging threats
- **Public and private organizations** to adapt seamlessly operated security controls to be included in the complex modern environments
- **Security professionals** to elaborate on threat models and continuous improvement to protection and detection tools
- **Risk managers** in any risk assessment process to identify, assess and prioritize the risks

All the types of the provided information aim at supporting decision makers in all kind of organizations to understand the threat landscape and make informed decisions regarding cyber-security by receiving integrated and consolidated information about the ad-hoc and sensor networking for M2M communications. This document can also be useful for experts working in the EU's electronic communications sector and for experts working in the information security field.

1.3 Scope of the Study

As described in the ENISA regulation, one of the objectives of the agency is to assist the Union institutions, bodies, offices and agencies in developing policies in network and information security by including accumulated expertise related to availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems. For instance, the new ENISA regulation undelines the necessity to analyse current and emerging risks (and their components), stating: "the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information". In particular, under *Art. 3*, Tasks, *d), iii),* the new ENISA regulation states that ENISA should enable effective responses to information security risks and threats.

This document is published by ENISA to provide a threat analysis and best practices guideline to ad-hoc and sensor networking trends, and it also addresses the risks and threats of these technologies underpinning the emergence of a 'smart' society. The ad-hoc and sensor networking threat information is directed to executives, security architects and security managers. Nonetheless, the provided information can also be

[10] A Global Strategy for the European Union [online] Available at: http://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union [Accessed 18 Nov. 2016].

considered by non-experts. Furthermore, since the Agency assists the European Commission and EU Member States, it cooperates with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the Internal Market.

1.4 Methodology

The current study examines various use cases to identify the respective assets and then collect, analyse and categorize the ad-hoc and sensor networking threats. For the project execution, our methodology performed research and collected the information through various sources (i.e. journals, conference papers, white papers, industry recommendations, online documents). Various sources have been identified and studied during our investigation.

We consider previous ETLs to specify the format, to review the ENISA taxonomy threats, and study the approach taken in those ETLs. Besides, we also consider several other sources regarding the existing EU policies and we identify evolving threats, risks and challenges related to ad-hoc and sensors networks with a special focus on the M2M communication architectural model. All these threats are assessed, categorized and analyzed by means of several references to the collected sources. Then, we perform an analysis of the existing good practices and present how the threat exposure can be reduced, while we identify gaps in existing practices. A presentation of the state-of-the art developments in the area of threat intelligence is also undertaken. Finally, we study how we can adapt best security protection practices towards a more agile management of security controls.

All the collected sources are written in English, and all the referenced web resources were last accessed in November 2016.

1.5 Structure of this Study

The structure of this document is as follows: in chapter 2 we provide the ad-hoc and sensor networking for M2M communications basics and present the architecture; in chapter 3 we illustrate the asset taxonomy for ad-hoc and sensor networks in M2M communications, and present the use cases that are analysed in the current study; in chapter 4 we identify threats against ad-hoc and sensor networks, and in chapter 5 we map these threats to the assets; in chapter 6 we consider which threat agents are more relevant to ad-hoc and sensor networks attacks; in chapter 7 we present the vulnerabilities and risks in ad-hoc and sensor networks; in chapter 8 we present a set of recommendations and good practices for ad-hoc and sensor networks; in chapter 9 we provide the gap analysis, and finally in chapter 10 we conclude the study.

In addition, we have also included two annexes at the end of this document. Annex A contains the ad-hoc and sensor network assets matrix for specific use cases, while Annex B contains the ad-hoc and Sensor Networks' Full Threat Taxonomy.

2. Ad-hoc and sensor networking architecture

The term M2M is used to describe technologies that allow the communication between devices with no or limited human intervention[11]. The M2M communication requires wired or wireless connection between the nodes. In the case of Wireless ad-hoc networks, the M2M communication is wireless. M2M mainly focuses on the machine-type-communication (MTC), where the devices are communicating end-to-end. The key components of the M2M models are field-deployed wireless devices with embedded sensors or wireless communication networks with radio-frequency identification (RFID) features.

Wireless ad-hoc networks for M2M communications, also known as WANETs, can be classified in three types, based on their application[12]:

Wireless Mesh Networks (WMN) use a mesh topology consisting of radio nodes. The nodes are the mesh client, and the mesh routers or the mesh gateways. In WMN the mesh clients, often laptops, cell phones etc., behave both as hosts and routers for the network. This way each client contributes to the range expansion of the network. Most WMN implementations are found in harsh environments or in situations like field operations of military forces, satellite communications inside a constellation, public transportation monitoring or real time telemetry on car races. Likewise, they are also deployed in broadband home networking, community and municipality networking[13].

A Mobile ad-hoc Network (MANET) is an "on demand" contacted network, mainly between mobile devices such as smartphones and tablets. Each node behaves like a router, forwarding any traffic unrelated to its own use. The fact that nodes move independently of each other makes this type of network unreliable and of a constant changing topology. Some more specific implementations of MANET include the military ad-hoc networking between soldiers in the field, vehicles and headquarters, ship-to-ship ad-hoc mobile communication, Personal Area Networks (PAN)[14] etc.

A Wireless Sensor Network (WSN)[15] is a network of smart sensor nodes. A smart sensor node is a device equipped with a processor, a memory, a wireless network interface, and one or more sensors and actuators. The sensors give the device the ability of monitoring several physical or environmental conditions. The memory is limited to processing aid, thus, all the data acquired by the node are transmitted wirelessly to a base station for storage and further processing. Also via WSN the base-station or any other node can send data back to one sensor node; e.g. a command for the actuator. Various applications of WSNs have emerged in several fields, such as in healthcare, military, manufacturing and industrial/public systems, environment and smart homes as shown in Figure 2.

[11] Mehmood, Y., Görg, C., Muehleisen, M., Timm-Giel, A. (2015). Mobile M2M communication architectures, upcoming challenges, applications, and future directions. *Journal on Wireless Communications and Networking*, 1, pp.1-37

[12] Rani, V., Dhir, R. (2013). A Study of Ad-Hoc Network: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, 3(3), pp.135-138.

[13] Di Pietro, R., Guarino, S., Verde, N., Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks – A survey. *Elsevier, the International Journal of Computer Communications*, 51, pp.1-20.

[14] Ahmed, E., Ali, B., Osman, E., Ahmed, T. (2016). Performance Evaluation and Comparison of IEEE 802.11 and IEEE 802.15.4 ZigBee MAC Protocols Based on Different Mobility Models. *International Journal of Future Generation Communication and Networking,* vol. 9, no. 2, pp.9-18.

[15] Pinar, Y., Zuhair, A., Hamad, A., Resit, A., Shiva, K., Omar, A. (2016). Wireless Sensor Networks (WSNs): The Shortcomings of Wireless Sensor Networks, *IEEE Long Island Systems, Applications and Technology Conference*, pp.1-8

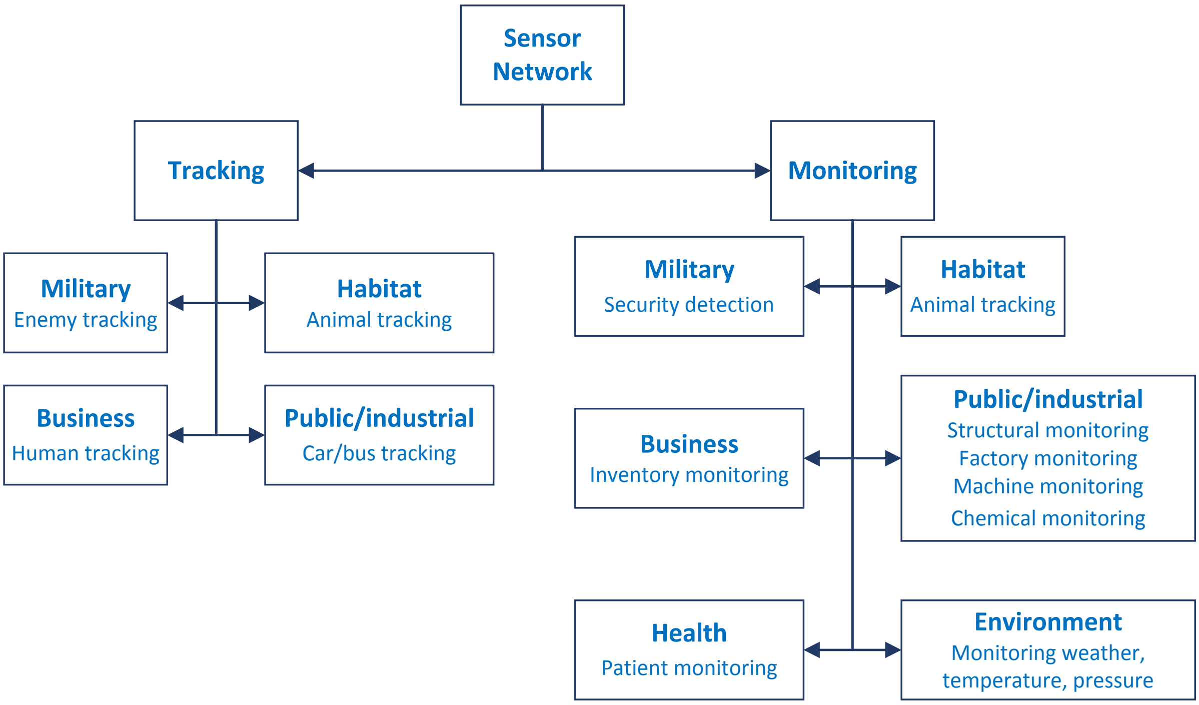
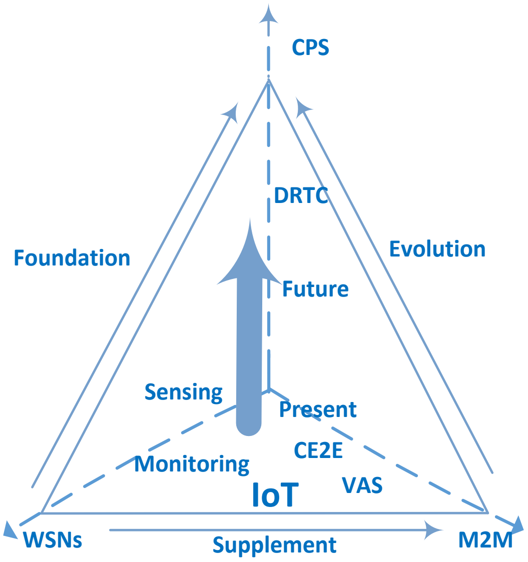


Figure 2 WSN Applications[15]

Additionally, the rapid evolution of M2M communications generates new challenges and opportunities for the information industry; such as for smart robots, cyber-transportation systems (CTS), M2M telematics and predictive analytics, smart grids and cyber-physical systems (CPS). CPS is an evolution of M2M[16,17] in intelligent information processing and an important form of IoT[18]. The respective CPS applications are going to benefit from massive wireless networks and IoT based on the information they collect from the surrounding environment. The correlations among M2M, WSNs, CPS, and IoT are shown in Figure 3.

[16] Pticek, M., Podobnik, V. and Jezic, G. (2016). Beyond the Internet of Things: The Social Networking of Machines. *International Journal of Distributed Sensor Networks*, SAGE Publications, pp.1-15.
[17] Ali, A., Shah, G. and Arshad, J. (2016). Energy efficient techniques for M2M communication: A survey. *Journal of Network and Computer Applications*, 68, Elsevier Publishing, pp.42-55.
[18] Mišić, V. and Mišić, J. (n.d.). Machine-to-machine communications. CRC Press (eds.), ISBN-13: 978-1466561236.



CPS: Cyber-Physical Systems
DRTC: Distributed real-time control
CE2E: Communicating end-to-end
VAS: Value added services

Figure 3 Correlations between M2M and WSN[19]

The current document encompasses the M2M architectural model. This model is composed of different domains, each of them having its own characteristics, assets, threats and vulnerabilities, existing cyber threats, trends, security challenges, associated risks and required countermeasures related to ad-hoc and sensors networks, with a special approach to the M2M communications architectural model.

The European Telecommunication Standards Institute (ETSI)[20] considers an M2M network as a three-part structure that includes the:

1. M2M Device domain (usually embedded)
2. M2M Network domain (connection between devices, sensors and gateways, network to network connection)
3. Application domain (data manipulation and usage by specific business-applications)

In the current study, ***we consider two additional domains*** to address the operational challenges as well as the products and the business processes automation and workflows, namely the.

1. Operational domain (includes physical security, control systems and utilities)

[19] Mehmood, Y., Görg, C., Muehleisen, M., Timm-Giel, A. (2015). Mobile M2M communication architectures, upcoming challenges, applications, and future directions. *EURASIP Journal on Wireless Communications and Networking*, 2015(1), pp.1-37.

[20] European Telecommunications Standards Institute (ETSI). (2013). *Machine-to-Machine communications (M2M); Functional architecture*. Technical Specification, ETSI TS 102 690 V1.1.1 (2011-10). [online] Available at: http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf [Accessed 18 Nov. 2016].

2. Product/business processes domain (e.g. healthcare, transportation)

These five elements form different interlinked domains[21], facilitate the data processing by various application services and achieve full interoperability of network and services[11]. The full-picture of the five elements is depicted in Figure 4.

In the *Device domain*, M2M devices constitute several ad-hoc and sensor network nodes for data forwarding. These devices are equipped with specific sensing technologies for real-time monitoring to take the appropriate transmission decisions to the gateway (i.e. single-hop or multi-hop transmission). The M2M gateway acts as the entrance to another network and collects the packets from the M2M nodes via the M2M network. This network furnishes a connection between all kinds of intelligent devices (or sensors) and gateways. In the *Network domain*, communication networks achieve connections and transmit the sensory data between gateways and applications.

Various application services are used by the specific business-processing engines in the *Application domain*. These services are responsible for storing the data and for providing the data to the M2M applications for management.

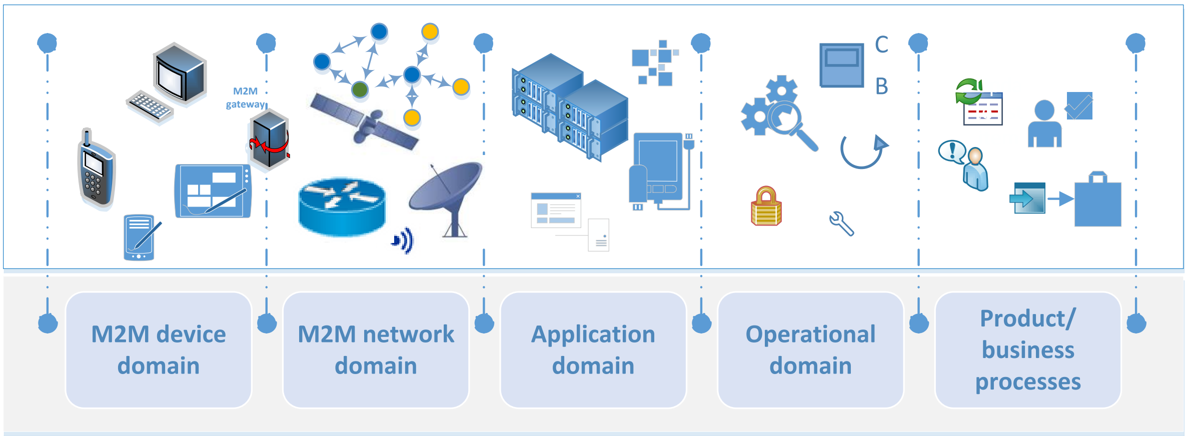


Figure 4 M2M Architecture

In the M2M communications architectural model, the *operational* and *product/business processes domain* can also widen the business possibilities and utilize the real-time information[22] produced by the M2M system employing a convergence of various technology families.

[21] Lu, R., Li, X., Liang, X., Shen, X., & Lin, X. (2011). GRS: The green, reliability, and security of emerging machine to machine communications. *IEEE communications magazine*, 49(4), pp.28-35.

[22] Galetić, V., Bojić, I., Kušek, M., Ježić, G., Dešić, S., Huljenić, D. (2011). *Basic principles of Machine-to-Machine communications and its impact on telecommunication industry*, MIPRO, Proceedings of the 34th International Convention, 23-27 May, Opatija, Croatia, pp.380-385.

3. Ad-hoc and sensor assets identification

Anything of value can be considered as an asset. Assets could be abstract assets (like processes or reputation), virtual assets (data for instance), physical assets (cables, a piece of equipment), human resources, money, etc[23]. In this study, we focus on the ETSI taxonomy[20] and the aforementioned M2M architecture (Figure 4). We analyze the assets related in the area of specific use cases, as there is a very large number of interconnected devices, and a significant amount of asset types in the ad-hoc wireless and sensor networking for M2M communications sector. Conclusively, the approach presented should not be considered as exhaustive, but rather an analysis of assets in different business cases and diverse perspectives.

In the Device domain, we capture these devices which are capable for data processing, while in the Network domain, we study the assets that enable the communication between the applications. We also include the operational aspects and the business process modeling in order to combine classical functions and processes with ad-hoc and sensor networking extensions, and capabilities. Data exchange, control systems, monitoring, and metering applications can be part of several business processes that enable the standardization, and the interoperability of the implementations of M2M solutions.

3.1 Asset taxonomy

The ad-hoc and sensor network assets are identified and classified based on the building blocks of the following domains:

1. ***Application domain***
   a. Data
   b. Critical applications
   c. eHealth
   d. Cloud-based applications
2. ***Device domain***
   a. Car/vehicles
   b. Mobile devices
   c. RFID tags
   d. RFID readers
   e. Radars
   f. Transmission nodes
   g. Interconnection point
   h. Support systems
   i. Wearable
   j. Indoor positioning systems
   k. Computer Electronics (CE) devices

[23] European Union Agency for Network and Information Security (ENISA). (2015). *Guideline on Threats and Assets*. Technical guidance on threats and assets in Article 13a. [online] Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets/at_download/fullReport [Accessed 18 Nov. 2016]

3. *Network domain*

a. Communication protocols
b. Cooling systems
c. Power supplies
d. Home Automation
e. Mobile user and location registers
f. Radio
g. Public-Key Infrastructure (PKI)
h. Appliance controls
i. Addressing servers
j. Mobile switches
k. Public Switched Telephone Network (PSTN) switches
l. Physical security & control systems
m. Routers & switches
n. Mobile base stations and controllers
o. Servers
p. WBSNs (Wireless Body Sensor Networks)

4. *Operational domain*

a. Physical security
b. Control systems
c. Utilities

5. *Product/business processes domain*

a. Supply and provisioning
b. Manufacturing
c. Healthcare
d. Transportation

3.2 Asset categories

According to the European Telecommunication Standards Institute (ETSI), the M2M architecture[20] consists of three domains; the *Device domain*, the *Network domain* and the *Application domain*. As presented in Chapter 2, we extend the model including the *Operational domain* and the *Product/business processes domain*. Based on this categorization, the valuable ad-hoc and wireless sensor network assets are listed below. A full list of these assets is shown in Figure 5.

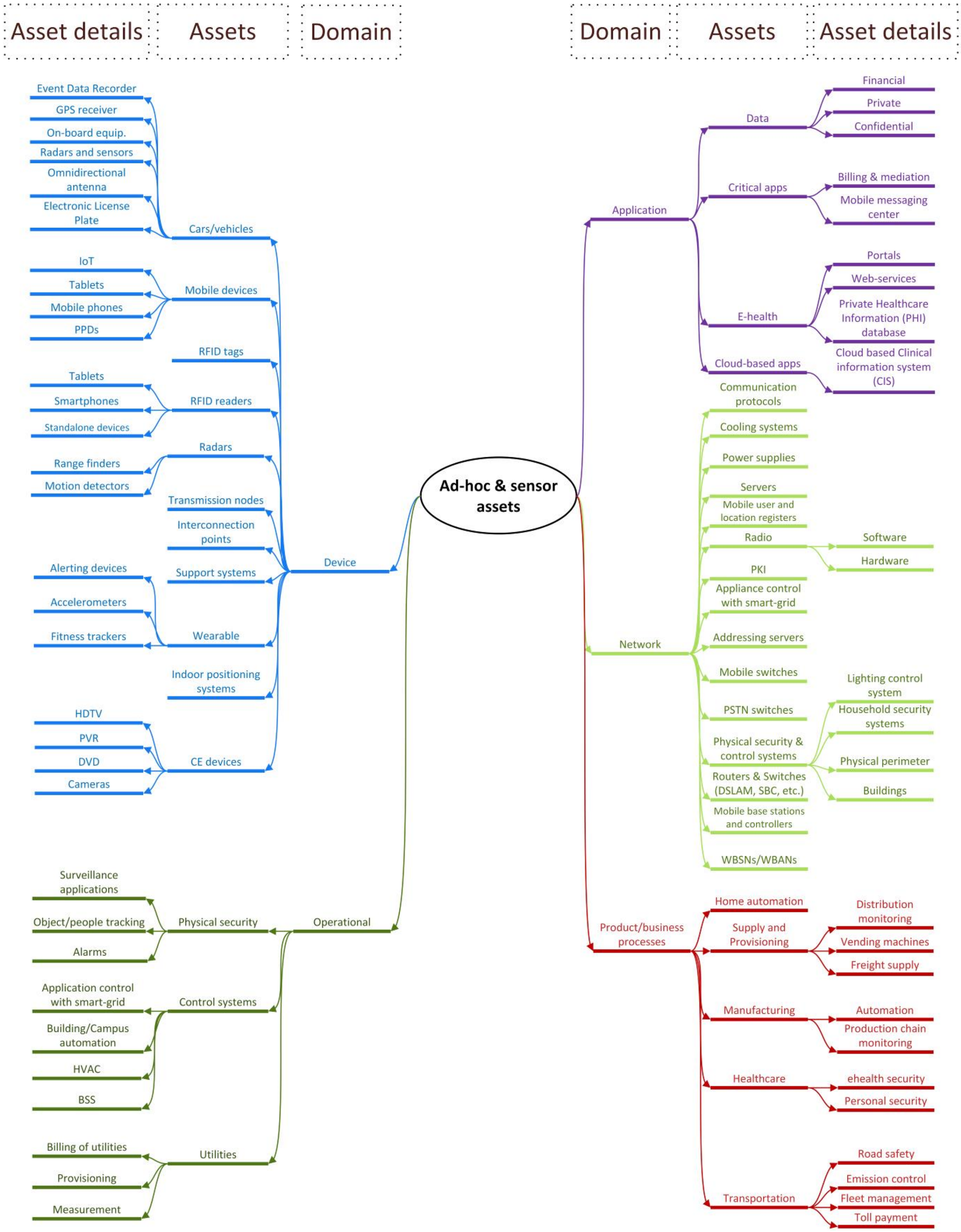


Figure 5 Assets Taxonomy

3.2.1 Application domain

The Application domain involves M2M and client applications. It is the middleware layer between the end-user and the data provided by the M2M *Device domain*, after being processed by various application services. The assets of this domain are described below, however is needed to mention that applications listed in this domain are not exhaustive and we are going only to cover certain interesting application areas.

a. Data

In this domain, the data collected from devices is stored, managed and represented via applications or web interfaces to user. The data can be used for information only, statistical analysis, and control capabilities.

b. Critical applications

Critical applications are special-purpose applications, combining information and data from diverse sources (i.e. sensors, devices, internet, and databases).

c. eHealth

In a Mobile Healthcare Network (MHN)[24] the data combination from wearables, smartphones and vitals monitoring equipment can provide to the individual or the physician the whole picture of a health case, and the Personal Health Record (PHR)[25]. An essential part of an MHN is the eHealth applications that store, represent and process the collected data to produce statistics. In the need of storing PHRs, a Private Healthcare Information (PHI) database is used with special concerns in privacy and data protection. Representation interfaces are the eHealth portals, web-based or mobile applications.

d. Cloud-based applications

The integration of sensor networks and cloud computing[26] is motivated by the processing and storage capabilities of the cloud. This sensor-cloud sensing-as-a-service (SSaaS) leads to the ability of having multiple applications accessing the sensor data at the same time. Additionally, the sensor-cloud model improves the sensor's resources' utilization, and the sensor management and provides the environment for developing software interfaces between sensors and the cyber or real world.

Furthermore, mobile computing applications accommodate an increasing effort to assist the sensor networking ecosystem. On these grounds, recent technology advances in mobile cloud applications include the Open Mobile Alliance's (OMA) Smartcard Web Server[27], which is literally coupled with a mobile device (e.g. Subscriber Identity Module (SIM) card) that connects directly with the Carrier to push applications to mobile phones. Another example is TokTok, a technology that allows access to cloud-based services like Gmail and Google Calendar by voice, using the mobile phone device[28].

[24] Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X. and Luo, H.H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. *IEEE Wireless Communications*, 22(4), pp.104-112.

[25] Kahn, J., Aulakh, V. and Bosworth, A. (2009). What It Takes: Characteristics of The Ideal Personal Health Record. *Health Affairs*, 28(2), pp.369-376.

[26] Dinh, T. and Kim, Y. (2016). An Efficient Interactive Model for On-Demand Sensing-As-A-Services of Sensor-Cloud. *Sensors — Open Access Journal*, 16(7), pp.1-28.

[27] Open Mobile Alliance (OMA). (2016). *OMA Smart Card Web Server*. [online] Available at: http://openmobilealliance.org/oma-smart-card-web-server/ [Accessed 18 Nov. 2016].

[28] Lin, H., Bai, D., Gao, D. and Liu, Y. (2016). Maximum Data Collection Rate Routing Protocol Based on Topology Control for Rechargeable Wireless Sensor Networks. *Sensors — Open Access Journal*, 16(8), p.1201-1227.

3.2.2 Device domain

The M2M Device domain in the ETSI architecture is the combination of M2M devices and the M2M Area Network. The M2M Device domain, as the term implies, is the group of devices capable of replying to data requests or transmitting this data autonomously. The connectivity between M2M devices and M2M Gateways is the M2M Area Network. The following subsections present the most common assets in the Device domain.

a. Cars and vehicles

The Vehicular ad-hoc Networks[29] (VANETs) are a subclass of the Mobile ad-hoc Networks (MANETs). The hardware asset of a VANET is mainly the on-board equipment installed in vehicles, which provides them with the means to communicate with other vehicles (Vehicle-to-Vehicle communication - V2V) or with the network infrastructure (Vehicle-to-Infrastructure - V2I and Infrastructure-to-Vehicle - I2V). Some VANET hardware assets[30] are presented below:

Event Data Recorder (EDR): records transmissions and receives messages and all the events that occurred in the vehicle environment during a trip

Global Positioning System (GPS) receiver: communicates the geographic location, the speed, the direction of the movement and the node acceleration at specified time intervals

Radars and sensors: used to detect obstacles in the vehicle environment

Omnidirectional antenna: used to access wireless channels

Electronic License Plate (ELP): provides an ID number used by the police or any other authority

b. Mobile device

A mobile device connects to the area network utilizing the built-in sensors (camera, gyroscope, thermometer, GPS, etc.), the embedded interfaces (GSM antenna, Wi-Fi, Bluetooth, etc.), and the Personalized Portable Devices (PPDs).

c. RFID tags

In the Device domain, the RFID systems[37] include *tags*, *readers* and the *RFID middleware*. *RFID tags* are the small labels attached on objects, animals or people to embed some information on them or to make them identifiable among others. An RFID tag circuit consists of a control unit and an antenna.

d. RFID readers

An *RFID reader* is a device or receiver often embedded in other common devices, (i.e. smartphones) that can get the information of a tag when it is within range. The software that ensures the communication between the reader and a database storing system is called *RFID middleware*. The latter filters, processes and sends the collected data from the reader to the database and provides an interface to enable data access for external applications.

e. Radars

[29] Aswad, R. and Abdala, M. (2016). Performance Enhancement of VANET Routing Protocols. *Journal of Telecommunications*, 32(1), pp.5-10.

[30] Wei, C., Jianding, Y. and Xiangjun, L. (2012). *The design of electronic license plate recognition terminal system based on nRF24LE1*. 5th International Symposium on Computational Intelligence and Design (ISCID). 28-29 Oct, Hangzhou, China, pp.127-129.

A micro-power Impulse Radar (MIR[63,31]) is applicable in many fields as a motion detector or range finder. Radars are widely used in the military for asset protection, in rescue applications, in vehicle automation (parking assistance, cruise control, etc.), in home security systems (keyless locks, automatic doors, etc.) and in manufacturing field (industrial automation).

f. Transmission nodes

In a clustered architecture, sensor nodes are grouped into clusters where each cluster has elected a node as Cluster Head (CH)[32]. This node is the one that transmits all the cluster nodes' data to the base station. This mitigates energy consumption, traffic congestion and data collisions into the network.

g. Interconnection points

According the ETSI M2M architecture, an interconnection point is the gateway between the devices and the communication network, which is also referred in the architecture as an M2M Gateway. The interconnection point manages the packets and provides efficient paths for transmitting these packets to the remote back-end server via the Network domain.

h. Support systems

Due to the complexity and the high volumes of traffic in ad-hoc and sensor networks, there is an emerging need for the appropriate support systems in a sustainable, converged, integrated and operational way. Business Support systems (BSS) is a collective term for the set of software solutions used by telecommunication providers to run their business operations. The term includes software for billing and charging, customer management, product design and management, sales and marketing, and order and order activation. BSS is also an operational asset of the networks in question.

i. Wearables

A wearable[33] can comfortably be worn or carried by an individual all day long and monitor several biometrics like body temperature, blood pressure, diabetes levels, transpiration, heart beat rate, etc. Generally, the wearable technology has some form of communication capability and allows the wearer to access the information in real time. Data-input capabilities feature the wearable devices, same as the local storage. Examples of wearable devices include watches, glasses, contact lenses, e-textiles and smart fabrics, headbands, beanies and caps, jewellery such as rings, bracelets, and hearing aid-like devices that are designed to look like earrings.

j. Indoor positioning systems

The indoor positioning systems (IPS) provide the capability to identify the location of an object or a person inside a building using radio waves, magnetic fields, acoustic signals, or other sensory information.

k. CE devices

The Consumer Electronic devices (DVDs, cameras, TV sets, PVR, game consoles, etc.) most commonly use Ultra Wideband (UWB) communication signals and are part of the Home Automation system.

[31] Azevedo, S. and McEwan, T.E. (1997). Micropower impulse radar. *IEEE Potentials*, 16(2), pp.15-20

[32] Joshi, G. and Kim, S. (2016). A Survey on Node Clustering in Cognitive Radio Wireless Sensor Networks. *Sensors*, 16(9), pp.1465-1484.

[33] Tehrani, K. and Michael, A. (2014). Wearable technology and wearable devices: Everything you need to know. *Wearable Devices Magazine*. [online] Available at: https://www.wearabledevices.com/what-is-a-wearable-device/ [Accessed 18 Nov. 2016].

3.2.3 Network domain

As mentioned in the Device domain description, the M2M Gateway ensures the inter-working and the interconnection between the devices and the communication network. The main part of the M2M Network domain is the communication between the M2M Gateway(s) and the M2M Application domain. The communication is performed either over wired networks (e.g., xDSL and PLC) or wireless networks (e.g., 3G cellular, Wi-Fi and Worldwide Interoperability for Microwave Access - WiMAX). The following list of assets is not exhaustive and includes some of the most common assets in this domain.

a. Communication protocols

The communication protocol is a key-component in the development of ad-hoc and sensor networks, and is often susceptible to various threats and attacks. The communication protocol may have various security vulnerabilities, faults in the code, weak responses, and insecure transport and network layer services.

b. Cooling Systems

Energy efficient and securely operated cooling systems ensure the availability and the proper operations of ad-hoc and sensor networks.

c. Power Supplies

In general, the power supply systems in routers, switches, servers and computers are critical network assets, which are extremely vulnerable to physical attacks or failures.

d. Mobile user and location registers

The mobile user and location registers are used to determine the geographic region, and to inform the nodes about the latest positional information.

e. Radio

Since most ad-hoc and sensor networks are based on wireless communications the radio itself is the medium, hence radio is an asset in Network domain.

f. PKI

Public Key Infrastructure (PKI) is a state-of-the-art mechanism in confidentiality (encryption) and authentication for almost every ad-hoc and sensor network application and communication.

g. Appliance controls

Because of recent advancements in ad-hoc and sensor networks, the users can now easily monitor the services and control remotely the appliances.

h. Addressing servers

The registration and address assignment is important in ad-hoc and sensor networks. They also affect other services and operations, such as routing. An efficient and resilient addressing solution should be employed.

i. Mobile switches

The telecommunication provider in most cases is a cellular network provider. The system of the provider consists of mobile user and location registers, mobile base stations, controllers, etc.

j. PSTN switches

The infrastructure networks usually rely on the core network components and may be built from PSTN backbone switches.

k. *Physical security and control systems*

Physical security is often underestimated and overlooked in the case of ad-hoc and sensor networks. An appropriate plan with the necessary control systems is vital to avoid compromising the sensors in the network.

l. *Routers and switches*

This group of assets is the core of Network domain. The routers, the DSLAMs, the Session Border Controllers (SBCs), and the network switches form the data grid over which the Devices Domain and the Application domain interconnect.

m. *Mobile base stations and controllers*

The Mobile base stations and controllers' topology affects the routing in ad-hoc and sensor networks, and the performance in sensory data exchange. Most of the applications can benefit from the topology of the sensor nodes and the data routing to the other sensor nodes, an external base station, or a controller.

n. *Servers*

The server system that assists the operation of network connectivity is another asset in the Network domain. Important services included in this domain are addressing and DNS naming, private key identification for devices or users, monitoring and administration of network traffic, etc.

o. *WBSNs / WBANs*

The Wireless Body Sensor Networks (WBSNs) or the Body Area Networks (WBANs) are emerging wireless networks of wearable computing devices. In general, this type of networks has interest in applications, such as ehealth, remote measuring of health information, assisting the patients and elderly, home automations, and monitoring human-body changes.

3.2.4 Operational domain

Automating operations, which until recently were manipulated by people, may ensure effectiveness in meeting customer requirements using as few resources as necessary. Some typical examples of the assets involved in this domain are listed below.

a. *Physical security*

The physical security of monitoring and safeguarding access of areas/zones, objects, or people is an operation of ad-hoc and sensor networks. Typical examples include alarm systems, video and camera surveillance applications, etc.

b. *Control systems*

The control systems that give access in buildings, houses or specific areas are assets of ad-hoc and sensor networks operations. One case is the use of smart grid to facilitate the development of appliance control systems. These systems consist[34] of energy storage devices, transmission cables, smart substations and transformers, Advanced Metering Infrastructure (AMI) and Home Area Networks (HANs). In general, these systems are utilized as Home Automation systems (e.g. Heating, Ventilation, and Air-Conditioning -HVAC), building or campus automation systems, etc.

[34] Syal, M.M. and Ofei-Amoh, K. (2013). Smart-grid technologies in housing. *Cityscape: A Journal of Policy Development and Research*, 15(2), pp.283-288.

c. Utilities

These networks may provide automation solutions in cases of measurement, provisioning and billing of water, electricity, oil, heat, etc.

In the following sections, we analyse the attributes and characteristics of several use case types in the abovementioned domains to identify the respective assets. The mapping between these use cases and the assets is also summarized in Annex A.

3.2.5 Product/Business processes domain

Ad-hoc and sensor networks may provide automation solutions for many areas of business organization and operation. Some of the assets in this domain are listed below.

a. Supply and provisioning

This is a high value area for a product-making company and needs to be accomplished in high speed and precision. Sensors and actuators are used to automate processes like freight supply, product packaging etc. Additionally, software in the application domain (e.g. Business Support systems - BSS) provides monitoring and managing abilities to the company's human resources. The vending machines are also common in this area.

b. Manufacturing

In a modern manufacturing environment, the manufacturing systems heavily utilize ad-hoc and sensor network operations to improve the quality of service, manage the manufacturing resources efficiently, and achieve near zero down time operations.

c. Healthcare

In healthcare, various ad-hoc and sensor networks applications are widely used for monitoring and data archiving. These applications should pay great attention to security, due to the data sensitivity and privacy issues. Sensors are often integrated and embedded with health monitoring devices providing real-time or batch-driven data.

d. Transportation

The fleet management issue is important for the business and affects the efficiency of the product distribution, the product cost and the business economics in general. By automating and monitoring the fleet, the emissions, road safety and toll payment, and the business profit are in-all eventually better controlled.

e. Home automation

Recently, the use of ad-hoc and sensor networks in home automation has gained increased attention and several solutions have evolved, such as remote monitoring of electricity, adjusting the water supply, controlling the gas consumption, and managing sensor equipped appliances.

3.3 Use case types

By collecting the information, the ad-hoc and sensor networks for M2M communications threats can be classified, including information on risks, opportunities, threat agents, impact, vulnerabilities, etc. The use cases that have been analysed and studied are based on the most common areas of sensor networks and interest. Due to the large heterogeneity in the type of the devices, their capabilities (i.e. communication, computational), the network domains, and the applications, we need to assess the most representative environments. Several small and inexpensive portable devices can be used for wireless sensor network applications for both military and civilian use. These sensor networks can be used to transfer the captured information to the destination by detecting any available environmental change. For instance, a civilian application can include some type of habitat monitoring, health monitoring and home automation, while the military applications could be used for tracking the enemies and improved efficiency.

We analyse five use cases which are listed below:

1. Ultra-wideband (UWB) communication and applications[35]
2. RFID applications and protocols
3. Mobile cloud computing and mobile social networking
4. Software-defined ad-hoc, and sensor networks
5. Body networks and eHealth

Concerning the UWB transmission technology[36], there have been considerable advancements and innovations recently. UWB includes features[35] that could be exploited in ad-hoc networks[37]. With respect to RFID applications and protocols, a typical example and common practice used in several business cases, products and web-sites is the smart tagging of things. Various forms of contactless communications and technologies can be utilized, such as Near-Field Communication (NFC), Quick-Response (QR) codes, and Bluetooth.

Mobile and cloud computing (MCC) is emerging rapidly, providing various technological, research and business opportunities. MCC technology refers to the mobile devices, mobile computing interfaces, mobile operators and cloud service providers that deliver increased computational resources, capabilities and functionalities to the mobile users. MCC involves mobile communications, mobile hardware, mobile software, cloud and network technologies for utilizing different services, and routing and packet forwarding in heterogeneous and distributed environments.

Software-defined ad-hoc wireless, and sensor networks may include several nodes spread across the area. New nodes may join/leave the networks, and can participate in data processing and forwarding. Based on the capabilities of the nodes, they can provide different communication services (i.e. security, data retention) and speeds. Finally, body networks and eHealth information sharing technologies are used increasingly and extensively to provide or access the data of the objects (i.e. patients, home & elderly care centre monitoring for chronic and elderly patients). The characteristics of these uses cases are presented in the following tables.

[35] Zhuang, W., Shen, X. and Bi, Q. (2003). Ultra-wideband wireless communications. *Wireless Communications and Mobile Computing*, 3(6), pp.663-685.

[36] Cuomo, F., Martello, C., Baiocchi, A. (2002). Radio Resource Sharing for Ad-hoc Networking With UWB. *IEEE Journal on Selected Areas in Communications*, 20(9), pp.1722-1732.

[37] Chong, C.C., Watanabe, F., Inamura, H. (2006). *Potential of UWB Technology for the Next Generation Wireless Communications.* IEEE Ninth International Symposium on Spread Spectrum Techniques and Applications, 28-31 Aug, Manaus-Amazon, Brazil, pp.422-429.

1.Ultra Wideband (UWB) communication and applications	
1.1 Characteristics	Extremely low transmission energy (less than 1mW)
	Very high bandwidth within short range (200Mbps within 10m)
	Extremely difficult to intercept, because the frequency is constantly shifting
	The short duration of the UWB pulses lead to multipath immunity (i.e. the propagation path can be discovered due to the fine time resolution)
	Radar, Geo-location / Positioning
1.2 Applications	Wireless Personal Area Networks (WPAN)
	Positioning, geo-location, localization, rescue applications
	Radar / Sensor: MIR (motion detector, range-finder, etc.)
	Military and commercial: Asset protection
	Anti-terrorist, search-and-rescue activities, law enforcement and emergency rescue organizations
1.3 Guidelines, strategies and standardization	IEEE 802.15: WPAN
	IEEE 802.15.1: Bluetooth, 1Mbps
	IEEE 802.15.3: WPAN/high rate, 50Mbps
	IEEE 802.15.3a: WPAN/Higher rate, 200Mbps, UWB
1.4 Advantages	Easier to achieve higher data rate, because of the shorter duration of the UWB pulses
	Less path loss and better immunity to multipath propagation
	Availability of low-cost transceivers
	Low transmit power and low interference
	Extensive command set of the IEEE 802.15.4 (standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs)). FCC approved wireless protocol, supports communications with multiple devices, very fast communications.
1.5 Problems/issues to-be considered	Distortion of the received waveform from each distinct delayed propagation path, which makes it difficult to explore path diversity inherent in the received signal
	Synchronization of very short pulses at the receiver
	Performance degradation due to multiple access interference and narrowband jamming
	Employing higher order modulation schemes to improve capacity or throughput
	Development of link and network layers to take advantage of the UWB transmission benefits at the physical layer

Table 1. Ultra Wideband (UWB) communication and applications

2.Radio Frequency Identification (RFID)	
2.1 Characteristics	Low frequency (less than 100 MHz) and high frequency (greater than 100 MHz) modes
	High-frequency tags can have their data read at distances greater than one meter
	New data can also be transmitted to the tags, a process not shown here[38]
2.2 Applications	Low/high frequency systems
	Supply chain and automated libraries
	Transport payment
	Automotive security
	Healthcare (e.g. track assets, monitor patients, automate payments)
2.3 Guidelines, strategies and standardization	ISO 11784: Data structure on the tag
	ISO 11785: Air interface protocol
	ISO 14443: Air interface protocol for RFID tags in payment systems & contactless smart cards
	ISO 15693: Air interface protocol for RFID tags in vicinity cards
	ISO 18046 & 18047: Testing the conformance of RFID tags and readers[39]
2.4 Advantages	No line of sight (NLOS)
	Work in harsh environment (e.g. high temperatures)
	Cost effectiveness & high efficiency
	Reliable and fast identification of mobile tags in RFID networks
	Fast and energy efficient multi-sensor data retrieval approaches
2.5 Problems/issues to-be considered	Large volumes of data & product information maintenance
	Configuration and management of readers and devices
	Data integration across multiple facilities
	Data ownership and partner data integration
	Data security and personal privacy[40] (e.g. patient *privacy* and dignity)

Table 2. Radio Frequency Identification (RFID)

[38] Want, R. (2004). RFID: A key to automating everything. *Scientific American*, 290(1), pp.56-65.

[39] RFID Journal. (2005). *A Summary of RFID Standards*. [online] http://www.rfidjournal.com. Available at: http://www.rfidjournal.com/articles/view?1335 [Accessed 18 Nov. 2016].

[40] van Lieshout, M., Grossi, L., Spinelli, G., Helmus, S., Kool, L., Pennings, L., Stap, R., Veugen, T., van der Waaij, B. and Borean, C. (2007). RFID technologies: Emerging issues, challenges and policy options. I. Maghiros, P. Rotter and M. v. Lieshout. Luxembourg, *European Commission, Directorate-General Joint Research Centre, Institute for Prospective Technological Studies*, pp. 40

3.Mobile Cloud Computing and Mobile Social Networking	
3.1 Characteristics	On-demand self-service (cloud computing users to manage their own virtual resources)
	Broad network and heterogeneous access
	Resource pooling; information can be shared with multiple users, who can access the resources anytime
	Rapid elasticity; the cloud must be able to scale up and down as load demands for IoT usage
	Measured service; subscription based or pay per use services
3.2 Applications	Web-browsing & web-mail
	Secure enterprise social networks that connects your business processes, enterprise applications, and content
	Augment reality; connect all objects through the Internet for remote sensing and control
	HD video streaming (e.g. cloud-based live video broadcasting network)
3.3 Guidelines, strategies and standardization	DTMF OGF GFD.183[41], DTMF OGF GFD.184[42]
	European cloud strategy[43], European data infrastructure[44]
	SNIA Cloud Data Management Interface (CDMI)[45]
	Federal Information Process Standards Publication (FIPS), standards for security categorization of federal information and information systems[46] for effective management and oversight of information security and consistent reporting on the adequacy and effectiveness of information security policies, procedures, and practices
	ISO/IEC 17788:2014[47], ISO/IEC 17789:2014[48],

[41] DTMF OGF GFD.183. (2011). *Open Cloud Computing Interface-Core.* [online] Available at: http://ogf.org/documents/GFD.183.pdf [Accessed 18 Nov. 2016]

[42] DTMF OGF GFD.184. (2011). *Open Cloud Computing Interface-Core.* [online] Available at: http://ogf.org/documents/GFD.184.pdf [Accessed 18 Nov. 2016]

[43] COM (2012) 529 Final, European Cloud Strategy. (2012). *Unleashing the Potential of Cloud Computing in Europe.* [online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF [Accessed 18 Nov. 2016]

[44] European Data Infrastructure glossary. [online] Available at: http://ec.europa.eu/digital-single-market/en/glossary#europeandatainfrastructure [Accessed 18 Nov. 2016]

[45] ISO/IEC 17826. (2012). *Information technology -- Cloud Data Management Interface (CDMI).* [online] Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=60617 [Accessed 18 Nov. 2016]

[46] Federal Information Process Standards Publication (FIPS) (2004). *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.* [online] Available at: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [Accessed 18 Nov. 2016]

[47] ISO/IEC 17788:2014. (2014). *Information technology -- Cloud computing -- Overview and vocabulary.* [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60544 [Accessed 18 Nov. 2016]

[48] ISO/IEC 17789:2014 (2014). *Information technology -- Cloud computing -- Reference architecture.* [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60545 [Accessed 18 Nov. 2016]

3.Mobile Cloud Computing and Mobile Social Networking	
	ISO/IEC 17826:2012[49], ISO/IEC DIS 19086-1[50], ISO/IEC DIS NP 19086-2[51], ISO/IEC DIS CD 19086-3[52], ISO/IEC DIS NP 19086-4[53], ISO/IEC AWI 19941[54], ISO/IEC WD 19944[55], ISO/IEC AWI 20889[56], ETSI Cloud Computing standards and Open Source[57], IEEE - P2301[58]/P2302[59]/ P2303[60], Open group - G135/ C141[61]
3.4 Advantages	Flexibility; access the data from anywhere in the world, using any mobile device
	Scalability; ever-changing technology landscape

[49] ISO/IEC 17826:2016 (2016). *Information technology -- Cloud Data Management Interface (CDMI)* [online] Available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=70226 [Accessed 18 Nov. 2016]

[50] ISO/IEC DIS 19086-1 (2016). *Information technology -- Cloud computing -- Service level agreement (SLA) framework - Part 1: Overview and concepts.* [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67545 [Accessed 18 Nov. 2016]

[51] ISO/IEC DIS NP 19086-2 (2016). *Information technology -- Cloud computing -- Service level agreement (SLA) framework and technology - Part 2: Metrics.* [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67546 [Accessed 18 Nov. 2016]

[52] ISO/IEC DIS CD 19086-3 (2016). *Information technology -- Cloud computing -- Service level agreement (SLA) framework - Part 3: Core conformance requirements*. [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67547 [Accessed 18 Nov. 2016]

[53] ISO/IEC DIS NP 19086-4 (2016). *Information technology -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 4: Security and privacy.* [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242 [Accessed 18 Nov. 2016]

[54] ISO/IEC AWI 19941 (2016). *Information technology Cloud Computing Interoperability and portability*. [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66639 [Accessed 18 Nov. 2016]

[55] ISO/IEC WD 19944 (2016). *Information technology -- Cloud computing -- Cloud services and devices: data flow, data categories and data use.* [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66674 [Accessed 18 Nov. 2016]

[56] ISO/IEC AWI 20889 (2015). *Information technology -- Security techniques -- Privacy enhancing data de-identification techniques*. [online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=69373 [Accessed 18 Nov. 2016]

[57] ETSI SR 003 382 V2.1.1 (2016-02). *ETSI Cloud Computing standards and Open Source*. [online] Available at: http://csc.etsi.org/resources/WP2-Report/Special_Report_033382-v2.1.1.pdf [Accessed 18 Nov. 2016]

[58] IEEE - P2301 project. *Guide for Cloud Portability and Interoperability Profiles (CPIP).* [online] Available at: https://standards.ieee.org/develop/project/2301.html [Accessed 18 Nov. 2016]

[59] IEEE - P2302 project. *Standard for Intercloud Interoperability and Federation (SIIF).* [online] Available at: https://standards.ieee.org/develop/project/23021.html [Accessed 18 Nov. 2016]

[60] IEEE - P2303 project. *Standard for Adaptive Management of Cloud Computing Environments.* [online] Available at: http://standards.ieee.org/develop/project/2303.html [Accessed 18 Nov. 2016]

[61] Open group - G135/C141. *Cloud Computing Portability and Interoperability*. [online] Available at: https://www2.opengroup.org/ogsys/catalog/G135 [Accessed 18 Nov. 2016]

3.Mobile Cloud Computing and Mobile Social Networking	
	Real time data availability; get access to real time data, whenever you want and wherever you want
	Multiple platforms; various platforms to access the data and applications stored in the cloud
	Increased resource availability, enhanced security and reliability, reduced long WAN latency, increased low-cost resources, green computing, streamlined work flow, ease of use and access
3.5 Problems/issues to-be considered	Security
	Performance
	No offline usability
	Connectivity

Table 3. Mobile Cloud Computing and Mobile Social Networking

4.Software-defined ad-hoc and sensor networks	
4.1 Characteristics	Dynamic topologies, fixed nodes
	Bandwidth-constrained, variable capacity links
	Resources & energy-constrained
	Limited physical security, security threats
4.2 Applications	Virtual navigation, Location-aware services
	Tele-medicine, tele-geo processing
	VAN, PAN, home and enterprise networking[14], tactical networks, sensor networks[62]
	Military applications, crisis-management applications, emergency services
	Educational applications, entertainment
4.3 Guidelines, strategies and standardization	IEEE 802.11 Family
	IEEE 802.15: WPAN IEEE 802.15.1: Bluetooth IEEE 802.15.3: WPAN/high rate, 50Mbps IEEE 802.15.3a: WPAN/Higher rate, 200Mbps, UWB IEEE 802.15.4: WPAN/low-rate, low-power, mW level, 200kbps[63]
	IEEE 802.16
	IEEE 802.20
	IEEE 1451
4.4 Advantages	Less cost, bigger and faster wireless networks
	Rely on same Wi-Fi standards
	Convenient where Ethernet connections fail, useful for Non-Line-of-Sight network configurations
	Allows local networks to run faster
	Adaptable networks, Self-configuring, Self-healing
4.5 Problems/issues to-be considered	Unstable data links, node cooperation, quality of service, scalability, limited wireless transmission range, packet losses due to transmission errors, Transport layer protocol performance
	Limited processing power, energy conservation
	Security, broadcast nature of the wireless medium, multicasting
	Interoperation with the Internet, client server model shift, pricing scheme
	Mobility-induced route changes, mobility-induced packet losses, potentially frequent network partitions

Table 4. Software-defined ad-hoc and sensor networks

[62] Ad-hoc Network Lecture. [online] Available at: http://www.slideshare.net/cprakash2011/lecture-5-6-ad-hoc-network [Accessed 18 Nov. 2016]

[63] Kim, Y.M. (2003). *Ultra Wide Band (UWB) Technology and Applications*. Presentation by NEST Group in the Ohio State University.

5.Body Networks and eHealth Applications	
5.1 Characteristics	Completeness
	Integrity
	Accessibility
	Availability[39]
5.2 Applications	Various telemedicine (remote diagnosis), electronic stethoscopes, Scientific and industrial applications (i.e. in medical imaging), applications of body network and eHealth[64]
	Teaching applications are in use with different purposes, medical monitors, medical laboratory equipment
	Nuclear medicine with medical devices and wearable sensor-based systems
	Therapeutic: physical therapy machines like continuous passive range of motion (CPM) machine, Treatment equipment includes infusion pumps, medical lasers and LASIK surgical machines
	Life support equipment is used to maintain a patient's bodily function
5.3 Guidelines, strategies and standardization	HL7 MLLP, HITRUST CSF
	EU Directive 2011/24/EU[65] (article 14), Regulation (EC) No 883/2004[66]
	Guidelines on minimum/non-exhaustive patient summary dataset[67]
	National responsible authorities on eHealth (2011/890/EU)[68]
	ISO/TR 28380 "Health Informatics – IHE Global Standards Adoption", ISO 27000, ISO 27799:2008 Health Informatics, ISO 80001[69]
5.4 Advantages	Employers reduce health care costs; Health care organizations use eHealth to reach a large part of the population cost effectively
	Providers face eHealth as an opportunity to improve efficiency, reduce administrative costs, facilitate communication, enhance patient care
	Improved relationship between patients and insurance companies
	Systems availability

[64] ENISA (2015). *Security and Resilience in eHealth Infrastructures and Services*. [online] Available at: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services [Accessed 18 Nov. 2016]

[65] EU Directive 2011/24/EU. (2011). *Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare.* [online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF [Accessed 18 Nov. 2016]

[66] Regulation (EC) No 883/2004. (2004). *Regulation of the European Parliament and of the Council on the coordination of social security systems*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02004R0883-20140101&from=EN [Accessed 18 Nov. 2016]

[67] EU guidelines (2013). *Guidelines on minimum/non-exhaustive patient summary dataset*. [online] Available at: http://ec.europa.eu/health/ehealth/docs/guidelines_patient_summary_en.pdf [Accessed 18 Nov. 2016]

[68] Commission implementing decision. (2011). *Rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth*. [online] Available at: http://ec.europa.eu/health/ehealth/docs/decision_ehealth_network_en.pdf [Accessed 18 Nov. 2016]

[69] ISO/IEC 80001. (2016). *Application of risk management for IT-networks incorporating medical devices*. [online] Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863 [Accessed 18 Nov. 2016]

5.Body Networks and eHealth Applications	
5.5 Problems/issues to-be considered	Lack of interoperability, cross-border incidents and incident management
	Access control and authentication
	Data integrity, network security, data loss, security expertise and awareness
	Standardisation, compliance, trust, and sensitiveness of data handled

Table 5. Body Networks and eHealth Applications

4. Threats Taxonomy

Threat taxonomy is a classification of threat types and threat groups at various levels of detail. The purpose of such a taxonomy is to establish a point of reference for the encountered threats, while providing a possibility to shuffle, arrange, amend and detail threat definitions. Therefore, a threat taxonomy is dynamic and should be used to maintain a consistent view on threats based on the collected information.

The current threat mind map (Figure 6) is based on the ENISA Threat Taxonomy[70], which has collected and combined numerous threats from various sources into a unified and united threat catalogue. During the ENISA Threat classification exercise, several other existing threat catalogues were analysed to consolidate the security and risk management information.

In the current study, we have also considered threats in the fields of *operational and product/business processes* domains to extend the ENISA's work which focused in physical threats, information security, and cyber-space areas

A detailed presentation of the threats taxonomy in ad-hoc wireless and sensor networking is provided in Annex B.

[70] European Union Agency for Network and Information Security (ENISA). (2016). *Threat Taxonomy - A tool for structuring threat information*. [online] Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information [Accessed 18 Nov. 2016]

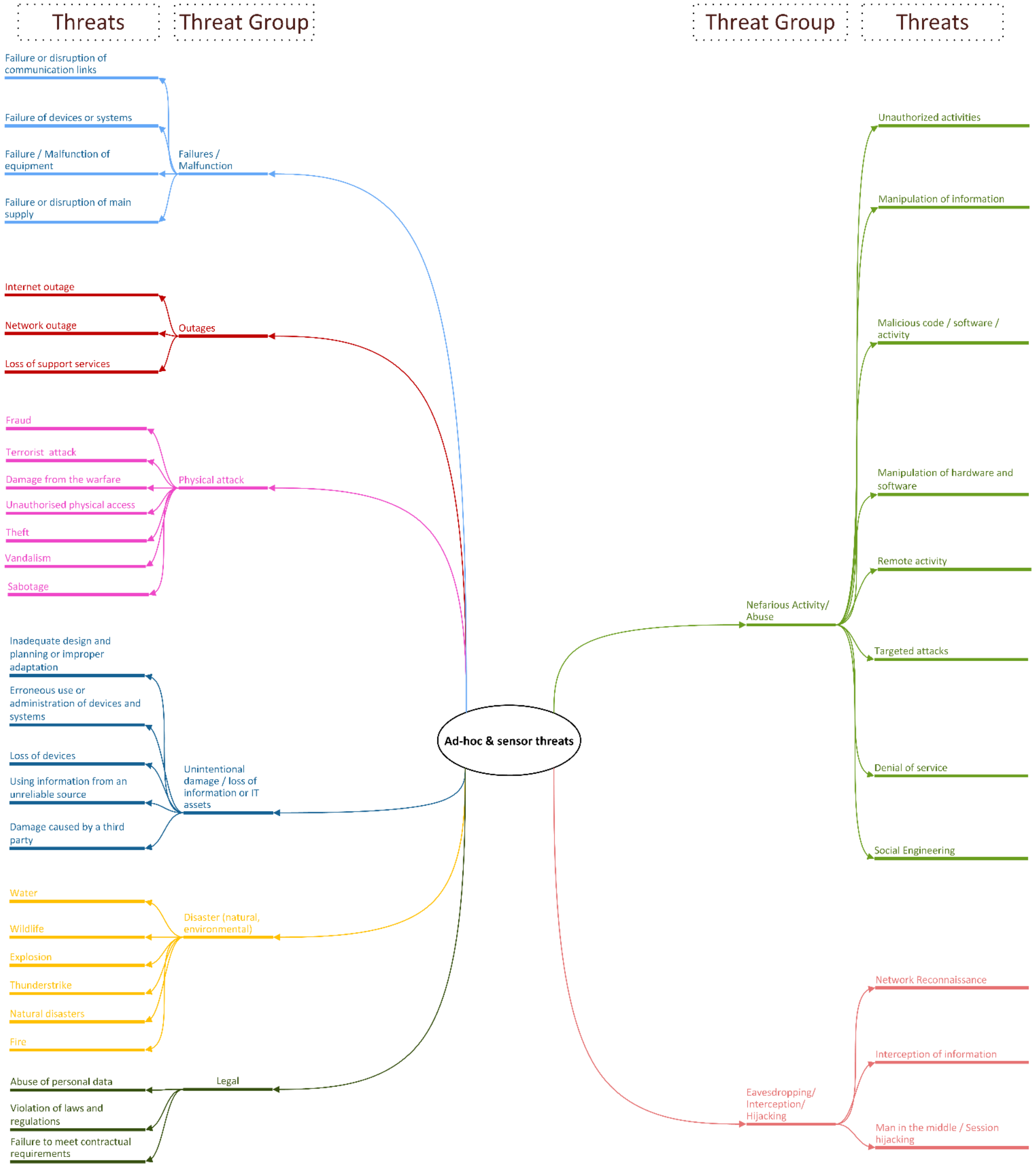

Threats
Threat Group
Threat Group
Threats
Failure or disruption of communication links
Failure of devices or systems
Failure / Malfunction of equipment
Failure or disruption of main supply
Failures / Malfunction
Internet outage
Network outage
Loss of support services
Outages
Fraud
Terrorist attack
Damage from the warfare
Unauthorised physical access
Theft
Vandalism
Sabotage
Physical attack
Inadequate design and planning or improper adaptation
Erroneous use or administration of devices and systems
Loss of devices
Using information from an unreliable source
Damage caused by a third party
Unintentional damage / loss of information or IT assets
Water
Wildlife
Explosion
Thunderstrike
Natural disasters
Fire
Disaster (natural, environmental)
Abuse of personal data
Violation of laws and regulations
Failure to meet contractual requirements
Legal
Ad-hoc & sensor threats
Nefarious Activity/ Abuse
Unauthorized activities
Manipulation of information
Malicious code / software / activity
Manipulation of hardware and software
Remote activity
Targeted attacks
Denial of service
Social Engineering
Eavesdropping/ Interception/ Hijacking
Network Reconnaissance
Interception of information
Man in the middle / Session hijacking

Figure 6 Threats taxonomy

5. Mapping Threats to Assets

According to the ENISA Glossary[71], a threat is *"any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service"*.

Based on the identified assets, a taxonomy of relevant threats impeding the ad-hoc sensor networks or at least significant parts is developed.

Since this study focuses on information security, the presented threat taxonomy mainly covers cyber security threats. However, for a faultless operation, physical assets are also required and, therefore, several specific non-IT threats are assumed.

A full taxonomy map of ad-hoc and sensor network threats is shown in Annex B. The taxonomy of threats is based on the first and second level categorization suggested by the ENISA Threat Taxonomy 2013-2015[70]. In the following sections, a short description of the most popular threats is presented.

5.1 Threat Group: Unintentional damage / loss of information or IT assets

The following group of threats refers to those damages or loss of information caused by human errors in the administration of systems or misconfiguration of systems. Additionally, these damages may be caused by an unintentional intervention or by the actual loss of devices or of part of them.

5.1.1 Threat: Inadequate design and planning improper adaptation

The scope of planning and designing sensor networks is the better area coverage in a way that permits the unblocked access between the end users (e.g. an application, a business process) and the primary data which are collected from the monitored or controlled area[72]. Any error or lack of consideration in the design could cause low availability or downtime and resource consumption.

Ad-hoc networks constantly change architecture, due to the node mobility. Their communication basis is the transmission between neighbouring nodes[73]. The lack of proper design could lead to network instability and resource over-consumption in every change of the number of participants (nodes).

The fact that the ad-hoc and sensor network assets have limited or no computational abilities and low resources is one factor of their behaviour. Another factor is that the environment or the area targeted to be monitored in each case, could be hostile, open to unattended or unauthorized access, constantly changing (due to mobility) and geographically wide[28] an inadequate design could result to the improper or insufficient area coverage, to assets' miscommunication or to assets' resource exhaustion, trying to overcome design problems.

[71] European Union Agency for Network and Information Security (ENISA). (2016). *Glossary — ENISA*. [online] Available at: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary [Accessed 18 Nov. 2016].

[72] Raza, M., Kumar, V.P., Nafareih, A. and Robertson, W. (2016). An Analysis of the Effects of Network Implementation Choices on Healthcare Applications. *Procedia Computer Science*, 94, pp.318-323.

[73] Srtist, N. (2016). Self-Stabilized FRCA using connected dominating set for Wireless Mobile Ad-hoc Sensor Networks. *Journal of Theoretical and Applied Information Technology*, 90(1), pp.67-76.

The data collected and transmitted in these networks are of high value and sensitivity (e.g. Private Healthcare Information - PHI). However, the low computational power of assets makes it difficult or impossible to protect the data and the data transmission itself. A method of data protection through encryption and decryption, though affective, is highly demanding in computing resources. An inadequate design of how this problem will be overcome may permit information to be compromised[74].

Further to the above, the lack of planning or the existence of a design error may allow the existence of software (Applications) that do not take under consideration the devices power and computing limitations[28] with software update (i.e. cars and other devices).

Assets targeted by this threat group are those from the ***Device Domain*** and the asset ***Data*** in the ***Application Domain***.

5.1.2 Threat: Using information from an unreliable source

Any system or device with computational power and an operating system (OS) is vulnerable to OS exploits. This threat occurs mainly due to the vulnerable versions of preinstalled software used in corporate environments. In most cases, *third-party applications* can be installed and activated in the devices, posing potential risks to the enterprise. These applications may hide various software faults, security bugs, vulnerabilities, and coding errors that can be exploited to an adversary under certain conditions. This is an unintentional threat, because the software and the applications risks could exist by design.

As reported in the IBM X-Force Threat Intelligence Report[75], the cybercrime events show an increasing interest in personally identifiable information (PII) and high-value data (e.g. health-records) since 2014. Besides, in the case of business-critical applications (e.g. billing, e-Health), sensitive and personal may traverse ad-hoc and sensor networks. Therefore, these networks are susceptible to attacks and malicious activities.

All the assets in ***all Domains*** can be a target for this threat.

5.1.3 Threat: Erroneous use or administration of devices and systems

The Application Programming Interfaces (APIs)[76] are software elements, which are used by software developers in their attempt to construct applications or graphical user interfaces. Cloud service providers utilise APIs to allow access to cloud-based services[77]. The APIs can be used by several devices and applications simultaneously for various purposes. However, it is difficult to determine who should or should not be granted access[78]. Since an API is a public library, the unauthorized access and nefarious use of the APIs content cannot be prevented easily. It should be noted that via this access, any data, system or service of the network becomes vulnerable.

[74] Zhou, F.S.X.D.Y. (2016). A Key Management and Cross-layer Routing Scheme for Wireless Sensor Networks. *International Journal of Security and Its Applications*, 10(7), pp.119-134.

[75] IBM. (2016). *IBM X-Force Threat Intelligence Report 2016*. IBM Security. [online] Available at: http://www-03.ibm.com/security/xforce/downloads.html [Accessed 18 Nov. 2016].

[76] Monperrus, M., Eichberg, M., Tekes, E. and Mezini, M. (2011). What should developers be aware of? An empirical study on the directives of API documentation. *Empirical Software Engineering*, 17(6), pp.703-737.

[77] Saini, B. (2016). Understanding Cloud Computing Service Model and Security Issues in IaaS. *International Journal of Trend in Research and Development*, 3(2), pp.615-617.

[78] Stevens, R., Crussell, J. and Chen, H. (2016). *On the Origin of Mobile Apps: Network Provenance for Android Applications*. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, 9-11 Sep, New Orleans, LA, pp. 160-171.

In the case of the permissions API, which contains information and access information for systems within the network, the adversary may perform an unauthorized manipulation of the API, and use erroneously the devices and systems.

All assets in ***all Domains*** can be a target for this threat.

5.1.4 Threat: Loss of devices

In ad-hoc and sensor networks, the threat of physically losing devices can affect the stability of the network. In most cases, the areas that sensor networks are designed to cover are geographically wide. As the risk is considerably high, this leads to the use of a big number[79] of devices to achieve a sufficient coverage of the area. These areas (e.g. underwater, underground, terrestrial, etc.)[80] could also provide open access to anyone. Moreover, the network's nodes are mostly devices with small size[79]; this characteristic makes them vulnerable to robbery incidents.

Further in ad-hoc networks, the covered area is undetermined and may change in real-time[81]. The number of devices is also changing constantly. In addition to the above, the nodes usually are small devices (e.g. smartphone, smart-card, RFID, etc.), which are easy to be stolen containing sensitive or personal information.

These characteristics make the ad-hoc and sensor networks and, more specifically, the assets in the ***Device Domain*** vulnerable to Loss of Devices threat.

5.1.5 Threat: Damage caused by a third party

A *malware* is a hostile fragment of programming code that targets sensitive information inside a system. For instance, the term *information-stealing mobile malware* describes the malware which is remotely accessing a system and is focused in gathering information when installed with the main purpose of targeted advertisement.

Data leakage[82] is the illegitimate outcome produced by a third-party application which is focused on gathering personal information due to the existence of critical vulnerabilities or integrated backdoors on the source code of the applications. Consequently, the information is then used without the owner's permission for several malicious activities such as the exposition to the *black market*[83]. The data in question is related to the customer's market profile.

Asset targeted by this threat is ***Data Domain*** from the ***Application Domain***.

[79] Mahdavi, M. and Ismail, M. (2016). Rescheduling of Nodes Duty Cycles to Prevent Partitioning in Wireless Sensor Networks. *Bulletin de la Société Royale des Sciences de Liège*, 85, pp.418-423.

[80] Basit, S.A. and Kumar, M. (2015). A Review of Routing Protocols for Underwater Wireless Sensor Networks. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(12), pp.373-378.

[81] Sarika, S., Pravin, A., Vijayakumar, A. and Selvamani, K. (2016). Security Issues in Mobile Ad Hoc Networks. *Procedia Computer Science*, 92, pp.329-335.

[82] Gordon, P. (2007). *Data Leakage-Threats and Mitigation*. Information Security Reading Room. SANS Institute.

[83] Gartner, (2016). *Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of Internet of Things.* [online] Available at: http://www.gartner.com/newsroom/id/3185623 [Accessed 18 Nov. 2016].

5.2 Threat Group: Disaster (natural, environmental)

Natural and environmental disasters cause severe large-scale network and service disruptions, and have on average the greatest impact of all system failures[84]. The recovery and restoration of the services take the longest time; in 2014 the recovery time lasted 81 hours[85], while in 2013 it was more than 50 hours[84]. Taking into consideration the great exposure to the numerous users and habitants, this depicts that disasters not only last long, but also, they are the most difficult to manage.

Nowadays, we witness an increased number of interlinked sensors, integrated into the infrastructure and buildings, and incorporated in various systems and services. These sensors can be monitored and controlled by various means (i.e. smart phones, workstations over the internet), and they reveal behavioural patterns of the monitored objects[86]. Thus, it is critical to ensure the data integrity and the service operations of WSNs against any natural or environmental disaster. In the ad-hoc wireless and sensor networks, the nodes in the infrastructure are often fixed, and in several cases WSNs are utilized in monitoring and security services (i.e. monitor human activities and the environment like climate control, gather data for medical diagnostics, transport critical-mission data and confidential measurements, provide the location information to the corresponding receiver). Still, the WSNs are also used by weather, emergency response and disaster management systems for immediate inference upon network and service disruptions[87]. The sensory measurements are collected on a regular basis by spatially dispersed networks distributed over a certain region. Thus, WSNs can enhance the surveillance and awareness of any status changes in disaster responses[88], and prevent massive destructions from natural or environmental disasters.

Nevertheless, the WSNs are susceptible to many natural or environmental disasters, as any other IT component or network. They are vulnerable to the power failures and cuts, communication problems and delays, jamming and channel errors, hardware problems, physical damage, insecure routing, and failures in data aggregation.

Assessing the impact of natural and environmental disasters is of paramount importance and will facilitate to identify the factors and methods that can contribute to reduce WSNs damage and service disruptions after natural disasters occur.

Assets targeted by this threat include the assets from the ***Device domain***, the ***Network domain*** and the assets ***Control Systems***, ***Physical Security***, ***Vending Machines*** and ***Road Safety***.

[84] Karsberg, C., Skouloudi, C. and Dekker, D. (2013). *Annual Incident Reports 2013*. European Union Agency for Network and Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/annual-incident-reports-2013/at_download/fullReport [Accessed 18 Nov. 2016].

[85] Karsberg, C., and Skouloudi, C. (2014). *Annual Incident Reports 2014*. European Union Agency for Network and Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/annual-incident-reports-2014/at_download/fullReport [Accessed 18 Nov. 2016].

[86] Barnard-Wills, D., Marinos, L., Portesi S. (2014). *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*. Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence/at_download/fullReport [Accessed 18 Nov. 2016].

[87] Erjongmanee, S., Ji, C., Stokely, J., and Hightower, N. (2008*). Inference of Network-Service Disruption upon Natural Disasters*. Knowledge Discovery from Sensor Data, Second International Workshop, Sensor-KDD 2008.24-27 Aug, Las Vegas, NV, USA.

[88] Mangla, A., Bindal, A.K., Prasad, D. (2016). Disaster management in wireless sensor networks: A survey report. *International Journal of Computing and Corporate Research*, 6(3). In Press.

5.3 Threat Group: Legal

This group includes threats due to the legal implications such as the violation of laws or regulations, the breach of legislation, the failure to meet contractual requirements, the unauthorized use of Intellectual Property (IPR) resources, the abuse of personal data, and the necessity to obey judiciary decisions and court orders.

5.3.1 Threat: Abuse of personal data

The incorporation of Wireless Body Sensor Networks (WBSNs), Personalized Portable Devices (PPDs) and Wireless Body Area Networks (WBANs) in the healthcare sector to optimize the quality of medical services and the treatment of patients introduce several privacy and ethics issues. These issues are highly associated with the eHealth and pHealth sensors' attack surface. The ad-hoc and wireless network sensors may encounter harsh and anomalous physiological conditions in the remote monitoring, which require the continuous supervision to provide intensive care. The operations and the concentration of data by the medical sensors such as in the case of the cardio net system[89], should be managed by the doctors and nursery. Upon receiving the data, the sensors dispatch the data to the back-end server for processing by using a short-range wireless network. However, during this process, the WBANs are threatened mainly by exhausting attacks, which are namely: *(a)* the collision attacks, *(b)* the denial of sleep attacks and *(c)* the selfish attacks [90].

In the field of Mobile Healthcare Networks (MHNs), where wearable sensor devices communicate based on the device-to-device (D2D) concept, the protection of the personal data plays a significant role. Hence, if the personal data (e.g. patient's daily health data) is processed in the Cloud, it should be protected from being accessed by unauthorized parties, e.g. insurance company or a mobile intruder who can disseminate health records through an Online Social Network. By that means, the Quality of Privacy (QoP) is of great importance[91].

Sensitive banking information can be maliciously retrieved in the case of near field communication (NFC) cards. The attacker can utilize NFC radio waves and then access to data stored on the victim's card[92].

Furthermore, social engineering fraud can also be a way to abuse personal data in ad-hoc or mobile networks[93].

The assets targeted by these threats include the asset groups ***Applications Domain*** and ***Device Domain*** and the assets ***Physical Security***, ***Supply and Provisioning*** and ***Healthcare***.

5.3.2 Threat: Failure to meet contractual requirements

Failure to meet contractual requirements, or break a contractual one could result to security incidents.

[89] European Telecommunications Standards Institute (ETSI). (2013). *ETSI TR 102 732, Machine to Machine Communications (M2M): Use cases of M2M applications for eHealth*. [online] Available at: http://www.etsi.org/deliver/etsi_tr/102700_102799/102732/01.01.01_60/tr_102732v010101p.pdf [Accessed 10 Oct. 2016].

[90] Jo, M., Han, L., Tan, N.D. and In, H.P. (2015). A survey: energy exhausting attacks in MAC protocols in WBANs. Springer, *Telecommunication Systems*, 58(2), pp.153-164.

[91] Zhang, K. and Shen, X. (2015). Security and Privacy Challenges in MHN. *In: Security and Privacy for Mobile Healthcare Networks*, pp.11-20. Springer International Publishing: Switzerland.

[92] Madhoun, N., Guenane, F. and Pujolle, G. (2016). *An online security protocol for NFC payment: Formally analysed by the scyther tool.* 2016 2nd IEEE International Conference on Mobile and Secure Services (MobiSecServ), 26-27 Feb., Gainesville, USA, pp.1-7.

[93] Richards et al., (2016). *Mobile Payment Verification System for Socially Engineering Fraud.* US2016/00944290A1.

All assets in ***all Domains*** can be a target for this threat.

5.3.3 Threat: Violation of rules and regulations

The vast diaspora of deployed applications within the ad-hoc and sensor networking ecosystem highlights the need for complying with the rules and regulations that rely on these applications as well on the society's well-being. Stakeholders prone to break the rules are[94] *(a)* the operators (i.e. which have a direct link with physical infrastructure) and *(b)* the digital service providers (which have a cross border nature).

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain***, ***Network Domain***, ***Operational Domain*** and ***Product/business processes Domain***.

5.4 Threat Group: Outages

Due to the nature of the ad-hoc wireless and sensor networks, specific constraints exist. Apart from the limited storage capacity and computational costs[95], energy consumption is among the critical success factors and important constraints for ad-hoc and sensor networks.

5.4.1 Threat: Internet outage

We should not underestimate the great importance of evidence of *internet outage* reports and incidents, as nowadays heavily internet-dependent businesses rely extensively on the Internet services, and, thus, any Internet outage is likely to hit business operations severely. Even though most businesses have defined the processes and the countermeasures to respond to internet outages, there are still several complex dependencies, capacity issues, performance delays, and business continuity risks in the case of internet failures[96]. The internet outage can be caused by numerous factors either accidentally or intentionally; human errors, problematic and erroneous maintenance works, BGP misconfiguration and massive route leaks[97], failed international cable affecting mobile and data domestic operations, and cyberspace dangers and cyberattacks[98,99] result in Internet blackouts or brownouts. Not only the service disruptions damage the brand of the service provider, but they also create several business implications and frustration to the users[100].

[94] Weber, R. and Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*. In Press.

[95] Rajkumar, Salehi, A., Chandrakanth, D. (2013). *Detection of Sinkhole Attack in Wireless Sensor Networks*. IEEE International Conference on Space Science and Communication (IconSpace2013), 1-3 Jul, Melaka, Malaysia, pp.361-365.

[96] InfoSecurity Magazine. *Comment: Total Internet Failure – When Online Goes Offline*. [online] Available at: http://www.infosecurity-magazine.com/magazine-features/comment-total-internet-failure-when-online-goes/ [Accessed 18 Nov. 2016].

[97] BGPMON. *Massive route leak causes Internet*. [online] Available at: http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/ [Accessed 18 Nov. 2016].

[98] The Wall Street Journal. *NATO-Linked Websites Go Down, Cyberattack Suspected*. [online] Available at: http://www.wsj.com/articles/nato-linked-websites-go-down-cyberattack-suspected-1468001918 [Accessed 18 Nov. 2016].

[99] Reuters. *HSBC says internet banking services down after cyber-attack* [online] Available at: http://www.reuters.com/article/us-hsbc-cyber-idUSKCN0V71BO [Accessed 18 Nov. 2016].

[100] ABC News. *Telstra outage: Company apologises for internet service disruption.* [online] Available at: http://www.abc.net.au/news/2016-05-29/telstra-apologises-for-internet-outage-with-$25-credit-customers/7456832 [Accessed 18 Nov. 2016].

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain***, ***Network Domain***, ***Operational Domain*** and ***Product/business processes Domain***.

5.4.2 Threat: Network outage

An attacker may try to deplete the network infrastructure and service resources by submitting illegitimate requests, until the maximum limit is reached. This results in service outage and disruptions, as no further legitimate request can receive any further resource. By injecting invalid requests, the resources are exhausted and this raises denial of service attacks.

A common example of network outage is the *outage of cable networks*. If the power or network cables are unprotected, they can be damaged accidentally or intentionally. Often, the cables are pulled out by the staff as they stumble over them, unauthorized personnel (i.e. cleaning services) unplug the cable and plug the loose end into an empty "hole" that seems to fit, or the cable connection is abruptly terminated (i.e. a ship's anchor accidentally slices internet cables[101]). The unavailability and *loss of support services* essential for proper operation of the information system and the business processes are often causing disruptions and outages.

Intermittent problems and *outages in a wireless networks* environment are also likely due to technical exploits and vulnerabilities (i.e. IEEE 802.11 and IEEE 802.15 families). In the case of *outages of mobile networks*, aside from the communication problems with the networks (i.e. 3G, GSM, LTE, satellite links), several operational and business issues can arise that result in service disruptions and outages. Insolvency, financial instabilities, subcontractor's issues, outsourcing implications, difficulties in contractual arrangements are few typical reasons that the service providers may fail to deliver the expected quality of the services and lead to impairments. Additionally, the business processes may fail because of misalignment and inappropriate communication with the service provider, or even because of inadequately documented procedures[102].

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain***, ***Network Domain***, ***Operational Domain,*** and ***Product/business processes Domain***.

5.4.3 Threat: Loss of support services

Another typical example of outage is the unavailability of the necessary support services, which are required for the proper operation of the networks and the systems.

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain***, ***Network Domain***, ***Operational Domain,*** and ***Product/business processes Domain***.

5.5 Threat Group: Nefarious Activity/Abuse

The fact that the base of ad-hoc and sensor networks is a group of devices with low or no data storage and low power autonomy makes these networks vulnerable to nefarious activity attacks. This group of attacks includes intentionally created threats aiming at the infrastructure.

[101] Fortin, J. (2012). *East African Internet Cables Damaged by Ship's Anchor Near Mombasa*. [online] Available at: http://www.ibtimes.com/east-african-internet-cables-damaged-ships-anchor-near-mombasa-416986 [Accessed 18 Nov. 2016].

[102] Bundesamt für Sicherheit in der Informationstechnik. (2012). *Threats Catalogue – Elementary Threat.* [online] Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile [Accessed 18 Nov. 2016].

5.5.1 Threat: Denial of Service

In this context, ad-hoc and sensor networks suffer from traditional denial of service (DoS) attacks as experienced in other data and communication networks. Sensor networks are met in critical deployment environments, like healthcare systems. Thus, DoS and distributed DoS (DDoS) attacks are of great importance to be mitigated by timely detecting them[103]. In ambient assisted living (AAL)[104], especially in eHealth environments, the multi-hop nature of wireless mesh networks (WMNs) is vulnerable against unwanted rerouted traffic. Therefore, such a DoS attack situation (e.g. hello flooding) can be compromised by utilizing resilient routing protocols. Although there are several different characteristics[105] between WSNs and MANETs and several specific attacks targeted at each type of these networks[106], they are both susceptible to malicious node and routing attacks. For instance, in a *flooding attack*, the attacker tries to drain its victim's resources by remotely sending numerous connection establishment requests. In a cloud-based system, which could be a cornerstone component of an IoT solution, this kind of attack severely affects the Autonomic Manager, which is the component in charge of controlling and self-tuning the necessary changes in the system's life cycle[107].

However, many ambiguities exist in how we can theoretically define a DoS attack in ad-hoc and sensor networks. Nevertheless, emerging research work[108] has illustrated formal methods that evidently define such an attack situation.

DoS attacks are mainly caused by[109]: *(a)* producing varied effects on different OSI levels on the target (i.e. *Slowloris*[110]), *(b)* amplification / reflection techniques (i.e. DNS and NTP amplification, reflection change) and *(c)* flooding mechanisms (e.g. ping of death), *(d)* protocol exploit attacks (e.g. TCP SYN attacks) and *(e)* malformed packet attacks (e.g. land attack and fragmented packet attacks)[111]. For example, the *resource starvation attack* can be achieved by sending many packets that require authentication resulting in initiating

[103] Abbas, H., Latif, R., Latif, S. and Masood, A. (2016). Performance evaluation of Enhanced Very Fast Decision Tree (EVFDT) mechanism for distributed denial-of-service attack detection in health care systems. *Annals of Telecommunications*, pp.1-11.

[104] Alanazi, S., Al-Muhtadi, J., Derhab, A., Saleem, K., AlRomi, A., Alholaibah, H. and Rodrigues, J. (2015). *On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications*. 17th IEEE International Conference on E-health Networking, Application and Services (HealthCom). 14-17 Oct, Boston, USA, pp.205-210.

[105] Reddy, V., Negi, A. and Venkataraman, S. (2016). *A Comparison of Trust in MANETs and WSNs*. 6th IEEE International Advanced Computing Conference, 27-28 Feb, Bhimavarm, India, pp.577-581.

[106] Ramachandran, S., Shanmugam, V. (2012). Performance comparison of routing attacks in MANET and WSN. *International Journal of Ad-hoc, Sensor & Ubiquitous Computing (IJASUC),* 3(4), pp.41-52.

[107] Mendonça de Almeida F., de Ribamar Lima Ribeiro A., Moreno E.D. (2015). *An Architecture for Self-healing in Internet of Things*. 9th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM), 19-24 July, Nice, France, pp.76-81.

[108] Saghar, K., Farid, H., Kendall, D. and Bouridane, A. (2016). *Formal specifications of Denial of Service attacks in Wireless Sensor Networks*. IEEE 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST). 12-16 Jan, Islamabad, Pakistan, pp.324-333.

[109] Machaka, P. and Nelwamondo, F. (2016). Data Mining Techniques for Distributed Denial of Service Attacks Detection in the Internet of Things: A Research Survey. In: *Data Mining Trends and Applications in Criminal Science and Investigations*, pp.275-334. IGI Global.

[110] NMAP - http-Slowloris. *A web server test for the Slowloris DoS attack.* [online] Available at: https://nmap.org/nsedoc/scripts/http-slowloris.html [Accessed 18 Nov. 2016]

[111] Distributed DoS attack list. *Tools and reports on DDoS, University of Southern California, School of Engineering*. [online] Available at: http://www.isi.edu/~mirkovic/bench/attacks.html [Accessed 18 Nov. 2016]

resource expensive cryptographic processing[112]. When malicious nodes are connected to the internal network, they can launch different types of attacks, such as *routing poisoning* or *packet dropping*. Based on the characteristics of the attacks, they can be distinguished as *goal-oriented attacks*, *performer-oriented attacks and layer-oriented attacks*[113]. Concerning the performer-oriented attacks, the inside attackers can perform *black hole* and *grey hole attacks*[114,115]. During a black-hole attack, all the network traffic is redirected, which results in data packet loss. In the case of a grey hole attack, there is a *selective forwarding* of data packets. These types of attacks usually happen in mesh networks.

Sensor networks are prone to *jamming mechanisms*, which means that an adversary may inject unwanted signals into the communication channel. These signals can entirely engage the channel so that authentic communications cannot take place or the packets in transmission be corrupted [116]. In a DoS attack incident using jamming techniques, energy issues exist regarding the attacker counterpart that may run out of energy, when its energy budget is limited, and may also result in a node failure. In this vein, state-of-the-art ongoing works have aimed at how the attacker can save energy by utilizing an estimation on whether to jam the channel to degrade the ability of the intrusion detection[117].

As the technology shift brings out new advances in ad-hoc networking, mobile devices and sensors can dominate the telecommunication market in the not-so-distant future. Moving towards a mobile and cloud networking convergence, multiple security issues arise while mobile-based agents lack a shared language/ontology and thus they are prone to DoS attacks by classifying their nature[118].

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain***, ***Network Domain*** and ***Product/business processes Domain***.

5.5.2 Threat: Malicious code / software / activity

Ad-hoc and sensor networks should be monitored for environmental parameters, structural integrity of the built environment and usage of urban spaces, services and utilities. However, the sensors can be compromised through *malicious injected code* or by exploiting their physical interface. An attacker may seek to elicit an inappropriate system response, (e.g. triggering an overload on a power grid and lead to partial shutdown) or to mask a desired system response (e.g. silencing an intrusion alarm)[119].

Due to the potential vulnerabilities of the actuators and sensors, it is crucial to study and analyse the malicious code (i.e. malware) propagation within the networks. For propagation analysis purposes, recent

[112] Basicevic, I., Ocovaj, S. and Popovic, M. (2015). Evaluation of entropy-based detection of outbound denial-of-service attacks in edge networks. *Security and Communication Networks*, 8(5), pp.837-844.

[113] Chelli, K. (2015). *Security Issues in Wireless Sensor Networks*. Proceedings of the World Congress on Engineering (WCE), 1-3 Jul, London, U.K., pp.519-524.

[114] Kahtani, A. (2012). *Survey on security attacks in Vehicular Ad-hoc Networks (VANETs)*. 6th IEEE International Conference on Signal Processing & Communication Systems (ICSPCS), 12-14 Dec, Gold Coast, Australia, pp.1-9.

[115] Naeem, T., Loo, K.K. (2009). Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks. *International Journal of Digital Content Technology and its Applications*, 3(1), pp.88-93.

[116] Zuba, M., Shi, Z., Peng, Z., Cui, J. and Zhou, S. (2012). Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks. *Security and Communication Networks*, 8(16), pp.2635-2645.

[117] Zhang, H., Cheng, P., Shi, L. and Chen, J. (2015). Optimal Denial-of-Service Attack Scheduling with Energy Constraint. *IEEE Transactions on Automatic Control*, 60(11), pp.3023-3028.

[118] Kim, D., Jung, S., Hwang, D. and Kim, S. (2015). Mobile-Based DoS Attack Security Agent in Sensor Networking. *Wireless Pers Communication*, 86(1), pp.91-107.

[119] Illiano, V.P. and Lupu, E.C. (2015). Detecting malicious data injections in wireless sensor networks: A survey. *ACM Computing Surveys*, 48(2), Article 24, 33 p.

research has introduced mathematical models in a per-device (i.e. autonomous) manner[120]. Furthermore, modern malware is characterized by sophisticated obfuscation techniques, and recent research approaches have led to novel detection and classification techniques[121].

The concept of *Hardware Trojan* (HWT) emerges in wireless sensor networks. A HWT is a deliberate modification of the hardware during the fabrication process and can be designed to quietly monitor, to actively send out sensitive information, or to make the infected host device unusable[122]. Within the IoT ecosystem, the sensor nodes can be deployed in a distributed network to mutually acknowledge the trustworthiness of their sensor neighbour. Under this scheme, we can detect information leakages which are caused by a HWT[123].

Ad-hoc networks may employ mobile devices in a specific purpose, like for gaming, such as in the famous games Blizzard's World of Warcraft (WOW) and Linden Research's Second Life (SL)[124]. In this case, massive multiplayer online games (MMOG) can be exposed to malicious activities.

The assets targeted by these threats include asset groups ***Application Domain***, ***Device Domain***, ***Network Domain*** and ***Product/business processes Domain***.

5.5.3 Threat: Manipulation of hardware and software

Contrary to the outsiders (i.e. individuals outside the network access perimeter) who are not able to communicate directly with the network, the insiders have increased access to the resources and privileged knowledge of the internal network. This insider attack is a growing concern for most implementations, as this attack is more difficult to be prevented because of the unknown attack patterns and the variety of the internal attacks. If an alert for an invalid pattern is received, an extra analysis is required to verify whether there is a malicious attempt or not.

Some malicious activities are also likely to go undetected[125], as they can bypass the authentication and authorization methods, since they are already connected to the internal network. *Rogue access points,* wireless access points that are installed without any prior consent or knowledge, may expose the internal information to the outside world and could provide illegitimate access to unauthorized users.

The assets targeted by these threats include asset groups ***Application Domain***, ***Device Domain***, ***Network Domain***, ***Operational Domain*** and ***Product/business processes Domain***.

[120] del Rey, A., Hernández Encinas, A., Hernández Guillén, J., Martín Vaquero, J., Queiruga Dios, A. and Rodríguez Sánchez, G. (2016). An Individual-Based Model for Malware Propagation in Wireless Sensor Networks. *Advances in Intelligent Systems and Computing,* 474, pp.223-230.

[121] Hansen, S., Larsen, T., Stevanovic, M. and Pedersen, J. (2016). *An approach for detection and family classification of malware based on behavioral analysis.* IEEE International Conference on Computing, Networking and Communications (ICNC). 15-18 Feb, Kauai, USA, pp.1-5.

[122] Jalalitabar, M., Valero, M. and Bourgeois, A. (2015). *Demonstrating the Threat of Hardware Trojans in Wireless Sensor Networks.* 24th IEEE International Conference on Computer Communication and Networks (ICCCN). 3-6 Aug, Las Vegas, USA, pp.1-8.

[123] Liu, C., Cronin, P. and Yang, C. (2016). *A mutual auditing framework to protect IoT against hardware Trojans.* 21st IEEE Asia and South Pacific Design Automation Conference (ASP-DAC). 25-28 Jan, Macau, China, pp.69-74.

[124] Hili, G., Cobourne, Sh., Mayes, K. and Markantonakis, K. (2015). Practical Attacks on Virtual Worlds. In: *Risks and Security of Internet and Systems*, J. Lopez et al. (Eds.), 8924, pp.180-195. Springer International Publishing.

[125] Xiao, Y. (2016). *Security in sensor networks*, ch. 11, p.275. CRC Press.

5.5.4 Threat: Manipulation of information

WSNs are commonly utilizing a many-to-one communication pattern meaning that various sensors collect and send data to the single one control centre (i.e. the sink node or the base station). This is the reason why WSNs are vulnerable to *sinkhole attacks*. The attacker claims itself as having the shortest path to the base station and, therefore, it can remotely alter the passing data and by that means to threat the network operation[126].

Among the various models proposed for M2M communications and the IoT by various researchers, Semantic middleware and Service Oriented Architecture (SOA) oriented middleware are based on the Extensible Mark-up Language (XML) metadata exchange for interoperability, while the SOA and Representational State Transfer (REST) based systems are more popular in the enterprise environments. Main exploits related to the above are[127]: *(a)* duplication of a device, *(b)* black hole or sink hole attack (which are also DoS incidents) in the Routing Protocol for Low-Power and Lossy (RPL) Networks, *(c)* replay attacks, when valid data is retransmitted or delayed by an adversary to gain illegitimate and unauthorized access, *(d)* confidentiality compromise, when the relayed data can be manipulated, *(e)* active introduction of network traffic (i.e. spoofing, impersonation) to send malicious traffic to other nodes, *(f)* passive monitoring of network traffic (i.e. sniffing, snooping) in Zigbee and IEEE 802.15.4 networks because of their weak implementation of the nodes encryption keys (i.e. they are transmitted in clear text). Examples of important issues on the routing process are the *routing table overflow* (i.e. transmit false information to the neighbours, flood their tables and hence deny the real routes) and the *routing table poisoning* (i.e. advertise a false route with the smallest hop and the latest sequence number) in the Ad-hoc On-Demand Distance Vector (AODV) protocol[128].

The assets targeted by these threats include asset groups ***Device domain***, ***Network domain*** and the ***Applications domain***.

5.5.5 Threat: Remote activity

A paradigm on remote activity includes the *Botnet* utilization in terms of a network of infected machines, which is controlled by a remote machine and aims to initiate attacks against more victim machines. In terms of mobile computing and by leveraging the advantages of M2M communications in masking malicious code propagation, MobiBots can infect and coordinate these devices in a large-scale manner. For example, a MobiBot can infect a 96-node network in only few minutes and totally can scale up to 10,000-node networks[126].

For instance, when it comes to embedded systems in Home Networking, where sensors are a core component to study, there are specific needs; i.e. connecting to the Internet for firmware updates. Nowadays, *remote firmware updates* do not comply to the myth of ultimate security as they are responsible for distributing malicious content through the Internet. Another example of malicious firmware is the control on vehicles and their accelerator. Furthermore, another firmware rootkit is responsible for maliciously manipulating network packets by controlling the CPU of the network interface card (NIC)[129].

[126] Han, G., Li, X., Jiang, J., Shu, L. and Lloret, J. (2014). Intrusion Detection Algorithm Based on Neighbour Information Against Sinkhole Attack in Wireless Sensor Networks. *The Oxford Computer Journal*, 58(6), pp.1280-1292.

[127] Billure, R., Tayur, V. and Mahesh, V. (2015). *Internet of Things - a study on the security challenges.* IEEE International Conference on Advanced Computing Conference (IACC). 12-13 June, Banglore, India, pp.247-252.

[128] Airehrour, D., Gutierrez, J. and Sayan Kumar, R. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, 66, pp.198-213.

[129] Choi, B., Lee, S., Na, J. and Lee, J. (2016). Secure firmware validation and update for consumer devices in home networking. *IEEE Transactions on Consumer Electronics*, 62(1), pp.39-44.

The assets targeted by these threats include the asset groups ***Device Domain***, ***Network Domain***, ***Operational Domain*** and ***Product/business processes Domain***.

5.5.6 Threat: Targeted attacks

Mobile participatory sensing[130] takes advantage of the sensing resources available in mobile phones for an in-depth analysis of about the participating individuals and their environment. In this ad-hoc networking concept, when downloading the tasks from the application server or reporting sensor readings to the server, the participant's privacy information[131] (e.g. identity and location) can be revealed even if a pseudonym is used. For example, a reverse look-up address search may reveal their name, as participants typically commute between their domicile and workplace. Furthermore, the current participants' location can also be identified based on the collected sensor readings. For example, pictures, audio samples, and pollution data may include unique features, exposing the participants' whereabouts.

Targeted attacks also exist in the physical layer of any sensor communication. The *Spectrum Sensing Data Falsification (SSDF)* or else the Byzantine attack[132] is conducted in pursuit of two objectives: *(a)* vandalism and *(b)* exploitation. The first objective refers to interference to the primary systems by means of the malicious users reporting channel vacancy which indicates that the channel is busy. Thus, the sensing data induce the dedicated node (i.e. the fusion centre – FC) to allow other sensors to have false access to the channel. The second objective refers to exclusion of idle channels. Here, the attackers send channel busy information when their sensing data concludes that the channel is idle.

Likewise, the back off mechanism manipulates the back off time for the case of the medium access control (MAC) and especially the IEEE 802.11. The back off misbehaviour[133], or else *back off attack*, is unpredictable in such networks and results in a node which intends to acquire the channel with a higher chance by reducing its back off (i.e. waiting) time.

The assets targeted by these threats include the asset groups ***Device Domain*** and ***Network Domain***.

5.5.7 Threat: Social Engineering

In the scope of M2M communications, as the core of the IoT ecosystem, which also include humans, social engineering remains a major security threat to individuals and organizations, and is often launched through phone (*phone fraud*) or email (*phishing*). Recent studies argue that a correlation exists between the individuals' intention to resist social engineering and their security actions (i.e. self-reported or observed) in multiple cultural environments[134].

The growing trend towards BYOD (bring your own device) has deteriorated the problem. Ad-hoc networking and vulnerable mobile applications can be misused to conduct attacks for user-ID spoofing or hijack user

[130] Holler, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S. and Boyle, D. (2014). *From Machine-to-Machine to the Internet of Things*. Oxford: Elsevier Ltd.

[131] Christin, D. (2016). Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software*, 116, pp.57-68.

[132] Zhang, L., Ding, G., Wu, Q., Zou, Y., Han, Z. and Wang, J. (2015). Byzantine Attack and Defence in Cognitive Radio Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 17(3), pp.1342-1363.

[133] Lu, Z., Wang, W. and Wang, C. (2015). Modelling and Evaluation of Back off Misbehaving Nodes in CSMA/CA Networks. In: *Modeling and Evaluating Denial of Service Attacks for Wireless and Mobile Applications*, pp.1-33. Springer International Publishing.

[134] Flores, W., Holm, H., Ekstedt, M. and Nohlberg, M. (2015). *Investigating the Correlation between Intention and Action in the Context of Social Engineering in Two Different National Cultures*. 48th IEEE Hawaii International Conference on System Sciences. 5-8 Jan, Kauai, USA, pp.3508-3517.

accounts and much more. As such, the *baiting attack* refers to attackers who leave malware-infected storage media in a location where it is likely to be found by future victims. Another example is *phishing* by means of the attempt to acquire sensitive information by masquerading as a trustworthy entity[135]. Furthermore, the *waterhole attack* refers to compromising a website that is likely to be of interest of the chosen victim[135].

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain*** and ***Network Domain***.

5.5.8 Threat: Unauthorized activities

Stealing the identity within an ad-hoc and sensor network can be achieved by unleashing a *Sybil attack*[136]. Here, the adversaries can create many malicious identities either by forging a new identify or by stealing an identity from a legitimate node.

The assets targeted by these threats include the asset group ***Device Domain***.

5.6 Threat Group: Eavesdropping, Interception and Hijacking

This group includes threats that rely on the alteration/manipulation of the communication link between two parties. These attacks do not require the installation of additional tools or software on the victims' infrastructure. Insecure network access is a known threat, when connecting to insecure networks (i.e. public hot-spots) that are exposed to several attacks due to their openness and public characteristics. Usually, they are lacking security measures and policy rules, which also facilitate the eavesdropping or malicious activities[137].

5.6.1 Threat: Network Reconnaissance

WSNs are highly distributed ad-hoc networks. Due to specific limitations of their nodes communication radius, they route their traffic through a base station (BS); or else in a hop-by-hop basis. The *selective forward attack* is an example in which the attacker places a malicious sensor node on a path between a data source and a base station[138]. Hence, the attacker can identify and process network traffic at its illegitimate advantage.

Due to the unstable wireless channel that is common in such networks, the packet loss rate is high and varies from time to time. Hence, it is difficult to distinguish between a malicious drop and normal packet loss. Recent studies propose alternative data forwarding behaviours of sensor nodes per the deviation of the monitored against the estimated normal loss[139]. In this vein, adaptive network defence management for

[135] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, pp.113-122.

[136] Li, X., Han, G., Qian, A., Shu, L. and Rodrigues, J. (2013). *Detecting Sybil attack based on state information in Underwater Wireless Sensor Networks*. 21st IEEE International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2013). 18-20 Sept, Primosten, Croatia, pp.1-5.

[137] Cloud Security Alliance. (2012). *Top Threats to Mobile Computing*. [online] Available at: https://cloudsecurityalliance.org/wp-content/uploads/2012/07/Top_Threats_to_Mobile.docx [Accessed 18 Nov. 2016].

[138] Stehlik, M., Matyas, V. and Stetsko, A. (2016). *Towards better selective forwarding and delay attacks detection in wireless sensor networks*. 13th IEEE International Conference on Networking, Sensing, and Control (ICNSC). 28-30 Apr, Mexico City, Mexico, pp.1-6.

[139] Ren, J., Zhang, Y., Zhang, K. and Shen, X. (2016). Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*, 15(5), pp.3718-3731.

countering attacks can be applied in specific application areas such as in[140,141] *(a)* oil and gas infrastructure, *(b)* nuclear power plants, *(c)* smart cities and *(d)* eHealth environment.

The assets targeted by these threats include the asset groups ***Application Domain***, ***Device Domain***, ***Network Domain***, ***Operational Domain*** and ***Product/business processes Domain***.

5.6.2 Threat: Interception of information

Spectrum sensing is at the core of operational techniques seen in a wireless network. Interception of information may occur. The most famous such action is called *primary user emulation (PUE)*. In such an incident, the attackers may modify the radio transmission frequency to mimic the primary signal (i.e. the signal by the primary user – PU). Therefore, the secondary users (SU) erroneously identify the attackers as a PU. The PUE attackers can be classified as[142] *(a)* selfish and malicious (i.e. stealing bandwidth) and *(b)* static and mobile (i.e. per their location).

In the mobile computing environment, various techniques for malware detection exist, such as dynamic program-execution based mechanisms for the Android operating system. Nevertheless, malicious intruders can easily prevail on them by deploying dump code blocks and API calls[143]. The latter is accommodated in an *advanced persistent threat (APT)*, which results in passively and maliciously capturing information from the network.

In a company or corporation, the interception of information is one of the tools for corporate espionage or cyber-espionage[144]. The high skilled personnel employed by companies today tend to use these skills for their own profit by intercepting and selling inside information or by operating as external agents and trying to intercept information of opponent companies. In the first case where they intercept within the company, the existence of ad-hoc access to the company's Intranet or the transmission of data over the air, makes cyber-espionage more easy to be successful.

The assets targeted by these threats include the asset groups ***Device Domain***, ***Network Domain***, and ***Product/business processes Domain***.

5.6.3 Threat: Man in the middle / Session hijacking

Under certain circumstances, a malicious node can enter the network and pretend to be another node. Once the node joins the network, then spoofing and data interception may occur. In other cases, this type of attack is known as *man-in-the-middle* (MiMA), as the nodes can intercept the communication and receive the information, and relay wrong information between two parties communicating directly. This threat can lead

[140] Al-Hamadi, H. and Chen, I. (2015). Adaptive Network Defence Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks. *IEEE Transactions on Network and Service Management*, 12(3), pp.451-466.

[141] Mathur, A., Newe, T. and Rao, M. (2015). *Healthcare WSN: Cluster Elections and Selective Forwarding Defence.* 9th IEEE International Conference on Next Generation Mobile Applications, Services and Technologies. 9-11 Sept, Cambridge, UK, pp.341-346.

[142] Yu, R., Zhang, Y., Liu, Y., Gjessing, S. and Guizani, M. (2015). Securing cognitive radio networks against primary user emulation attacks. *IEEE Network*, 29(4), pp.68-74.

[143] Gaoxiang, W., Songjie, W., Na L. and Ling Y. (2015). *Capturing and characterizing network actions of mobile applications for behavior consistency*. IEEE International Conference on Computing and Network Communications (CoCoNet). 16-19 Dec, Trivandrum, India, pp.898-905.

[144] Williams, K.Y. (2015). Insider-Threat Detection in Corporate Espionage and Cyber-Espionage. In: Silva, E. (n.d.). (2015). *National security and counterintelligence in the era of cyber espionage*. pp.62-77. IGI Global.

to system instability or to abnormal behaviour due to fake information and even collisions of packets due to increased transmission requests or intercepted connections[145].

Based on recent research[146,147], although ad-hoc and sensor networks as well as RFID systems deploy distance bounding (DB) cryptographic protocols, they still obtain considerable high security mechanisms to defend against illegitimate actions. DB protocols are vulnerable in *mafia fraud*[147] (*or else* grandmaster problem) and *terrorist fraud* attacks[146]. In the mafia fraud, an attacker executes a man-in-the-middle attack between a verifier (i.e. the one who verifies the location of the user) and a user and erroneously informs the latter about the location of the user node. An instance of this attack is a physically located ATM machine. In a terrorist fraud, a dishonest user colludes with a "terrorist" attacker in a way that the latter can erroneously inform the verifier node about the location of the user node.

Another example is the applications hosted by Vehicular ad-hoc Networks (VANETs) which are described as a part of the Intelligent Transport Systems (ITS) ecosystem. These networks include a variety of emerging applications, such as traffic management and control, nearby information services, and real-time information routing calculations. Such applications, which belong in the superset of Dedicated Short-Range Communications (DSRC) applications family, can facilitate cooperative collision warnings[148] and emergencies notifications as well as commercial related applications which enable internet access, map navigation and fuel savings. In more detail, when it comes to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications using the road-side units (RSUs)[149,150], major privacy issues could arise under man-in-the-middle attacks. These attacks are feasible because of the unencrypted communication[150] between the RSUs and the vehicles.

The assets targeted by these threats include the asset groups ***Device Domain***, and ***Network Domain***, and the assets ***eHealth*** and ***cloud-based applications***.

5.7 Threat Group: Failures / Malfunction

5.7.1 Threat: Failure of devices or systems

Akin to any other computer machinery, sensor nodes suffer from software bugs that potentially end up in either a temporal out-of-service condition or in a complete failure of these devices. *Offline bug fixing* and *self-healing* are two techniques[151] that can be used to detect and deal with these conditions before the deployment or during runtime.

[145] Dong, Z., Espejo, R., Wan, Y. and Zhuang, W. (2015). Detecting and Locating Man-in-the-Middle Attacks in Fixed Wireless Networks. *Journal of Computing and Information Technology*, 23(4), p.283-293.

[146] Falahati, A. and Jannati, H. (2014). All-or-nothing approach to protect a distance bounding protocol against terrorist fraud attack for low-cost devices. *Electronic Commerce Research*, 15(1), pp.75-95.

[147] Avoine, G., Mauw, S. and Trujillo-Rasua, R. (2015). Comparing distance bounding protocols: A critical mission supported by decision theory. *Computer Communications*, 67, pp.92-102.

[148] Vahdat-Nejad, H., Ramazani, A., Mohammadiand, T., Mansoor, W. (2016). A survey on context-aware vehicular network applications. *Vehicular Communications*, 3, pp.43-57.

[149] Chaubey, N.K. (2016). Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study. *International Journal of Security and Its Applications*, 10(5), pp.261-274.

[150] Lim, K. and Manivannan, D. (2016). An efficient protocol for authenticated and secure message delivery in vehicular ad-hoc networks. *Vehicular Communications*, 4, pp.30-37.

[151] Brzozowski, M. and Langendoerfer, P. (2015). Bug-Tolerant Sensor Networks: Experiences from Real-World Applications. In: *Ad Hoc Networks*, N. Mitton et al. (Eds.), 155, pp.251-262. Springer International Publishing.

In addition to the above, a failure of systems can be dramatically harmful not only for the devices they employ, but also for the potential impact to the human population they accommodate. For instance, the computer worm named *Stuxnet,* employed to attack the Natanz nuclear facility located in Iran, exploited the PLCs in the industrial control systems infrastructure. This incident[152,153] highlighted that machinery design errors and vulnerabilities as well as the human factor[154] can even lead to fatal accidents.

The assets targeted by these threats include the asset groups ***Device Domain***, and ***Network Domain,*** but also the assets ***Manufacturing*** and ***Control Systems***.

5.7.2 Threat: Failure or disruption of communication links

Jamming attacks have been a major problem for ad-hoc and sensor networks and they are increasingly concerning the military and disaster response state authorities. The jamming device seeks to choose a location by choosing the same channel the nodes are using, so that the data is blocked or disrupted from successful transmission. The disruption of communication links is also threatened in an alternative manner by[155] *(a)* constant jammer (i.e. who continuously transmits randomly), *(b)* deceptive jammer (i.e. constantly, but not randomly)*, (c)* random jammer (i.e. randomly and reserving power), *(d)* reactive jammer (i.e. listen to the channel and reserve power). Jamming attacks are considerably severe as the jamming signals are[156] *(a)* resistant to collisions*, (b)* can travel for longer distances and *(c)* likely to be transmitted in short durations (e.g. as an ACK frame).

The assets targeted by these threats include the asset groups ***Device Domain***, and ***Network Domain***, and the asset ***Radio***.

5.7.3 Threat: Malfunction of equipment

Enterprises and organisations also be affected by equipment failure, e.g. air conditioning, heating or cooling systems, power supplies.

The assets targeted by these threats include the asset groups ***Device Domain***, and ***Network Domain***, and the assets ***Power Supplies*** and ***Cooling Systems***.

5.7.4 Threat: Disruption of main supply

Electric power transmission and distribution systems are susceptible to attack generally with little risk to the attacker, a fact well recognized by saboteurs and terrorists.

The assets targeted by these threats include the asset groups ***Device Domain***, and ***Network Domain***.

5.8 Ad-hoc and sensor network assets exposure to threats

In this section the threat exposure of ad-hoc and sensor network assets is summarized and categorized. The categorization is based on the assessment of the threats' impact on an asset or an asset group and this

[152] Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), pp.365-404.

[153] Hagerott, M. (2014). Stuxnet and the vital role of critical infrastructure operators and engineers. *International Journal of Critical Infrastructure Protection*, 7(4), pp.244-246.

[154] *Also, see* Section 5.5.6 of this document.

[155] Vadlamani, S., Eksioglu, B., Medal, H. and Nandi, A. (2016). Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*, 172, pp.76-94.

[156] Al-Mefleh, H. and Al-Kofahi, O. (2016). Taking advantage of jamming in wireless networks: A survey. *Computer Networks*, 99, pp.99-124.

impact is shown in Table 6. The table includes the relation of threats and threat groups, provided by the Threat Taxonomy in Chapter 4.

THREAT GROUP	THREAT	ASSET GROUP	ASSET/DETAIL
Unintentional damage / loss of information or IT assets		Device domain Network domain Application Domain Operational Business Processes	
	Inadequate design and planning or improper adaptation	Device domain	Data
	Using information from unreliable source	Device domain	
	Erroneous use or administration of devices and systems	Device domain	
	Loss of devices	Device domain	
	Damage caused by a third party		Data
Disaster (natural, environmental)		Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety
	Water	Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety
	Wildlife	Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety
	Explosion	Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety
	Thunder strike	Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety
	Natural disasters	Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety

THREAT GROUP	THREAT	ASSET GROUP	ASSET/DETAIL
	Fire	Device domain Network domain	Control Systems Physical Security Vending Machines Road Safety
Legal		Application Domain Business Processes	
	Abuse of personal data		Healthcare Physical Security Supply & provisioning
	Violation of laws and regulations	Device domain Network domain Application Domain Operational Business Processes	
	Failure to meet contractual requirements	Device domain Network domain Application Domain Operational Business Processes	
Outages		Device domain Network domain Application Domain Operational Business Processes	
	Internet outage	Device domain Network domain Application Domain Operational Business Processes	
	Network outage	Device domain Network domain Application Domain Operational Business Processes	

THREAT GROUP	THREAT	ASSET GROUP	ASSET/DETAIL
	Loss of support services	Device domain Network domain Application Domain Operational Business Processes	
Nefarious activity / abuse		Device domain Network domain Application Domain Operational Business Processes	
	Denial of service	Device domain Network domain Application Domain Business Processes	
	Malicious code, software or activity	Device domain Network domain Application Domain Business Processes	
	Manipulation of hardware and software	Device domain Network domain Application Domain Business Processes	
	Manipulation of information	Device domain Network domain Application Domain	
	Remote activity	Device domain Network domain Operational Business processes	
	Targeted attacks	Device domain Network domain	
	Social Engineering	Device domain Application Domain Network domain	

THREAT GROUP	THREAT	ASSET GROUP	ASSET/DETAIL
	Unauthorized activities	Device domain	
Eavesdropping, Interception, Hijacking		Device domain Network domain Application Domain Operations Business Processes	
	Network Reconnaissance	Ditto	
	Interception of information	Device domain Network domain Business processes	Manufacturing Control systems
	Man-in-the-middle / Session hijacking	Device domain Network domain	E-health Cloud-based apps
Failures / Malfunction		Device domain Network domain	
	Failure of devices or systems	Device domain Network domain	Control Manufacturing
	Failure or disruption of communication links	Device domain Network domain	Radio
	Failure or malfunction of equipment	Device domain Network domain	Power Supplies Cooling systems
	Failure or disruption of main supply	Device domain Network domain	
Physical attack		Device domain Network domain	
	Terrorist attack	Device domain Network domain	
	Damage from the warfare	Device domain Network domain	
	Unauthorized physical access	Device domain Network domain	
	Theft	Device domain Network domain	Mobile devices RFID tags & readers Cars & vehicles

THREAT GROUP	THREAT	ASSET GROUP	ASSET/DETAIL
			Interconnection points Transmission nodes
	Vandalism	Device domain Network domain	
	Sabotage	Device domain Network domain	

Table 6 Association between threats and assets

6. Threat Agents

In this chapter, we present a list of threat agents categories. Threat agents or threat sources are the individuals or groups of people who use the threats and vulnerabilities of a system for their purposes. This study is based on the ENISA Threat Landscape[157] 2013's consolidation of several publications. For each threat agents' category, we focus on the characteristics[158] emission, location, quantity, motivation, rationality, mobility and skill. The proposed categories are the following:

Corporations often adopt offensive tactics with the motive of gaining an advantage over competitors. They usually commit attacks as outsiders. Also, corporations are rational attackers since they consider the ratio of outcome gain and cost of the attack. The level of sophistication of their attack methods is relevant to the size and sector of the company.

Cyber criminals' motivation is financial gain or in many cases the hacking itself, as a skill test or obstacle. They are highly skilled and this factor may lead to irrational attacks, where the risk is bigger than the attack's expected outcome. They can work in local, national or international groups.

Cyber terrorists group involves terrorists that exploit the impacts of cyber-attacks in critical infrastructure like energy production system, telecommunications, government sites, etc. Their level is lower than the cyber criminals and they commit more rational attacks. Their motivation is usually politics or religion. They are considered as outside agents and can also work in groups.

Script kiddies use existing computer scripts or code to hack. They lack the expertise to create their own tools. Their motivation is the thrill of danger. The attacks committed by them are mostly naïve since they do not have the background to estimate the outcome/risk ratio or it is indifferent to them.

Online social hackers (hacktivists) are activists that use hacking as a tool. This group is like cyber terrorists. Their motive is also politics or social matters; their skill level may vary and they may work in groups. They target critical public infrastructure.

Employees are insiders that may be responsible for unintentional damage due to error or nefarious attacks in collaboration with outsiders intentionally or to make personal profit. They provide inside information and make the targeted system extremely vulnerable.

Nation states in the cyberwar and cybercrime have developed extremely sophisticated cyber weapons, systems with resources and high level experts. These characteristics makes them prominent threat agents.

Natural disasters are not controlled by an adversary group; however, they should be considered as a threat agent for ad-hoc and sensor networks. Mainly sensor networks are vulnerable to natural disaster since the network nodes could be in a wide area of rough or open to access environments (i.e. underwater, underground, flying, spread in a wide terrestrial area, etc.).

[157] European Union Agency for Network and Information Security (ENISA). (2013). *ENISA Threat Landscape 2013*. [online] Available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats [Accessed 18 Nov. 2016]

[158] Cayirci, E. and Rong, C. (2008). Security in wireless ad-hoc and sensor networks. John Wiley & Sons

In the following table, we propose a cross relation between threats and agents in ad-hoc and sensor networks.

	CORPORATIONS	CYBER CRIMINALS	CYBER TERRORISTS	SCRIPT KIDDIES	HACKTIVISTS	EMPLOYEES	NATION STATES	NATURAL DISASTERS
Disaster							●	●
Outages						●	●	●
Legal	●					●		
Failures, Malfunction		●			●	●	●	
Unintentional damage				●	●	●		
Nefarious Activity	●	●	●	●	●	●	●	
Physical attacks							●	●
Eavesdropping, Interception, Hijacking	●	●	●	●	●	●	●	

Table 7 Association between threats and agents

7. Vulnerabilities and Risks in Ad-hoc and Sensor Networks

Ad-hoc and sensor networks deployment is significantly increasing not only due to the increasing volume of IoT devices, but also due to the industrial and research interest ad-hoc and sensor networks have attracted since the '80s. "*Smart <anything>*" (e.g. cities, buildings, vehicles, home appliances, phones etc.) is a big trend and, hence, these network vulnerabilities have become a major issue among researchers and practitioners. Thus, publicly available information on ad-hoc and sensor networking for M2M communications security issues widely originates from research, standardisation and industrial activities.

Henceforth, sensors and their significance on the M2M communications paradigm are about to change some aspects of what can we consider something as vulnerable. These networks are characterized by flexible architecture, spatial nature, the communication means, and the complexity of the devices. To extract this information, we focus on standardization organisations like National Institute of Standards and Technology (NIST), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU), on governmental authorities like Defence Advanced Research Projects Agency (DARPA) and Qatar's National Centre for Security but also on published research works. More details are presented in the next chapter.

In this chapter, a short description of the vulnerabilities and risks for ad-hoc and sensor networks is provided. A thorough assessment of the related good practices is presented in the next chapter.

7.1 Ad-hoc and sensor networks vulnerabilities

The ad-hoc and sensor networks akin to any other IT system suffer from emerging threats and obscure vulnerabilities in every of the five domains, related to confidentiality, integrity, availability, privacy and authenticity[159]. More specifically, the major vulnerabilities in these networks concern the device security, the data protection, the communication integrity and availability (for both the protocols and hardware involved), the business process availability, privacy, and the operation stability. The device security is mostly handled with the use of authentication methods and the appropriate monitoring tools. The authentication methods in collaboration with data classification aim to ensure the protection of data. With the proper management and specialized protocol techniques, the network communication can be secured. The risk management procedures also lead to the business process availability and operation stability.

The resource exhaustion of devices is a vulnerability of ad-hoc and sensor networks, because of the nature of these devices (i.e. small devices, with low-level of power independency)[160]. This can be eliminated with data classification, appropriate management and simulation/visualization/testing activities.

The use of wireless communication[161] in ad-hoc and sensor networks potentially gives rise to certain vulnerabilities owning to the nature of the communication channel (i.e. open air, water). Besides, the

[159] Ashraf, Q. and Habaebi, M. (2015). Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, 49, pp.112-127.

[160] International Electrotechnical Commission – IEC. (2014). *Internet of Things: Wireless Sensor Networks*. [online] Available at: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf [Accessed 18 Nov. 2016].

[161] Scarfone, K., Dicoi, D., Sexton, M. and Tibbs, C. (2008). *Guide to Securing Legacy IEEE 802.11 Wireless Networks*. [online] National Institute of Standards and Technology (NIST). Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890006 [Accessed 18 Nov. 2016].

interception and interference vulnerabilities apply in the case of using RFID communication[162], Bluetooth[163], NFC[92], and Zigbee[163]. Another typical example is the access control violation[164] that exploits vulnerabilities, such as unencrypted transmissions caused by specific protocols used for wireless communication between an access control reader (e.g. RFID reader) and the controller device.

7.2 Ad-hoc and sensor networks risks

Several risks affect the assets and the operations of ad-hoc and sensor networks. Throughout the literature, it is highlighted that these networks can often be exploited for nefarious activities and eavesdropping attacks leading to a high data loss risk. Since these networks have a variety of types of physical positioning (underwater, underground, etc.), the risk of loss of devices in the case of natural or environmental disasters (earthquake, flood, tornado) is also significant[165].

The variety of physical positioning of ad-hoc and sensor networks, the resource constraints of the devices and the topology of the networks may lead to the leakage of personal or sensitive data. Notably, the privacy leakage risk behaviours[166] in ad-hoc and sensor networks could threaten even human lives.

Overcoming and managing nefarious activities can be accomplished with tighter risk management and operational controls, and with the availability of specialized tools and techniques that resolve these risks. Besides, various other risk management techniques (i.e. risk rating, risk matrices) can be adopted to provide consistency in prioritizing the risks, present the complex risk data, and facilitate the reviews to allocate the sufficient resources and mitigation methods.

It should be noted risk assessment is an ongoing procedure and the constant monitoring of the network is a necessity. Therefore, the continuous feedback and risk assessment from the stakeholders will certainly be an added value at any point of this procedure.

[162] Karygiannis, T., Eydt, B., Barber, G., Bunn, L. and Phillips, T. (2007). *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. [online] National Institute of Standards and Technology (NIST). Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51156 [Accessed 18 Nov. 2016].

[163] Boyes, H. (2013). Resilience and cyber security of technology in the built environment. [online] Centre for the Protection of National Infrastructure (CPNI) - http://cpni.gov.uk. Available at: http://www.cpni.gov.uk/documents/publications/2013/2013063-resilience_cyber_security_technology_built_environment.pdf?epslanguage=en-gb [Accessed 18 Nov. 2016].

[164] 3M Cogent, (2014). *Beyond Weigand: Access Control in the 21st Century*. [online] Available at: http://multimedia.3m.com/mws/media/833804O/beyond-wiegandaccess-control-in-the-21st-century.pdf [Accessed 18 Nov. 2016].

[165] Cerrudo, C. (2015). An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. [online] IOActive. Available at: http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf [Accessed 18 Nov. 2016].

[166] Feng, N., Hao, Z., Yang, S. and Wu, H. (2016). Supporting Business Privacy Protection in Wireless Sensor Networks. *Journal of Sensors*, 2016, pp.1-11.

8. Good Practices

To tackle the issue of good practices in the field of ad-hoc and sensor networking for M2M communications, we conduct a qualitative analysis on current approaches and routines. To achieve this, we use and categorise what is publicly available in the literature which either originates from the *industry*, the *public organisations* or from the field of *research and development* (R&D).

We acknowledge that several sources of good practices currently exist which provide an extensive set of security measures and controls. In more detail, our sources are: the *Centre for the Protection of National Infrastructure (CPNI)*[163,167,168], the *International Telecommunication Union (ITU)*[169,170], the *International Electrotechnical Commission (IEC)* [160], the *Federal Trade Commission*[171,172,173], the *GSM Association (GSMA)*[174], the *Securing Smart Cities global initiative*[175], the *National Institute of Standards and Technology*

[167] PA Consulting Group, (2012). HOLISTIC MANAGEMENT OF EMPLOYEE RISK (HoMER). [online] Center for the Protection of National Infrastructure (CPNI), http://cpni.gov.uk. Available at: http://www.cpni.gov.uk/documents/publications/2012/2012021-homer.pdf?epslanguage=en-gb [Accessed 18 Nov. 2016].

[168] Council on Cybersecurity. (2014). *The Critical Security Controls for Effective Cyber Defence*. [online] Centre for the Protection of National Infrastructure (CPNI) - http://cpni.gov.uk. Available at: http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-critical-security-controls.pdf?epslanguage=en-gb [Accessed 18 Nov. 2016].

[169] International Telecommunications Union – ITU. (2013). *ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones*. ITU-T X-series Recommendations – Supplement 19 [online] Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.Sup19-201304-I!!PDF-E&type=items [Accessed 18 Nov. 2016].

[170] International Telecommunications Union – ITU. (2015). *Internet Security Report*. [online] Available at: http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf [Accessed 18 Nov. 2016].

[171] Federal Trade Commission - FTC. (2013). *Privacy & Security in a Connected World*. [online] Available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [Accessed 18 Nov. 2016].

[172] Federal Trade Commission - FTC. (2012). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*. [online] Available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [Accessed 18 Nov. 2016].

[173] Federal Trade Commission - FTC. (2015). *Building Security in the Internet of Things*. [online] Available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf [Accessed 18 Nov. 2016].

[174] GSM Association - GSMA. (2016). *IoT Security Guidelines for IoT Service Ecosystem*. [online] Available at: http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.12-v1.0.pdf [Accessed 18 Nov. 2016].

[175] Cerrudo, C., Hasbini, A. and Russell, B. (2015). Guidelines for Smart Cities. [online] Securing Smart Cities. Available at: http://securingsmartcities.org/wp-content/uploads/2015/11/Guidlines_for_Safe_Smart_Cities.pdf [Accessed 18 Nov. 2016].

(NIST)[161,162,176,177,178,179], *Qatar's National Center for Information Security (Q-CERT)*[180,181,182], the *Sandia National Laboratories*[201] and several *Other (i.e. ENISA, IETF, DARPA, Research Papers,* etc.)

[176] Computer Security Division. (2015). *Annual Report*. [online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-182.pdf [Accessed 18 Nov. 2016].

[177] National Institute of Standards and Technology (NIST) - Computer Security Division. (2014). *Annual Report*. [online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-176.pdf [Accessed 18 Nov. 2016].

[178] National Institute of Standards and Technology - NIST. (2006). *Special publication 1048, Case-Study Measurement Needs a Compilation*. [online] Available at: http://pml.nist.gov/test-structures/10-FilesToDownload/NISTSP1048.pdf [Accessed 18 Nov. 2016].

[179] National Institute of Standards and Technology - NIST. (2013). *Guide to Enterprise Patch Management Technologies*. [online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf [Accessed 18 Nov. 2016].

[180] Qatar Computer Emergency Response Team (Q-CERT). (2016). *Best Practices Protecting Your Mobile Device*. [online] Available at: http://www.qcert.org/sites/default/files/public/documents/my-bp-best_practices_for_protecting_mobile_devices-eng.pdf [Accessed 18 Nov. 2016].

[181] Qatar Computer Emergency Response Team (Q-CERT). (2011). *PORTABLE DATA STORAGE SECURITY INFORMATION FOR CIOs/CSOs*. [online] Available at: http://www.qcert.org/sites/default/files/public/documents/au-bp-portable_data_storage_security_information_for_cio-eng-2011.pdf [Accessed 18 Nov. 2016].

[182] IT Security Expert Advisory Group (ITSEAG). (2008). *Defence in depth*. [online] Qatar Computer Emergency Response Team (Q-CERT). Available at: http://www.qcert.org/sites/default/files/public/documents/au-bp-defence_in_depth-eng-2008.pdf [Accessed 18 Nov. 2016].

[91,92,94,118,119,124,126,165,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198]. In quantitative terms, most *other* analysed documents cover a modest part of the security measures/controls in our field of study. However, all the above sources are considered of the same importance and are illustrated in **Error! Reference source not found.**.

We have identified a considerable number of security measures/controls which we have categorised as follows:

- Authentication
- Data protection

[183] Spanò, E., Di Pascoli, S., Iannaccone, G. (2016). Low-Power Wearable ECG Monitoring System for Multiple-Patient Remote Monitoring. *IEEE Sensors Journal*, 16(13), pp.5452-5462.

[184] Australian Government Information Management Office, Department of Finance and Deregulation. (2009). *National e-Authentication Framework*. [online] Available at: http://www.qcert.org/sites/default/files/public/documents/au-bp-national_eauthentication_framework-eng-2009.pdf [Accessed 18 Nov. 2016].

[185] European Union Agency for Network and Information Security -ENISA. (2014). *Smart Grid Threat Landscape and Good Practice Guide*. [online] Available at: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide [Accessed 18 Nov. 2016].

[186] Defence Advanced Research Projects Agency - DARPA. (2013). *DARPA Seeks More Robust Military Wireless Networks*. [online] Available at: http://www.darpa.mil/news-events/2013-03-18 [Accessed 18 Nov. 2016].

[187] Patil, A. and Gaikwad, R., (2015). Comparative Analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Network. *Procedia Computer Science*, 48, pp.387-393.

[188] National Electrical Manufacturers Association - NEMA. (2015). *The magazine of electro industry: Growing the Internet of Things*. [online] Available at: http://www.nema.org/Communications/Awards/Documents/Growing-the-Internet-of-Things_Gold-Cover.pdf [Accessed 18 Nov. 2016].

[189] Mansouri, D., Mokddad, L., Ben-othman, J. and Ioualalen, M. (2015). *Preventing Denial of Service attacks in Wireless Sensor Networks*. IEEE International Conference on Communications (ICC), 8-12 June, London, pp.3014-3019.

[190] Wang T., Jin H. and Nahrstedt K. (2015). *mAuditor: Mobile Auditing Framework for mHealth Applications*. ACM Mobihoc Conference, 22-25 June, Hangzhou, China. pp.7-12.

[191] Bhagat, S., Kothari, C., Bapat, V. and Kulkarni, V. (2015). *Classification and determination of physical intrusion using Wireless Sensor Networks*. IEEE 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 13-15 July, Denton, USA, pp.1-5.

[192] Patil, S. and Chaudhari, S. (2016). DoS Attack Prevention Technique in Wireless Sensor Networks. *Procedia Computer Science*, 79, pp.715-721.

[193] Mouton, F., Leenen, L. and Venter, H. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, pp.186-209.

[194] TELEFONICA. (2016). *The city as a platform for Digital Transformation*. [online] Available at: https://www.telefonica.com/documents/341171/45062944/POLICY+PAPER_Smart+Cities_The+City+as+a+platform+for+Digital+Transformation+April+2016.pdf/10f6ad6b-0350-4c98-b11d-0433adf5d0fc [Accessed 18 Nov. 2016].

[195] Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures*. Ad-hoc networks*, 1(2), pp.293-315.

[196] Internet Engineering Task Force – IETF. (2015). *Request for Comments (RFC) 7416: A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)*. [online] Available at: https://tools.ietf.org/html/rfc7416 [Accessed 18 Nov. 2016].

[197] Fagade, T. and Tryfonas, T. (2016). Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks. *Lecture Notes in Computer Science*, pp.128-139.

[198] Sert, S., Onur, E. and Yazici, A. (2015). *Security attacks and countermeasures in Surveillance Wireless Sensor Networks*. 9th IEEE International Conference on Application of Information and Communication Technologies (AICT), 10-14 Oct., Rostov-on-Don, Russia, pp.201-205.

- Monitoring
- Simulation, visualisation and testing activities
- Data classification
- Management and support
- Risk management
- Specialised tools & techniques

The identified security measures/controls are mapped against the threats, finalising the puzzle of relations between threat exposure and proposed security measures, controls and policy. This information can be also found in **Error! Reference source not found.** which concludes the current chapter.

8.1 Authentication

1. Apply authentication methods for access to a system/service by a device/individual (e.g. enforce the use of strong password, one-time-access accounts, certificates with common revocation and reissuing, authentication with biometrics, security tokens, challenge-handshakes protocols, challenge-response authentication mechanisms, salted password hashing, globally shared key)[162,163,165,167,168,171,172,174,175,176,180,181,182,184,185,192,195]

2. Develop protocols that identify the viability of the neighbours (trusted network) and resolve any issues optimally[186]

3. Utilize multicast authentication of sensor data for low security overhead[176,177]

4. Authenticate packets (e.g. hello packets), so that they cannot be spoofed[195]

5. Enforce a trusted model to form neighbours for nodes and eliminate a compromised node from advertising its location[195]

6. Secure and robust M2M communications model (i.e. ETSI TS 102 921 M2M communications)[160,174,185]

7. Apply centralized authentication used in strong authentication schemes[174,176,185]

8. Plan and implement security by design[171,173]

9. Design and implement security measures at several levels; plan defence-in-depth (i.e. degradation or failure mode, redundant paths, hierarchical routing, network-layer security delivery, multi-hop routing measures)[173]

10. Use standardised network & entity authentication (i.e. ISO/IEC 13157-4:2016)[160,174]

11. Comply with architectural sensor network principles (i.e. ISO/IEC 29182-3:2014)[174]

12. Use Network Authentication Services (i.e. 3GPP TS 33.220)[174]

13. De-couple the application authentication and authorization processes with the network authentication process[174]

14. Employ Keyed-Hash Message Authentication Code (HMAC) for the communication between tags and readers[162]

15. The remote terminal must have security functions, such as entity authentication, key management, encryption with the application server in the application level or network level[160]

16. The gateway should have security functions, such as entity authentication, and MAC or integrity, with the application server[160]

17. Implement a trust relationship using mobile-based security agents that use single-sign-on mechanisms[118] or trust management-based techniques (i.e. Event-Based, Anomaly-Based, Second-Hand Information) to distinguish malicious interference from events or faults[119]

18. Use anti-cheating products (e.g. Punkbuster) to prevent unauthorised modifications in virtual-world clients and two-factor authentication mechanisms (e.g. World of Warcraft authenticator)[124]

19. Extend the Europay MasterCard and VISA (EMV) technical standard for smart payment cards to treat and manage effectively the EMV weaknesses by using Point of sale (POS) authentication and session requests and confirmations[92]

20. Detect the malfunctioning node by using auto regression and trust evaluation techniques[198]

21. Authenticate nodes and verify its programming details to prevent hardware node subversion[198]

22. Ensure that the communicating nodes are authenticated prior to data encryption applied in the routing exchange to defend against Deliberate Exposure Attacks[196]

23. Ensure confidentiality of the node routing information by requesting routing information which must be authenticated and must be authorized for that access to defend against Remote Device Access Attacks[196]

8.2 Data protection

1. Develop security solutions for group management, data protection (e.g. data cryptography) for data at rest or in transit and secure mechanisms for horizontal handover[162,168,171,173,174,175,176,177,181,182,185]

2. Develop microcontroller cryptographic implementations to cater for security and privacy in constrained environments (i.e. need for low security overhead, tolerance of Lossy networks, time-criticality, and high data rates)[177]

3. Control the privacy attributes to manage the information provided to third parties[174,185]

4. Detect replay attacks by maintaining an increasing counter for each link and including the next value of the counter with each packet and discarding packets containing older values[174,195]

5. Use encryption techniques to prevent Selective Forwarding Attacks[185,195]

6. Secure disposal of RFID tags[162]

7. Enforce Non-Revealing Identifier format on RFID tags[162]

8. Encrypt sensitive user data[169]

9. Use digital signatures[169]

10. Deploy user confirmation process before the installation and execution of applications[169]

11. Secure data aggregation based on DTLS protocol where each aggregation node selects the next safe and reliable hop[160]

12. Utilise encryption libraries[160]

13. Deploy privacy preservation schemes, health data access control and privacy-preserving health data processing[91]

14. Prevent message corrupting by using Elliptic Curve Cryptography (ECC) over public key infrastructure (PKI)[198]; applied on Dedicated Short-Range Communications (DSRC) applications[149]

15. Accommodate Link layer encryption and authentication using a globally secret key to prevent routing attacks[198]

16. Enforce public key cryptography (Ad-hoc networks) & symmetric key cryptography (sensor networks)[195]

17. Use a cryptosystem either lattice-based such as NTRUEncrypt or a multivariate one such as TTS[199]

18. Orchestrate a secure data aggregation scheme based on cryptographic primitives to entrust the data concealment on the *homomorphic encryption* (HE) scheme[200]

8.3 Monitoring

1. Schedule audits, alerts and logs running frequently in every system and device (specific examples: Low-Power Wearable ECG Monitoring System for Multiple-Patient Remote Monitoring)[161,163,165,167,168,174,175,182,183,185]

2. Restrict or monitor any unauthorized physical access for specific areas (a Wi-Fi area, a highly-equipped room like a computer centre, an RFID tag's range). This control can be accomplished by a surveillance system or a Security Service Agency[162,163,167,168,175,182,184]

3. Use Remote Intrusion Monitoring (RIM), Intrusion Detection systems (IDS) and other attack detection tools. Deeply inspect packets for IDS/IPS filtering of malicious traffic[161,168,182,185,201]

4. Develop mathematical and statistical analysis research to collect and handle large datasets to model normal network behaviour[201]

5. Use centralised monitoring systems for security, data analysis and correlation in WSNs. This leads to safer conclusions and reduction of the resources' cost per identity[183,201]

6. Utilize an Energy Weight Monitoring system, which avoids redundant packet transmission or loop and saves power of the nodes, prevents the WSNs from Vampire Attacks[187]

7. Transform the sensors to automated control centres as part of fully integrated and connected systems[188]

[199] Shih, J.R., Hu, Y., Hsiao, M.C., Chen, M.S., Shen, W.C., Yang, B.Y., Wu, A.Y. and Cheng, C.M. (2013). Securing M2M with post-quantum public-key cryptography. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 3(1), pp.106-116.

[200] Shim, K.A. and Park, C.M. (2015). A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(8), pp.2128-2139.

[201] SANDIA National Laboratories. (2010). *Assessment of Current Cybersecurity*. [online] Available at: http://prod.sandia.gov/techlib/access-control.cgi/2010/104765.pdf [Accessed 18 Nov. 2016].

8. Deploy special nodes (gNodes) that monitor sensor clusters or control nodes (cNodes) that monitor the traffic throughput in clusters[189]

9. Use low-overhead and non-obtrusive auditing framework which monitors (in real-time) resource usage patterns of eHealth apps and triggers alerts to users if abnormal patterns are detected[190]

10. Scrutinise the movement of data across network boundaries, to minimize exposure to attackers[170]

11. Maintain a constant amount of traffic to different destinations through the generation of arbitrary traffic flows to defend against Traffic Analysis Attacks[196]

8.4 Simulation, visualization and testing activities

1. Establish the appropriate business models, design methods, and common set of standards[160,163,167,175,185,188]

2. Collaborate with suppliers and vendors and review the security requirements and assessments. Whenever possible and needed, change the default systems' configuration to avoid the existence of backdoors, with the vendors' approval and collaboration[185]

3. Prefer hardware, software and applications purchased by security concerned vendors. Keep the vendors under constant evaluation[162,175,180,182,185]

4. Conduct physical security surveys and assess the vulnerabilities of the network and the services[185]

5. Develop and enforce the benchmarking procedures and principles for OS, micro-code, and patches[178]

6. Develop software assurance metrics, privacy and security methods, benchmarking methodologies, and reference datasets to measure the assurance, vulnerabilities, resiliency during the development, testing, and deployment activities in order to provide for a quality assurance and certification process[178,185]

7. Develop standard evaluation and measurement methodology of data transfer[178]

8. Embed measurement capabilities for signal interference, and strength[178]

9. Develop, support, and commercialize measurement standards for the performance and service lifecycle of the components[160,178,185]

10. Ensure that communication standards include conformance specifications, and provide automated testing tools and tests that can be generated dynamically and rapidly[160,178]

11. Ensure the security architecture convergence that influences the business viability[160,185]

12. Implement input validation at the presentation and application layer[174]

13. Secure and preserve the interfaces and integration points with other services or components[173,185]

14. Exploit simulation activities to detect the effect of the configuration changes and determine the optimal setup. Visualization can also prevent the spread of potential attacks[201]

15. Employ social engineering to uncover behaviours in ad-hoc wireless and sensor environments[201]

16. Standardise the wireless and sensor network testing framework (i.e. ISO/IEC DIS 19637)[174]

17. Produce new testing methods (i.e. Fuzzing) to detect possible defects[173]

18. Use freely accessible libraries for testing and assessment activities[178]

19. Deploy (a) Misuse Detection which compares well-known attack patterns, (b) Anomaly Detection which features a normal behaviour and (c) Specification-based Detection which counts deviations from normal behaviours[191]

20. Compare with historical routing/topology data to defend against Overclaiming and Misclaiming Attacks[196]

8.5 Data classification

1. Create roles to assign permissions to individuals or devices. Restrict network access by network segregation (VLANs, IP subnetting, ACLs)[163,165,167,168,175,181,182,184]

2. Enforce proper use of permissions granted by the role of an individual or a device and stay within the limits and the purpose of that role[167,168,184]

3. Define security classification policies for data and sets of data types[174]

4. Evaluate the use of XML technologies with data exchange standards to support system integration and interoperability[178]

5. Incorporate reasonable data collection limits and security review methodologies[162,167,168,172,182,184]

6. Make organizations accountable for their privacy practices[162,167,168,172,182,184]

7. Develop and maintain comprehensive data management procedures[172,185]

8.6 Management and Support

1. Use a centralized management framework for audit functions and for monitoring people, processes and systems[163,167,168,170,175,182]

2. Request for direct and immediate support from hardware or software vendors in case a problem or attack occurs[163,165,168]

3. Keep a successfully tested "Plan B" in case of failure or attack. The alternative would preferably be totally independent to the active solution/implementation (disaster-recovery plan, business-continuity plan)[163,165,168,182,185]

4. Create and maintain a virtual, real-time map of the infrastructure and the communication paths between nodes[167,168,182]

5. Schedule routine backups[163,167,168,180,182]

6. Disable or change password for every default/guest account[163,168,175,180,181,182]

7. Apply and test automated updates for firmware/OS/software and applications configured to eliminate weaknesses[169,175,180,182,202]

8. Define management models for administration (i.e. ISO/IEC 30100-1:2016, ISO/IEC DIS 30140-1)[174]

9. Deploy and enforce standard patch management technologies, appropriate measures and procedures, and standard security techniques (i.e. issues related to timing, prioritization, testing when planning and executing the patch management processes)[179]

10. Design and implement the appropriate tools for attribute management by consumers and empower them to be competent to identify security vulnerabilities, potential threats or to make decisions about their data[172,173]

11. Maintain an endpoint and service recovery model[174]

12. Formulate the acceptable conformance criteria and standards for reliability, resiliency, security and privacy[178]

13. Implement and use a Disaster Recovery System[185]

14. Maintain safe start, stop and fail modes for smart grid components: systems shall be capable of operating in an operational or non-operational state according to some policies[168,175,185]

15. Retrieve adequate customers' information regarding security issues or concerns[185]

16. Walk through how consumers will use the network or service in a day-to-day setting to identify potential risks and possible security soft spots[173]

17. Maintain and update an inventory with the information of authorized and unauthorized software/OS/applications/devices within the network[168,183]

18. Maintain and protect RFID tags' passwords (access, lock and kill passwords)[162]; and interconnect the RFID transceiver with a back-end server which manages these passwords[162]

19. Enforce system security of RFID readers and middleware RFID systems[162]

20. Choose appropriate placement of RFID tags and readers[162]; also, protect RFID readers with electromagnetic shielded tunnels[162]

21. All systems and devices should have protected or stopped any unnecessary service, process or port/socket (OS hardening, firewall rules)[161,163,165,168,170,174,175,180,181,182,185]

22. Prevent network devices from using autorun programs to access removable media[170]

23. Ensure that all wireless access points are manageable using enterprise management tools[170]

24. Compare network devices configurations against standards for each type of device[170]

[202] National Institute of Standards and Technology – NIST. (2013). *Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise.* [online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [Accessed 18 Nov. 2016]

25. Carefully identify and separate critical data from information that is readily available to internal network users[170]

26. Control access of processes and users to resources and/or services[169]

27. Harden the network components (i.e. disable SNMP protocol on Access Point (AP) or enable SNMPv3)[161]

28. Employ secure and controlled management (i.e. disable HTTP interface on Access Point (AP) or enable HTTPS)[161]

29. Configure the Channel number and the power output of Access Point (AP)[161]

30. Apply configuration best practices (i.e. avoid default SSID name on APs)[161]

31. Use strong security mechanism (i.e. avoid using pre-shared keys (PSK))[161]

32. Use security controls (i.e. use of MAC Access Control Lists (MAC ACL) on APs)[161]

33. Apply network configuration best practices (i.e. use Dynamic Host Control Protocol (DHCP) for IP assignment)[161]

34. Comply with configuration strategy (i.e. maximum beacon time interval (announcements of position) on APs)[161]

35. Prevent unauthorized management (i.e. prevent unauthorized resetting of Access Points (APs))[161]

36. Control access on RFID information[162]

37. Manually request and permit the connection of STAs (device with a wireless interface) with an Access Point (AP)[161]

8.7 Risk management

1. Employ efficient threat modelling and risk assessment[165,174,185]

2. Create, maintain and update a threat knowledge database[163,168,182]

3. Appoint a specific team of individuals responsible for preventing attacks and recovering from them[163,168,182]

4. Align security strategy to the organization overall IT strategy based on the defined risk profile[185]

5. Apply penetration testing and vulnerability scanning of third-party components that are integrated into or utilized by the network[173]

6. Mitigate the risks with patch management technologies (i.e. patches being altered, credentials being misused, vulnerabilities) and avoid resource overload conditions, resource starvation, network congestion, etc.[179,185]

7. Keep informed via security forums and mailing lists (i.e. bugtraq) of the latest threats from trusted security sources[173]

8. **Enforce standardised performance assessment to reduce the risks and improve the resiliency of the service[178]**

9. Analyse the risks of the solution thoroughly and retention of collection of data[173]

10. Document the ad-hoc wireless and sensor networks architecture and configuration; identify and review critical components and service that require additional levels of protection[185]

11. Create blacklists (known malicious IP lists) and whitelists (valid IP list) and accordingly deny or permit access[168]

12. Enforce security using an economical modelling[192]

13. Deploy a sector-specific regulation (e.g. IoT-specific or polycentric regulation)[94]

14. Deploy models on information gathering and social engineering attack formulation[193]

15. Promote and encourage security-aware culture within the organization[162,163,167,168,171,173,182,184,194]

8.8 Specialized tools and techniques

1. Use of firewall, antispyware and antivirus software in all devices, if possible. Additionally, firewall protect any web application, interface or API[161,163,168,170,180,182]

2. Use of Wireless Intrusion Detection Systems (WIDS)[168]; also, utilise low-level packet inspection within the WIDS coverage are as proposed by the ISO/IEC/IEEE P21451-1-4 standard[203]

3. Allow positioning of nodes arranged in grid (less need for location information to be advertised)[195]

4. Use multipath routing against Selective Forwarding Attacks. Choosing the next hop probabilistically, reduce the risks and prevent the compromised node from gaining the control[195,196]

5. Reject received calls/SMS/MMS/e-mails from unknown recipients[180]

6. Code Signing to verify the identities to users of the code (and decide whether to install or not the software)[185]

7. Design and maintain flat-based, hierarchical-based, location-based and hierarchical routing protocols to defend against wormholes and sinkholes attacks[160,195]

8. Detect Medium Access Control (MAC) attacks and prevent the WSN node from entering the sleep mode by using variations of the MAC Protocol (S-MAC, T-MAC, B-MAC or G-MAC)[187]

9. Develop cyber-security strategy around IEC 62351information security standard[185]

10. Implement output data filtering for restricted characters[174]

[203] Institute of Electrical and Electronics Engineers (IEEE). (2014). *P21451-1-4 - Standard for a Smart Transducer Interface for Sensors, Actuators, and Devices - eXtensible Messaging and Presence Protocol (XMPP) for Networked Device Communication*. [online] Available at: https://standards.ieee.org/develop/project/21451-1-4.html [Accessed 18 Nov. 2016].

11. Implement security controls and preventive countermeasures (i.e. rate limiting) that reduce the risk of DoS or automated attacks[173,185]

12. Use Lightweight Secure Mechanism to defend against Path Based DOS attacks. A new hash chain is needed and verified each time. In case the number is not verified, then the packet is dropped[187]

13. Use Next Generation Access Control Protocols and API definitions (NGAC-FA, NGAC-GOADS, INCITS 499, SP 800-178, etc.)[176,177]

14. Use Packet Leash, which allows connection between two non-neighbouring malicious nodes, to detect wormhole attacks, where applicable[187]

15. Prevent Sybil attacks by limiting the number of neighbours that a node can have, and by sending an error message[195]

16. Use Spread Spectrum and Cryptographic puzzle to protect the network against external Jamming attacks. For the prevention of jamming attacks in the internal model, packet hiding before classification of the packet can be used[187]

17. Use an overlay network in which the base station should be changed frequently. Consequently, changing or replacing the base stations make it more difficult to compromise these nodes[195]. Alternatively, usage of Long-Term Evolution (LTE) and Long-Term Evolution-Advanced (LTE-A)[204] base stations

18. Use gossiping algorithms to reduce the collisions and messaging costs[195]

19. Use the appropriate methods (i.e. vulnerability scanner, security scanner, open-port detector)[179]

20. Apply bidirectional verification where a number of L2 links are arranged in controller/spoke arrangements and are continuously validating connectivity; Deploy the Expected Transmission Count (ETX) with MESH-LINK protocol (HELLO Flood Attacks and ACK Spoofing Attacks)[195,196,198]

21. Employ cover-coding method in RFID communication[162]

22. Deploy sensor nodes which possessing radio frequency shielded sheltering mechanism[162,198]

23. Use tags with a “press-to-activate” switch[162]

24. Apply tag polling in small time intervals[162]

25. Use geographical insights for flow control or isolate nodes that receive traffic above a certain threshold or allow only trusted data to be received and forwarded or dynamically pick up the next hop from a set of candidates (Geographic Routing Protocol)[195,196]

26. Use authenticated end-to-end acknowledgements and global time synchronization against Sybil attack, and massive flood of replies[195]

[204] Jain, A. and Buksh, B. (2016). Solutions for Secure Routing in Mobile Ad Hoc Network (MANET): A Survey. *Imperial Journal of Interdisciplinary Research*, 2(4), pp.5-8.

27. Enforce key management and bootstrapping (i.e. token based pre-configuration of the keys during manufacturing of the nodes, physical protection of messages, in-band during a weak security set-up phase, out-of-band communication)[160]

28. Apply routing with feedback information that includes the information of delay, trust, location, excess capacity in acknowledgment frames of the media access control (MAC) layer[160]

29. Use secure wakeup and secure bootstrapping to prevent a special class of denial of service attacks, the so-called sleep deprivation attacks[160]

30. Process and compare of link-state routing information received from different peers or support indirect communications exchanges between non-adjacent routing peers to provide a secondary channel for performing distance-vector routing information validation (Spectrum Sensing Data Falsification Attack)[196]

31. Provide mechanisms for unicast messages; enforce mechanisms that protect messages between a point-of-service and a single mobile node or by distributing group keys regarding multicast messages (i.e. the Amendments 2 and 4 of IEEE 802.21)[176]

32. Employ a Message Observation Mechanism (MoM)[192]

33. Approach a Repeated Game Theory and a Bayesian Game Theory in defending against DoS attacks[192]

34. Implement detection based on signal strength and deploy an Ant Based Framework in defending against DoS attacks[192]

35. Embed security requirements within the OS architecture by implementing security governance frameworks[197]

36. Deploy distributed algorithms for detecting sinkhole attacks which do not use cryptography (i.e. no time overhead) or extra mobile nodes and utilise the collaboration information of neighbour nodes[126]

37. Camouflage or hide sensor nodes[198]

38. Utilise Randomized Multicast or Line-Selected Multicast to prevent node replication attacks[198]

39. Select routing protocols such as the Ariadne, the *Secure Efficient ad-hoc Distance vector (SEAD)* and the *Authenticated Routing for ad-hoc Network (ARAN)*[204]

The mapping of the identified security measures/controls against the threats is shown in **Error! Reference source not found.** to clarify the relation between threat exposure and the proposed security measures, controls and policy. The security measures/controls are grouped under the name of the organization or company that provided the corresponding literature. The security measures found in R&D literature can be found in the column under the name "OTHER".

9. Gap Analysis

Ad-hoc and sensor networks mainly consist of distributed nodes processing critical, sensitive, mass, and several other types of data. Moreover, these nodes often form dynamic topologies and incorporate changing characteristics such as high mobility and fluctuating bandwidth. These characteristics along with the real-time transmission of data streams, the low energy supply, the low processing power, the routing protocols and the authentication schemes could raise several security concerns.

Various security concerns could also arise regarding the integrated components used in the sensors. Typically, PLCs can read signals from different sensors, and the integration of sensors with the PLCs in Supervisory Control and Data Acquisition (SCADA) systems - aiming to optimize the level of production – should be examined thoroughly considering any security threats and risks. For instance, the electrification and water supply of cities could be at risk, if we do not consider on a perpetual basis all the appropriate and effective security countermeasures. In the same context, the integration of ad-hoc and sensor networks in domestic appliances enables the remote management of houses and offers increased flexibility; however, there are various security concerns for smart objects and connected devices (i.e. home-automation systems, smart TVs and refrigerators) threatening the internet interconnection of houses, because of security vulnerabilities and data privacy issues. In healthcare environments (i.e. hospitals), the fusion of sensors in clinical operations targeting to monitor the physiological vital signs of patients, leads to critical technical and legal considerations, such as business and technical restrictions in the implementation, and regulatory reviews. For example, a patient has the right to know the names of all the employees who may access the medical records, but on the flip side in the cases of “break-the-glass” and life-critical operations the average consultation time should be significantly shorter.

The aim of the current gap analysis is to determine the path towards optimizing the countermeasures and to establish specific target objectives set by the industry, the academic community, and the research work by the security experts (e.g. Black Hat Conferences) in working out the needs and resources to improve security and provide better protection. The gap analysis is performed upon all five areas of the M2M functional Architecture (*see* Figure 4 M2M Architecture): 1) Application Domain, 2) Device Domain, 3) Network Domain, 4) Operational Domain, and 5) Product/business processes Domain.

9.1 Gaps on the Device domain

Gap: The sophistication of attacks targeting the communication amongst mobile devices as well as with backend servers is greater than the level of security that practices offer.

A wide spectrum of attacks targets the weakest component in the M2M architecture which is the communication amongst the mobile devices of any ad-hoc network. When it comes to mission critical ad-hoc networks which are met in the military area where the lives of individuals depend on them and in production environments where designs and concealed information are endangered by disclosure, then the challenge of mitigating vulnerabilities of complex communications is of great importance. For example, the RFID tags are exposed to certain threats such as man-in-the-middle attacks (see 5.6.3) and tools such as the *Tastic RFID Thief*[205]. The orchestration of the *cover-coding method*, the *press-to-activate switch* and the *non-revealing identifier format* practices (*see* 8.2, 8.8), mitigate these threats. Thus, the attackers’ attention is

[205] Brown F. (2013). *RFID Hacking: Live Free or RFID Hard*. Black Hat USA 2013. [online] Available at: https://media.blackhat.com/us-13/US-13-Brown-RFID-Hacking-Live-Free-or-RFID-Hard-Slides.pdf [Accessed 18 Nov. 2016].

diverted to the RFID readers for conducting several attacks by utilizing combinations of vulnerabilities (see 5.6.3) which are appointed by the communication between the readers and the tags.

Access control is another facet which is affected by the gap of susceptible communications in ad-hoc networks. For example, the practice that leads to emerging security challenges in the context of RFID is *Access control on RFID information* (see 8.6). Access controls on RFID readers cannot be achieved when the Wiegand protocol facilitates communication with upstream devices[206]. The Gecko[207] and the BLEkey[208] exploit vulnerabilities of the Wiegand protocol and have managed to perform passive attacks by violating the access control transmitted information. The most recent penetration systems facilitate the interception of RFID data in transit, and could be remotely controlled by using Bluetooth Low Energy (BLE). These systems must be placed in the RFID readers to be able to perform their malicious activities. To this end, not only the monitoring of access points should be continuous, but also strict access should be applied to the monitoring system. This need is of high value, because the success of these attacks depends on whether the attacker can tamper with the monitoring system as an intermediate stage to the exploitation of the RFID readers.

9.2 Gaps on Network domain

Gap: The continuous assessment to resolve the proper positions and then deploy the WIDS's required resources.

It is evident that a host-based intrusion-detection solution cannot be implemented for each node of an ad-hoc and sensor network because of energy constraints. Furthermore, the need to monitor real-time data prior to their transmission results in delays. In the case of ad-hoc and sensor networks, even though the *use of Wireless Intrusion Detection Systems (WIDS)* (see 8.8) enables certain proactive activities which may lead to the identification of malicious incidents such as real-time data monitoring, detecting anomalies on network segments of exchanged packets among the sensors, and reporting, WIDS are restrained by specific challenges. Due to the dynamic topology of such networks, determining the best location for the WIDS's sensors, as well as the respective correlation server, is a complex and difficult task. Accordingly, for every new sensor which establishes a connection with an ad-hoc network, the WIDS's sensors coverage should be evaluated. In the case that the new sensor is out of WIDS's coverage, then a new WIDS sensor should be integrated. This process reveals a gap, as the sensors connect and disconnect dynamically in ad-hoc networks. Thus, in the event of leaving a new sensor out of a WIDS's coverage, the vulnerabilities of this sensor threaten the ad-hoc network.

Gap: The required time-period between the assessment of firmware updates and their deployment or with withdrawal depending on the identification of threats.

There is a major concern about the effectiveness of the practice named *changing or replacing the base stations that make it more difficult to compromise the mobile nodes* (see 8.8), which increases the level of security and the complexity in ad-hoc and sensor networks. By adopting this procedure, the networks operational expenses are also increased due to the topology magnitude and the number of sensors.

[206] 3M Cogent, (2014). *Beyond Weigand: Access Control in the 21st Century*. [online] Available at: http://multimedia.3m.com/mws/media/833804O/beyond-wiegandaccess-control-in-the-21st-century.pdf [Accessed 18 Nov. 2016].

[207] Franken, Z. (2008). *Are you protected by two screws and a plastic cover?......Probably!* Black Hat DC [online] Available at: https://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf [Accessed 18 Nov. 2016].

[208] Baseggio, M. and Evenchick, E. (2015). *Breaking Access Controls with BLEKey*. [online] Available at: https://www.blackhat.com/docs/us-15/materials/us-15-Evenchick-Breaking-Access-Controls-With-BLEKey-wp.pdf [Accessed 18 Nov. 2016].

However, the procedure’s long-term viability is in question. The expenses discourage any service provider of ad-hoc networks to implement the examined practice due to the cost-efficient nature of these networks. The diversity of security mechanisms for each one of the domains in the M2M architecture necessitates human interaction in order to mitigate the risks and ensure an adequate threat protection. Besides, we need to efficiently tackle the challenges of the release management (i.e. firmware upgrades, patches, hot-fixes, OS updates) and attain a high level of security. For instance, the automated firmware updates increase the security risks by raising potential vulnerabilities in the vehicles Engine Control Unit (ECU) and in distributed networks sensors. To this end, the automated or *remote firmware updates (*see 5.5.5) threat is mitigated by the testing process of this practice. However, the required time period to perform the testing process of the new updates and patches, leaves the sensors susceptible to vulnerabilities which could be mitigated by the examined updates as soon as they are approved and deployed. In this time period, the exploitation of any vulnerability is extremely dangerous, due to the fact that it depends on the capabilities of the attacker and the sophistication of the exploitation method.

Gap: The standalone characteristics of routing protocols which are employed in MANETs are not sufficient for threat protection.

By design, the routing protocols in ad-hoc networks and autonomous systems of mobile nodes (MANETs) are classified into three categories; namely the *proactive*, the *reactive/on-demand* and the *hybrid* ones[209]. The protocols also facilitate the exchange of routing information, which allows the ad-hoc and sensor nodes to learn and adapt to the node or topology changes. However, none of them can adequately safeguard the operation of such networks against the whole spectrum of attacks such as against *DoS* attacks (*see* 5.5.1) because of trade-offs and limitations which are inherited by their characteristics[210]. These limitations are not adequately addressed by the implementation of the practices named *design and maintain flat-based, hierarchical-based, location-based and hierarchical routing protocols* (*see* 8.8), which only partially safeguard the MANETs’ operation. Thus, the routing protocols are prone to a wider spectrum of malicious attacks such as jamming (see 5.5.1) and eavesdropping (see 5.6).

9.3 Gaps on the Application Domain

Gap: Security patches and updates do not mitigate zero-day exploits targeting M2M applications.

In the case that the software deficiencies of M2M applications are not known vulnerabilities (e.g. Exploit Database[211]) and, consequently, they are not managed and resolved by security patches, updates and hotfixes, then the M2M applications could be of interest for the perpetrators that leverage the power of zero-day exploits to obtain access. For instance, the attacks which arise from the threat of *nefarious activities* (see 5.5) are highly associated to zero-day exploits and lead to *malicious code injection*, *security misconfigurations* exploitation as well as *broken authentication*[212]. Thus, the development of applications should follow best practices and state-of-the-art solutions, which could prioritize the practical

[209] Petearson Anzola, J., Bolanos-Castro, S. and Tarazona-Bermudez, G. (2016). Design Methodology for Self-Organized Mobile Networks Based. International Journal of Interactive Multimedia and Artificial Intelligence, 3(7), pp.46-53.

[210] Airehrour, D. and Gutierrez, J. (2015). *An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing*. International Conference on Information Resources Management (CONF-IRM), 18-20 May, Ontario, Canada.

[211] Offensive Security (2015). *Exploit Database*. [online] Available at: https://www.exploit-db.com/ [Accessed 18 Nov. 2016].

[212] European Telecommunications Standards Institute (ETSI). (2014). *ETSI TR 118 508 Analysis of Security Solutions for the one M2M System.* Technical Report, v.1.0.0. [online] Available at: http://www.etsi.org/deliver/etsi_tr/118500_118599/118508/01.00.00_60/tr_118508v010000p.pdf [Accessed 18 Nov. 2016].

implementation of *confidentiality*, *integrity* and *availability* by leveraging security mechanisms such as cryptography and separation between operational and user data. Moreover, the deployment, the updating and the resolving of security emergency incidents should be guided by Community Emergency Response Teams (CERTs) spread worldwide. In that vein, the security in the application layer can be reinforced.

Gap: Cloud-based M2M applications cannot be safeguarded by the proposed practices due to the complex backend environment.

Due to their scaling demand on back-end resources, the M2M applications are increasingly based on the cloud computing (CC) paradigm and the respective deployment and service models. The CC service models belong in different layers of abstraction in the architecture and are mutually dependent for provisioning the end-services. Moreover, there are several security implications among the cloud computing service models. For example, specific vulnerabilities of the Platform-as-a-Service (PaaS) could potentially endanger the secure deployment of the Software-as-a-Service (SaaS). Consequently, the security dependencies between these models could lead to threats such as in *erroneous use or administration of devices and systems* (see 5.1.3). With the aim to secure the application layer in accordance with legacy environment practices, such as with *inventory maintenance and update with the information of authorized and unauthorized software/OS/applications/devices within the network* (see 8.6), many vulnerabilities outsourced by the CC models dependencies are not confronted. For example, the Virtualized Environment Neglected Operations Manipulations (VENOM)[211] vulnerability is leveraged by attackers to target the virtualisation systems of Cloud Service Providers (CSPs) which use the Infrastructure-as-a-Service (IaaS) model. In that case, the negative effects of a successful attack impact the Software-as-a-Service operations.

9.4 Gaps on the Operational Domain

Gap: The interaction with human factor and the poor video quality of surveillance systems.

Many ad-hoc networks operate in complex locations such as supply chains and production environments. These locations are complex since they cannot be locked down to be off-limits to unauthorized personnel. Thus, Closed-Circuit Television (CCTV) and surveillance systems[213] are employed in the context of the practice, *usage of centralized monitoring systems for security* (see 8.3). These systems facilitate real-time surveillance or capture of footage to assess it later. Their operation is supervised by highly trained employees who are liable for reporting suspicious activities. However, the response time of CCTV and surveillance systems in case of alerts is limited due to the human factor. Further, the video quality of many CCTV systems is poor, leading to inability of usage for forensic purposes. To this end, these gaps harden the success of the monitoring crime prevention procedures which are applied at ad-hoc networks.

Gap: Physical security is limited when defence-in-depth is implemented.

Even though throughout the operation and life-cycle of ad-hoc networks many mobile devices enter and leave, the assets of ad-hoc networks are constantly increasing. This situation combined with the practice of implementing a *security plan based on defense-in-depth* (see 8.1), leads to a gap which burdens many providers. By definition, defense in depth separates the M2M architecture into defense layers. Each layer, consists of certain security mechanisms and measures able to obstruct and prevent criminal activities. In many use cases, where ad-hoc networks are mounted in remote locations and they are vulnerable to threats such as *loss of devices* (see 5.1.4), then the physical layer demands a greater number of security resources.

[213] D. Hutter, (2016). *Physical Security and Why It Is Important*. SANS Institute. [online] Available at: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120 [Accessed xx Nov. 2016].

The gap lays on the fact that defense-in-depth necessitates dynamic resource allocation[214] of security mechanisms to cover the dynamic topology of ad-hoc networks. To this event, the linkage amongst this security plan and the budget of the provider do not fulfill the provider's cost-effective expectations. Thus, following defense-in-depth, the physical security which is of great importance, is also limited due to the spectrum of resources which are required to secure each layer of ad-hoc networks.

Gap: Fraudulent activities are addressed only with security mechanisms on M2M architecture without functional procedures.

The distributed nature and the shared resources of the M2M architecture expose the business processes to threats of *abusing personal data* as well as to *nefarious activities*. This exposure could potentially lead to *fraudulent activities,* which primarily violate the assets integrity and lead to a low-level of trust and privacy. The existence of operational defensive mechanisms aims to secure the enterprises technical layer (i.e. *trust relationship using mobile-based security agents that use single-sign-on mechanisms* or *trust management-based techniques* (*see* 8.1)). The implementation of these mechanisms without any support by the functional layer of the enterprises in which the policies documentation occurs, leads to inconsistencies such as a static approach against fraud threats.

9.5 Gaps on the Product/Business Processes Domain

Gap: The regulations mitigate only threats against the type of collected and processed data.

The structuring model of the business processes for ad-hoc and sensor networks incorporated in the enteprises should be based upon a regulatory framework that defines the legality and level of privacy. The security and operations regulatory framework should define and provide the success factors (e.g. confidentiality, integrity and level of privacy) for the sensory data and the communication. Then, the threat of *violating rules and regulations* (*see* 5.3.2) can be eliminated and eradicated. However, the regulatory frameworks take into consideration only the type of the collected and processed data without focusing on the type of the underlying environment. Accordingly, only threats against the type of collected and processed data are addressed by the regulations. Thus, the regulatory frameworks do not always pose certain threat protection methods and techniques to eliminate threats in ad-hoc and sensor networks. As a result, even if the ad-hoc networks operate according to the regulatory frameworks which also conform to the law, this is not adequate to achieve a high level of security. Thus, the enteprise is liable to define the objectives that would eliminate threats such as *outages* and *DDoS attacks*.

Gap: The regulations do not necessarily resolve all the responsibilities of individuals concerning the security activities.

Typically, the regulationsdefine the liabilities and the responsibilities concerning the security activities, which should be performed by the service providers. For example, the integration of *technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss*[215] could be employed. The regulatory frameworks do not explicitly define the obligatory actions that burden the end-users concering their security activities. As a result, the end-users are threatened, since they are uninformed about the security perspective of the M2M applications. In most cases, applications which

[214] Interagency Security Committee, (2015). Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide. Department of Homeland Security. [online] Available at: https://www.dhs.gov/sites/default/files/publications/isc-planning-managing-physical-security-resources-dec-2015-508.pdf [Accessed xx Nov. 2016].

[215] Data Protection Directive: officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=1 [Accessed 18 Nov. 2016]

collect PII are the e-Health applications and are enabled by the orchestration of Mobile Healthcare Networks (MHNs) (*see* 5.3.1).

***Gap:* The attack surface of external components derails security by design.**

Every communication layer of an ad-hoc and sensor network is threatened by *the lack of planning or design errors* (see 5.1.1) during their initiation phase. The implementation of the practice of *planning and implementing security by design* (see 8.1) provides adequate security mechanisms in each layer. However, the implementation of *security by design* fails to protect business processes due to their association to the attack surface of external components[216] integrated in ad-hoc and sensor networks. For example, SCADA systems consist of several external components (e.g. PLCs) facilitating the operational management of ad-hoc and sensor networks. PLCs are usually orchestrated in order to achieve the business' goals concerning the level of performance and QoS. With regard to PLCs which are manufactured by specific vendors, existing vulnerabilities enable *arbitrary file disclosure*[211] and *remote control*[211]. The vulnerabilities of PLCs introduce security risks that could not be mitigated in the context of security by design. Besides, the enteprises owing SCADA systems, such as power generation and water distribution facilities, can not alter or modify PLCs in order to eliminate their vulnerabilities because they are subject to Intellectual Properties Rights (IPR) such as copyrights and the industrial design rights of the vendors. Another example of this limitation is the fact that certain sensors operate with a preinstalled OS whcih may have various vulnerabilities without the possibility for installation of an updated version of OS or security patches. As a result, the vulnerabilities on these sensors can not be resolved by the examined practice named security by design, and they are susceptible to OS exploits (see 5.1.2).To this end, this constrain arises both for sensors and external components such as Remote Terminal Units (RTUs) and Programmable Automation Controllers (PACs) which are purchased by vendors. Correspondingly, security by design does not fully mitigate the threat of *lack of planning or design errors*, in the context of business processes.

9.6 Recommendations

The above gaps naturally result in a set of recommendations that can improve the overall security performance and can be classified either as organisational or as technical recommendations.

9.6.1 Organisational recommendations

In the context of security attributes, ad-hoc and sensor network development could be strengthened by practices that are documented with respect to standards and compliance, for that purpose we propose functional, policy and regulatory recommendations that can provide a clear guidance to interested organizations

Functional Recommendations

In the context of security attributes, ad-hoc and sensor network development could be strengthened by practices that are documented with respect to standards.

There is a growing concern about the natural persons' privileges that access sensorial datasets to perform a diversity of management operations (i.e. M2M service provider's operators). This concern refers to most of the challenges on the surveillance data management on areas monitored by closed circuit security systems, and indoor positioning data mainly on supply chains and data streams, which facilitate M2M home appliances remote control. For this purpose, it is of great significance to identify by whom the data is accessed, and the conditions they need to access the data. The appropriate roles should be defined to associate the end-users (e.g. M2M service provider's employees, clients) with specific segments of collected

[216] I. Arce, K. Clark-Fisher, N. Daswani, J. DelGrosso, D. Dhillon, C. Kern, T. Kohno, C. Landwehr, G. McGraw, B. Schoenfield, and M. Seltzer, (2014). *Avoiding the top 10 software security design flaws*. IEEE Computer Society.

data and authorize them with specific privileges concerning the computational operations. This procedure should be combined with strict monitoring on ad-hoc and sensor network to ensure and enable the secure collection of sensitive data. Moreover, the M2M applications development and deployment in CC environments should be performed by adapting and expanding the application security guidelines of standardization organizations and cover the needs and demands of the M2M architecture.

Policy Recommendations

Due to the privacy issues that should be considered in the ad-hoc and sensor networks with personal, confidential, sensitive data being exchanged, specific policies should be established about authorising procedures and sharing agreements regarding the sensorial data. For transparency purposes, policies should be considered, which relate to the liabilities definition and the management operations description. Furthermore, a privacy policy should articulate the reasons and methods, which are orchestrated for the collection as well as for the processing of sensorial data and the mechanisms mitigating threats against functional and operational procedures. Moreover, privacy compliance should be ensured in the context of a reliable and consistent M2M application. A standardized documentation concerning the privacy compliance should be followed; typical examples are the Privacy Threshold Analysis (PTA) or the Privacy Impact Assessment (PIA). Further to the sensitive data plane, the privacy policy is also associated with additional documents. For example, in the healthcare sector, the informed consent documents are associated with the privacy objectives which are set forth by the integrated ad-hoc networks deployed at hospitals environment. The patients are empowered to control and to approve the concentration as well as the processing of their sensitive information by the BSNs. In other terms, the patients agree to control the disclosure of their PII to a trusted and predefined third-party, such as to specific nursing staff and doctors.

The security level of M2M applications is highly affected by the back-end servers' vulnerabilities. For this purpose, these servers should be updated using security patches and they should also be subject to vulnerability management. The components of this management should be a technical assessment as well as the revaluation of the competent policy which defines acceptable methods to perform the assessment itself.

Security by design should be implemented for each layer of the ad-hoc network, which means that, on a higher layer of abstraction, the development of the password-management policy is of great significance for mitigating various threats. However, prior to the adaptation of this type of policy, many challenges, such as the mutation of passwords and the intervals of time under which the changing of passwords will take place, should be addressed. Moreover, the operational implementation of this policy should be ensured in the context of its compliance by orchestrating appropriate controls and assessments. Furthermore, the technical practises utilized to secure the RFID interaction between tags and readers should be compliant with standards and state-of-art security mechanisms.

Regulatory Recommendations

The collection and processing of PII should be performed by following the constraints placed by the European Directives, such as by the General Data Protection Regulation 2016/679[217], the Cross-Border Healthcare

[217] General Data Protection Regulation: officially Regulation 2016/679 on the protection of natural persons in regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [online] Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [Accessed 18 Nov. 2016].

Directive 2011/24/EU[218] and the Decision 2011/890/EU[219] on providing the rules for the establishment, the management and the functioning of the Network of national competent authorities on eHealth. However, the underlying infrastructure of M2M applications and operations should comply with the security and operations regulatory frameworks regarding the protection of personal data. For example, in two-years' time, these applications should operate under the guidelines of the General Data Protection Regulation 2016/679[217] which follows a risk-based approach and enables privacy by design. Finally, the service providers of ad-hoc networks should inform the end-users about their responsibilities (e.g. strong credentials, usage of digital signatures) concerning the PII concealment during the networks' operation and especially in cases where MHNs are orchestrated.

Business/Product processes Recommendations

The manufacturing of certain products (e.g. GPS receivers, medical sensors) should be threat-driven to minimize potential vulnerabilities, which would allow attacks during the deployment and development phases. The manufacturing enterprises of GPS receivers should also be aware of the constantly growing attack surface of their products. The GPS operation is based on the transaction of signals between the GPS receiver and four or more satellites. This transaction of signals takes place so as the GPS receiver can establish its current three coordinates and synchronize its clock with the constellation's atomic clocks. The predominant method, per which GPS operates, can be exploited due to vulnerabilities which enable spoofing attacks[220]. The defensive techniques which can be employed to construct a tamper-proof GPS receiver can only be applied during their manufacturing due to the individuals' lack of knowledge and resources. Moreover, end-to-end encryption should be implemented during the communication of GPS receivers and satellites. Therefore, this issue is recommended to be addressed by the companies during the design and modelling procedures.

In the context of addressing fraudulent activities inside the M2M architecture, proactive functional procedures, protocols and policies should be orchestrated aiming to provide fraud prevention and assurances to the end-users. More specifically, a code of conduct, and a fraud risk control policy consist the minimum safeguards which should be defined and incorporated in M2M architecture by means of the authorization policy upon the collected data. These proactive safeguards in the businesses functional layer should be strengthened by fraud detecting mechanisms.

9.6.2 Technical Recommendations

In order to improve and securely implement sensors networking in M2M communication, we provide different technical recommendations, with a special focus on authentication/authorization methods and proactive and reactive defences.

Authentication/Authorization Recommendations

In principle, we should aim to increase the security in the authentication process by deploying strong or *multi-factor authentication methods (MFA)*, wherever applicable. However, concerning device authentication for ad-hoc and sensor networks, any device could also rely on *certificate-based authentication* and on methods which harden the exploitation procedure by employing a secure network

[218] Cross-Border Healthcare Directive 2011/24/EU; officially Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024 [Accessed 18 Nov. 2016].

[219] Decision 2011/890/EU on providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth. [online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:344:0048:0050:EN:PDF [Accessed 18 Nov. 2016].

[220] M. L. Psiaki and T. E. Humphreys, (2016). GPS LIES. *IEEE SPECTRUM*, pp. 26-32.

registration. Furthermore, an elastic type of access control mechanism is recommended to be incorporated in ad-hoc and sensor networks such as the *attribute-based access controls*. Hence, these amplified secure devices could be mounted in non-secure locations and unattended installations. Moreover, in the context of RFID communication between the tags and the readers, it is recommended that the authentication process take place in upstream devices to associate unique passwords to individuals.

Proactive Defence Recommendation

In the recent years, there is a growing concern about DDoS and flooding attacks as well as about the sophistication of their offensive techniques. *botnets* are utilized in DDoS attacks against ad-hoc and sensor networks; because of the concealed nature of bots, the botnets may become an unpredictable adversary. From another perspective, the ad-hoc and sensor networks are targeted with the scope to be compromised and the devices are enrolled in *botnets,* which perform DDoS attacks. This method was followed during the US incident involving a critical internet infrastructure which was targeted by the Mirai-based IoT botnet. Thus, despite the orchestration of WIDS in the context of ad-hoc networks, the employment of IDS in every bottleneck of the M2M architecture such as the M2M gateway is recommended. Following the adjustment of this measure, any incoming junk traffic from the M2M devices targeting entities outside the ad-hoc and sensors network could be identified and prevented. To this end, the network traffic of every *internet-connected* device is monitored and proactive detection is orchestrated. Besides, it is recommended to ensure the continuous update of the IDS sensors' ruleset in strict time intervals and by following trustful sources of signatures. Furthermore, due to the characteristics of MANET routing protocols , it is strongly recommended that the network security assessment should primarily focus on the routing protocols vulnerabilities.

Reactive Defence Recommendation

The identification of zero-day exploits is impossible to be implemented by WIDS.The operation of the defensive mechanisms performing deep packet inspection (DPI) is based upon signatures of known attacks. Thus, it is recommended to create a defense zone consisting of a *honeynet*, alongside the ad-hoc and sensor networks. This network is composed of *honeypots* emulating the operation of sensors. The honeynet constitutes a type of darknet which is able to identify new methods of attacks and zero-day exploits. *Mobile Edge Cloud Computing* is recommended to be orchestrated so as to develop the *honeynet*. The operation of honeynets enables the tracking of malicious activities in order to analyse them and collect forensic information about the attacks and the attackers behaviour. A network of virtual entities emulating the operation of sensors should be employed and, in the event of a threatening incident, the malicious traffic could be offloaded in the Mobile Edge Cloud (MEC) in order for this traffic to be recorded and monitored. Due to the fact that the offloading process increases the overhead of energy consuption, virtual machines which operate inside the MEC should be utilised in order to avoid performance constraints contrary to the case of using sensors.

10. Conclusions

The development of the ad-hoc and sensor networking for M2M communications threat landscape in 2016 has been impressive in one thing: *it exponentially expands its own borders of impact whilst the industry, the authorities and the experts analyse the big picture to date*.

The threat landscape has evolved in terms of the assets quantitative set which is affected or may unintentionally contribute to this landscape expansion. By completing the current research document, our conclusions have been divided into three categories: ***policy***, ***business*** and ***technical*** (focused on ***research)*** conclusions.

Policy conclusions

- Establish specific policies about authorising procedures and sharing agreements. A privacy policy should articulate the reasons and methods which are orchestrated for the collection as well as for the processing of sensorial data and the mechanisms mitigating threats against functional and operational procedures.
- Ensure privacy compliance in the context of reliable and consistent M2M applications. Standardized documentation concerning the privacy compliance should be followed; typical examples are the Privacy Threshold Analysis (PTA) or the Privacy Impact Assessment (PIA).

Business conclusions

- Proactive functional procedures, protocols and policies should be orchestrated aiming to provide fraud prevention and assurances to the end-users. More specifically, a code of conduct, and a fraud risk control policy should be incorporated in an M2M architecture by means of the authorization policy upon the collected data.
- Ensure that the manufacturing of certain products (e.g. GPS receivers, medical sensors) should be threat-driven to minimize potential vulnerabilities which would allow attacks during the deployment and development phases.

Technical conclusions

- Incorporate an elastic type of access control mechanism such as the attribute-based access controls. Hence, these amplified secure devices could be mounted in non-secure locations and unattended installations.
- Employ an IDS in every bottleneck of the M2M architecture such as the M2M gateway. Following the adjustment of this measure, any incoming junk traffic from the M2M devices targeting entities outside the ad-hoc and sensors network could be identified and prevented.
- Create a defence zone which consists of a honeynet by orchestrating Mobile Edge Cloud Computing (MEC) to track of malicious activities. A network of virtual entities emulating the operation of sensors should be employed and, in the event of a threatening incident, the malicious traffic could be offloaded in the Mobile Edge Cloud (MEC) for this traffic to be recorded and monitored.

11. Bibliography/References

Related ENISA papers

Big Data Threat Landscape and Good Practice Guide. [online] Available at https://www.enisa.europa.eu/publications/bigdata-threat-landscape, 2016

ENISA Threat Landscape 2015. [online] Available at: https://www.enisa.europa.eu/publications/etl2015, 2016

Guideline on Threats and Assets. Technical guidance on threats and assets in Article 13a. [online] Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets, 2015

Security and Resilience in eHealth Infrastructures and Services. [online] Available at: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services, 2015

Threat Landscape and Good Practice Guide for Software Defined Networks/5G. [online] Available at: https://www.enisa.europa.eu/publications/sdn-threat-landscape, 2015

Cyber security for Smart Cities - An architecture model for public transport. [online] Available at: https://www.enisa.europa.eu/publications/smart-cities-architecture-model, 2015

Security and Resilience in eHealth - Security Challenges and Risks. [online] Available at: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services, 2015

Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations. [online] Available at: https://www.enisa.europa.eu/publications/cloud-in-finance, 2015

ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014, 2015

Threat Landscape and Good Practice Guide for Internet Infrastructure. [online] Available at: https://www.enisa.europa.eu/publications/iitl, 2015

Threat Landscape and Good Practice Guide for Smart Home and Converged Media. [online] Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence, 2014

ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats, 2013

ENISA Threat Landscape, Mid-year 2013. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-mid-year-2013, 2013

ENISA Threat Landscape - Responding to the Evolving Threat Environment. [online] Available at: https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape, 2013

Legislation

Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0611&rid=1, 2013

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - Achievements and next steps: towards global cyber-security. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0163&from=EN, 2011

Proposal for a Regulation of the European Parliament and of the Council establishing a European Securities and Markets Authority. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009PC0503&rid=1, 2009

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. [online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF, 2009

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&rid=5, 2008

Green Paper on a European Programme for Critical Infrastructure Protection. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52005DC0576, 2005

Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32004R0883R(01), 2004

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en, 2002

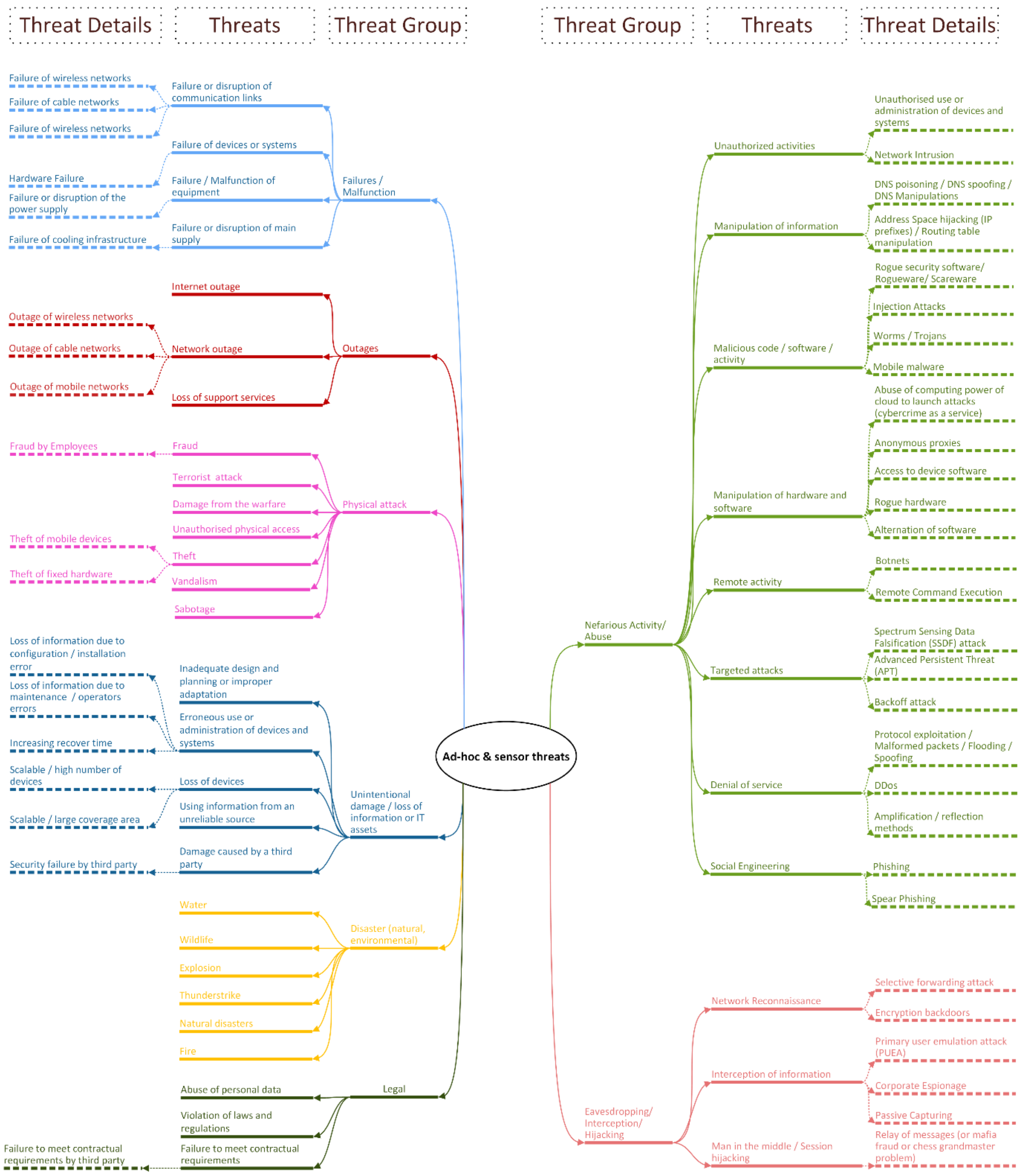
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=1, 1995

Annex A: Ad-hoc and sensor network assets matrix for specific use cases

	USE CASES ***1. ULTRA-WIDEBAND COMMUNICATIONS AND APPLICATIONS*** ***2. RFID APPLICATIONS AND PROTOCOLS*** ***3. MOBILE CLOUD COMPUTING AND MOBILE SOCIAL NETWORKING*** ***4. SOFTWARE-DEFINED AD-HOC, AND SENSOR NETWORKS*** ***5. BODY NETWORKS AND E-HEALTH***					
Domain	***Assets***	***1***	***2***	***3***	***4***	***5***
Device	Support systems	☒	☒	☒	☒	
	RFID tags, smart cards, etc.		☒			
	Radars (i.e. range finders, motion detectors)	☒				
	Wearable IT devices (i.e. fitness trackers, accelerometers)	☒	☒		☒	☒
	Interconnection points	☒	☒	☒		☒
	Mobile devices (i.e. IoT, tablets, mobile phones)	☒	☒	☒		
	RFID reader (i.e. smartphones, tablets, stand-alone devices)		☒			
	Indoor positioning systems	☒	☒		☒	
	Car and vehicles	☒	☒	☒	☒	
	CE devices (i.e. Cameras, DVD, PVR, HDTV)	☒				
Network	Mobile user and location registers	☒	☒	☒		
	Mobile base stations and controllers	☒	☒			
	Servers		☒	☒	☒	☒
	Routers & Switches (DSLAM, SBC, etc.)	☒		☒	☒	☒
	Routers (i.e. Intelligent network devices)		☒	☒	☒	☒
	Physical security systems	☒	☒		☒	
	PSTN switches			☒		
	Mobile switches			☒		
	Addressing servers			☒		
	Appliance control and integration with the smart grid and a smart meter				☒	
	PKI infrastructure		☒	☒		
	Radio (hardware and software)	☒	☒			
	Home automation (i.e. for the elderly and disabled)	☒	☒		☒	
	Power supplies	☒	☒	☒	☒	☒
	Cooling systems			☒		
	Communication protocols (i.e. Usage of unsecure communication channel in Wi-Fi networks)			☒	☒	☒
Applications	Data (i.e. financial, private, confidential)	☒	☒	☒	☒	☒
	Critical applications (i.e. Billing and mediation systems)	☒	☒	☒	☒	☒
	Cloud based Clinical information system (CIS)					☒
	eHealth (i.e. web-services, portals)					☒

	eHealth Private Healthcare Information (PHI) database	☒	☒			☒
Operational	Physical security (i.e. alarms, object tracking)	☒	☒		☒	☒
	Utilities (i.e. measurement, billing of utilities)	☒	☒	☒	☒	☒
	Control systems (i.e. HVAC - home energy monitors over the internet)		☒		☒	
Product/ business process	Transportation (i.e. fleet management, toll payment)	☒	☒	☒		
	Healthcare (i.e. eHealth security, personal security)	☒			☒	☒
	Manufacturing (i.e. production chain monitoring)		☒	☒	☒	
	Supply and provisioning (i.e. freight supply, distribution monitoring, vending machines)		☒	☒	☒	

Annex B: Ad-hoc and Sensor Networks’ Full Threat Taxonomy


Threat Details
Threats
Threat Group
Threat Group
Threats
Threat Details
Ad-hoc & sensor threats
Failure of wireless networks
Failure of cable networks
Failure of wireless networks
Failure or disruption of communication links
Failure of devices or systems
Hardware Failure
Failure or disruption of the power supply
Failure / Malfunction of equipment
Failures / Malfunction
Failure of cooling infrastructure
Failure or disruption of main supply
Internet outage
Outage of wireless networks
Outage of cable networks
Network outage
Outages
Outage of mobile networks
Loss of support services
Fraud by Employees
Fraud
Terrorist attack
Damage from the warfare
Physical attack
Unauthorised physical access
Theft of mobile devices
Theft
Theft of fixed hardware
Vandalism
Sabotage
Loss of information due to configuration / installation error
Inadequate design and planning or improper adaptation
Loss of information due to maintenance / operators errors
Erroneous use or administration of devices and systems
Increasing recover time
Scalable / high number of devices
Loss of devices
Unintentional damage / loss of information or IT assets
Scalable / large coverage area
Using information from an unreliable source
Damage caused by a third party
Security failure by third party
Water
Disaster (natural, environmental)
Wildlife
Explosion
Thunderstrike
Natural disasters
Fire
Abuse of personal data
Legal
Violation of laws and regulations
Failure to meet contractual requirements by third party
Failure to meet contractual requirements
Unauthorised use or administration of devices and systems
Unauthorized activities
Network Intrusion
DNS poisoning / DNS spoofing / DNS Manipulations
Manipulation of information
Address Space hijacking (IP prefixes) / Routing table manipulation
Rogue security software/ Rogueware/ Scareware
Injection Attacks
Worms / Trojans
Malicious code / software / activity
Mobile malware
Abuse of computing power of cloud to launch attacks (cybercrime as a service)
Anonymous proxies
Access to device software
Manipulation of hardware and software
Rogue hardware
Alternation of software
Botnets
Remote activity
Remote Command Execution
Nefarious Activity/ Abuse
Spectrum Sensing Data Falsification (SSDF) attack
Targeted attacks
Advanced Persistent Threat (APT)
Backoff attack
Protocol exploitation / Malformed packets / Flooding / Spoofing
Denial of service
DDos
Amplification / reflection methods
Social Engineering
Phishing
Spear Phishing
Selective forwarding attack
Network Reconnaissance
Encryption backdoors
Primary user emulation attack (PUEA)
Interception of information
Corporate Espionage
Eavesdropping/ Interception/ Hijacking
Passive Capturing
Man in the middle / Session hijacking
Relay of messages (or mafia fraud or chess grandmaster problem)

Annex C: Associations between threats and countermeasures

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
Unintentional damage / loss of information or IT assets	Inadequate design and planning / improper adaptation	[8.3].1, [8.4].1, [8.5].1, [8.6].1-5, [8.6].14, [8.7].1-3, [8.7].15					[8.3].1, [8.4].1, [8.4].3, [8.6].1-3, [8.6].14, [8.7].1	[8.7].15	[8.3].1, [8.5].1, [8.6].1, [8.6].3-5, [8.7].2-3, [8.7].15		
	Using information from unreliable source	[8.3].1, [8.4].3, [8.6].2, [8.6].6-7, [8.6].14, [8.6].21-22, [8.7].2, [8.7].11, [8.7].15, [8.8].1					[8.3].1, [8.4].3, [8.6].2, [8.6].6-7, [8.6].14, [8.6].21	[8.3].1, [8.6].6-7, [8.6].21, [8.7].15, [8.8].1	[8.3].1, [8.4].3, [8.6].6-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5		
	Loss of devices	[8.3].1-2, [8.6].2-4, [8.6].14					[8.3].1-2, [8.6].2-3	[8.3].1-2, [8.6].20	[8.3].1-2, [8.6].4		
	Loss of information in the cloud	[8.1].1, [8.3].1, [8.4].3, [8.5].1, [8.6].5-6,					[8.1].1, [8.3].1, [8.4].3, [8.6].6	[8.1].1, [8.3].1, [8.6].6, [8.7].15	[8.1].1, [8.3].1, [8.4].3, [8.5].1, [8.6].5, [8.7].2,		

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
		[8.7].2, [8.7].15							[8.7].15		
Disaster (natural, environmental)	Damage caused by third party	[8.1].1, [8.2].1, [8.3].1, [8.4].3, [8.5].5, [8.6].5-7, [8.6].14, [8.6].21, [8.7].2, [8.7].11, [8.7].15, [8.8].1					[8.1].1, [8.2].1, [8.3].1, [8.4].3, [8.6].6-7, [8.6].14, [8.6].21	[8.1].1, [8.2].1, [8.3].1, [8.5].5, [8.6].6-7, [8.6].21, [8.7].15, [8.8].1	[8.1].1, [8.2].1, [8.3].1 [8.4].3, [8.5].5, [8.6].5-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5		
	Water	[8.3].1, [8.6].2-5, [8.7].2			[8.4].13	[8.3].1, [8.6].11, [8.7].1	[8.3].1, [8.6].2-3, [8.7].1	[8.3].1	[8.3].1, [8.6].3-5, [8.7].2		[8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15
	Wildlife	[8.3].1, [8.6].2-5, [8.7].2			[8.4].13	[8.3].1, [8.6].11, [8.7].1	[8.3].1, [8.6].2-3, [8.7].1	[8.3].1	[8.3].1, [8.6].3-5, [8.7].2		[8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
	Explosion	[8.3].1, [8.6].2-5, [8.7].2			[8.4].13	[8.3].1, [8.6].11, [8.7].1	[8.3].1, [8.6].2-3, [8.7].1	[8.3].1	[8.3].1, [8.6].3-5, [8.7].2		[8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15
	Thunder strike	[8.3].1, [8.6].2-5, [8.7].2			[8.4].13	[8.3].1, [8.6].11, [8.7].1	[8.3].1, [8.6].2-3, [8.7].1	[8.3].1	[8.3].1, [8.6].3-5, [8.7].2		[8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15
	Natural disasters	[8.3].1, [8.6].2-5, [8.7].2			[8.4].13	[8.3].1, [8.6].11	[8.3].1, [8.6].2-3	[8.3].1	[8.3].1, [8.6].3-5, [8.7].2		[8.3].1, [8.4].4, [8.4].13, [8.6].3, [8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15
	Fire	[8.3].1, [8.6].2-5, [8.7].2				[8.3].1, [8.6].11	[8.3].1, [8.6].2-3	[8.3].1	[8.3].1, [8.6].3-5, [8.7].2		[8.3].1, [8.4].4, [8.4].13, [8.6].3,

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
											[8.6].13, [8.7].1, [8.7].4, [8.7].10, [8.7].15
Legal	Unauthorized use of intellectual property rights (IPR) protected resources		[8.6].1, [8.6].26								[8.8].35
	Abuse of personal data		[8.2].9-10, [8.6].26								[8.1].19, [8.2].13
	Violation of rules and regulations										[8.7].13
	Internet outage	[8.2].1, [8.3].1-3, [8.4].1, [8.4].3, [8.5].1, [8.5].5-6, [8.6].3, [8.6].6, [8.7].15, [8.6].22, [8.7].11, [8.8].1-2			[8.1].1, [8.2].1, [8.4].13, [8.5].5-7, [8.6].16, [8.7].5, [8.7].7, [8.7].15, [8.8].11	[8.1].1, [8.1].12-13, [8.2].1, [8.2].3-4, [8.4].3, [8.5].3, [8.6].8, [8.6].15, [8.8].10-11	[8.1].1, [8.2].1, [8.3].1-2, [8.4].1, [8.4].3, [8.6].3, [8.6].6, [8.6].21	[8.1].1, [8.1].14, [8.2].1-2, [8.2].6-7, [8.2].16, [8.3].1-3, [8.4].5-7, [8.5].4-6, [8.6].32-33, [8.6].35, [8.7].6, [8.7].15, [8.8].1, [8.8].13,	[8.1].1, [8.2].1, [8.3].1-3, [8.4].3, [8.5].1-2, [8.5].5, [8.6].3, [8.6].6, [8.7].15, [8.8].1	[8.3].3, [8.3].5, [8.4].16	[8.1].1, [8.2].1-5, [8.3].1, [8.3].3, [8.4].2-4, [8.4].13, [8.5].7, [8.6].3, [8.6].15, [8.7].6, [8.7].15, [8.8].8, [8.8].12, [8.8].17-18,

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
								[8.8].19			[8.8].20
	Network outage	[8.3].1-2, [8.4].1, [8.4].3, [8.5].2, [8.6].1-2, [8.6].6, [8.6].14		[8.1].6	[8.1].8-9, [8.2].1, [8.4].13, [8.6].10, [8.7].5, [8.7].7	[8.1].6-7, [8.1].10, [8.1].12-13, [8.2].4, [8.6].8	[8.3].1-2, [8.4].3, [8.6].1-2, [8.6].6	[8.1].7, [8.1].14, [8.2].1, [8.3].1-2, [8.4].5-7, [8.6].27-34, [8.6].37	[8.3].1-2, [8.4].3, [8.5].2, [8.6].6	[8.3].4	[8.1].2, [8.1].4-7, [8.2].4-5, [8.3].1, [8.3].5-7, [8.4].2-4, [8.4].13, [8.6].27, [8.7].10, [8.8].3-4, [8.8].14-15
	Loss of support services	[8.3].1, [8.4].1, [8.4].3, [8.6].1, [8.6].14			[8.1].1, [8.4].13, [8.7].5, [8.7].7	[8.1].1, [8.1].12-13, [8.2].3, [8.6].8, [8.6].11	[8.1].1, [8.3].1-2, [8.4].3, [8.6].1	[8.1].1, [8.1].14, [8.2].6-7, [8.3].1-2, [8.4].4-7, [8.7].6, [8.7].8, [8.2].16, [8.8].5	[8.1].1, [8.3].1-2, [8.4].3, [8.6].1	[8.3].4, [8.4].14	[8.1].1, [8.2].3-5, [8.3].1-2, [8.3].5-7, [8.4].2-4, [8.4].13, [8.7].6, [8.7].10, [8.8].15, [8.8].17, [8.8].25-26
Nefarious activity / abuse	Unauthorized activities		[8.1].15	[8.2].11				[8.1].1			
	Manipulation of information		[8.1].16					[8.1].1			[8.2].14, [8.2].17-18 [8.8].39

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
	Malicious code / software / activity		[8.6].17, [8.6].21-22								[8.1].17-18
	Manipulation of hardware and software		[8.6].7, [8.6].23-24	[8.8].7, [8.8].27-28				[8.8].31			[8.1].22-23, [8.2].15, [8.2].20, [8.3].11, [8.4].20, [8.8].4, [8.8].38
	Misuse of audit tools		[8.3].10, [8.6].1, [8.6].25								[8.3].9
	Remote activity		[8.6].17, [8.6].21-22								[8.8].4, [8.8].36
	Targeted attacks		[8.6].17, [8.6].21	[8.2].12							[8.8].30
	Denial of service			[8.8].29							[8.2].17, [8.3].8, [8.7].12, [8.8].20, [8.8].32-34
	Social Engineering		[8.2].8, [8.3].10, [8.8].1								[8.7].14
Eavesdropping, Interception, Hijacking	Network Reconnaissance	[8.3].1, [8.3].3, [8.5].1,					[8.3].1, [8.6].6, [8.6].14,	[8.1].14, [8.3].1, [8.3].3,	[8.3].1, [8.3].3, [8.5].1,		[8.2].4, [8.8].4, [8.8].25

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
		[8.6].6, [8.6].14, [8.6].21, [8.7].2, [8.7].15, [8.8].1-2					[8.6].21	[8.6].6, [8.6].21, [8.6].31, [8.8].1, [8.8].24	[8.7].2, [8.7].15, [8.8].1, [8.8].5		
	Interception of information	[8.2].1, [8.3].1, [8.3].3, [8.5].1, [8.6].1, [8.6].5-6, [8.6].14, [8.6].21, [8.7].2, [8.7].15, [8.8].1-2					[8.2].1, [8.3].1, [8.6].1, [8.6].6, [8.6].14, [8.6].21	[8.1].14, [8.2].1, [8.2].6, [8.2].8, [8.3].1, [8.3].3, [8.5].5, [8.6].6, [8.6].18-21, [8.6].27-32, [8.6].34-37, [8.8].1, [8.8].21, [8.8].23	[8.2].1, [8.3].3 [8.4].3, [8.5].1, [8.6].1, [8.6].5-7, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5		[8.2].4, [8.2].16, [8.8].20
	Intercepting compromising emissions	[8.3].1-3, [8.5].1, [8.6].1, [8.6].5-7, [8.6].14, [8.6].21, [8.7].2, [8.7].15, [8.8].1-2					[8.2].1, [8.3].1-2, [8.6].1, [8.6].6-7, [8.6].14, [8.6].21	[8.1].14, [8.2].1, [8.2].8, [8.3].1-3, [8.6].6-7, [8.6].19-21, [8.6].27-32,	[8.2].1, [8.3].1-3, [8.4].3, [8.5].1, [8.6].1, [8.6].5-7, [8.6].21, [8.7].2, [8.7].15,		[8.2].4, [8.2].16, [8.8].3, [8.8].20

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
								[8.6].34-37, [8.8].1, [8.8].21-24	[8.8].1, [8.8].5		
	Man-in-the-middle / Session hijacking	[8.2].1, [8.3].1, [8.3].3, [8.5].1, [8.6].6, [8.6].14, [8.6].21, [8.7].15, [8.7].2, [8.8].1-2		[8.2].11			[8.2].1, [8.3].1, [8.6].6, [8.6].14, [8.6].21,	[8.1].14, [8.2].1, [8.2].6, [8.2].8, [8.3].1, [8.3].3, [8.6].6, [8.6].21, [8.6].27, [8.6].31, [8.6].35, [8.8].1, [8.8].21, [8.8].24	[8.2].1, [8.3].1, [8.3].3, [8.4].3, [8.5].1, [8.6].6, [8.6].21, [8.7].2, [8.7].15, [8.8].1, [8.8].5		[8.2].4, [8.2].16, [8.8].4
Failures / Malfunction	Failure or disruption of communication links	[8.3].1, [8.6].3		[8.4].1, [8.4].9	[8.6].10, [8.7].7		[8.3].1, [8.6].3	[8.3].1, [8.4].6-9, [8.6].18-25, [8.6].36, [8.8].21-24	[8.3].1, [8.6].3-4		[8.3].1, [8.4].1, [8.4].6, [8.6].3, [8.6].13, [8.8].16
	Failure of devices or systems	[8.3].1, [8.6].3, [8.6].14, [8.6].22		[8.4].1, [8.4].9, [8.4].12	[8.4].17, [8.6].10	[8.4].16, [8.6].8	[8.3].1, [8.6].3, [8.6].7, [8.6].14	[8.3].1, [8.4].6, [8.4].9, [8.4].18, [8.6].12, [8.7].6	[8.3].1, [8.6].3-7		[8.3].1, [8.4].1, [8.4].6, [8.4].9, [8.6].3,

THREAT GROUP	THREAT	GOOD PRACTICES									
		CPNI	ITU	IEC	FTC	GSMA	SECURING SMART CITIES	NIST	Q-CERT	SANDIA	OTHER
											[8.6].13-14, [8.7].6, [8.8].6-7
	Malfunction of equipment	[8.3].1, [8.6].3, [8.6].14		[8.4].9	[8.4].17, [8.6].6, [8.6].10	[8.4].16	[8.3].1, [8.6].3, [8.6].14	[8.3].1, [8.4].5-6, [8.4].9, [8.4].10, [8.4].18, [8.6].12	[8.3].1, [8.6].3-5		[8.3].1 [8.4].6, [8.4].9, [8.6].3, [8.6].13-14
	Failure or disruption of main supply	[8.3].1, [8.6].3, [8.6].14		[8.4].9			[8.3].1, [8.6].3, [8.6].14	[8.3].1, [8.4].6, [8.4].9, [8.6].12	[8.3].1, [8.6].3-4		[8.3].1, [8.4].6, [8.4].9, [8.6].3, [8.6].13-14
Physical attack	Terrorist attack										
	Damage from the warfare										
	Unauthorized physical access										[8.4].19, [8.8].37
	Theft										
	Vandalism										[8.1].21
	Sabotage										[8.8].22

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)

Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-06-16-349-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-207-3
DOI: 10.2824/58281