OULUN YLIOPISTO
UNIVERSITY of OULU

FACULTY OF TECHNOLOGY

The use of IoT devices in logistics

Tapani Himanka

INDUSTRIAL ENGINEERING AND MANAGEMENT

Bachelor's Thesis

May 2016

OULUN YLIOPISTO
UNIVERSITY of OULU

FACULTY OF TECHNOLOGY

The use of IoT devices in logistics

Tapani Himanka

Thesis Supervisor: Majava J, University Lecturer

INDUSTRIAL ENGINEERING AND MANAGEMENT

Bachelor's Thesis

May 2016

ABSTRACT
FOR THESIS

University of Oulu Faculty of Technology

Degree Programme (Bachelor's Thesis, Master's Thesis) Industrial Engineering and Management		Major Subject (Licentiate Thesis)	
Author Himanka, Tapani		Thesis Supervisor Majava, J, university lecturer	
Title of Thesis The use of IoT devices in logistics			
Major Subject	Type of Thesis Bachelor's Thesis	Submission Date May 2016	Number of Pages 32

Abstract

In this thesis the goal is to look into the possibilities to utilize the functionality of an IoT device to interface with the IoT systems involved in its own logistics process. For this goal the use of IoT technologies for logistics processes is studied and the potential for a wireless IoT device to interface with the used technologies is explored. The research is done by literary study of recent articles and technology specifications. They key technologies are identified and concentrated on this thesis.

The thesis finds that the global standards for technologies involved in logistics processes are not very well established, but some trends and popular technologies are identified. The best potential for interfacing with logistics processes are through wireless sensor networks using ZigBee or Bluetooth LE.

The results of this thesis can be used for further inquiry in logistics processes utilized by logistic service providers. Only compatibility of standards and technologies were studied without going into detail with the physical phenomena involved with the wireless communications.

Additional Information

TIIVISTELMÄ
OPINNÄYTETYÖSTÄ Oulun yliopisto Teknillinen tiedekunta

Koulutusohjelma (kandidaatintyö, diplomityö) Tuotantotalous		Pääaineopintojen ala (lisensiaatintyö)	
Tekijä Himanka, Tapani		Työn ohjaaja yliopistolla Majava, J, yliopistonlehtori	
Työn nimi IoT-laitteiden käyttö logistiikassa			
Opintosuunta	Työn laji Kandidaatintyö	Aika Toukokuu 2016	Sivumäärä 32

Tiivistelmä

Tässä kandidaatintyössä tutkitaan mahdollisuuksia hyödyntää IoT-laitteen toiminnallisuutta olla yhteydessä laitteen omassa logistiikkaprosessissaan käytettäviin IoT-järjestelmiin. Tarkoitusta varten perehdytään IoT-teknologioiden käyttöön logistiikkaprosesseissa, ja tutkitaan laitteen mahdollisuuksia muodostaa yhteys käytettyjen teknologioiden kanssa. Työ on tehty kirjallisuustutkimuksena tuoreista artikkeleista ja teknologioiden spesifikaatioista. Keskeisimmät teknologiat tunnistetaan ja niihin keskitytään tässä työssä.

Kandidaatintyössä havaitaan, että globaalit standardit aiheeseen liittyvissä teknologioissa eivät ole kovinkaan vakiintuneita, mutta trendejä ja suosittuja teknologioita tunnistetaan. Todetaan, että parhaat mahdollisuudet yhteyden muodostamiseen logistiikkaprosesseihin, on langattomien sensoriverkkojen kautta hyödyntäen joko ZigBeetä tai Bluetooth LE:tä.

Työn tuloksia voidaan hyödyntää jatkotutkimukseen logistiikkapalveluntarjoajien logistiikkaprosesseista. Tutkimus tehtiin ainoastaan perehtymällä standardien ja teknologioiden yhteensopivuuteen ja langattoman tiedonsiirron fysikaalisiin ilmiöihin tarkemmin perehtymättä.

Muita tietoja

SISÄLLYSLUETTELO

Abbreviations

DVB-RCS	Digital Video Broadcasting-Return Channel via Satellite
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HART	Highway Addressable Remote Transducer
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IPv6	Internet Protocol version 6
LAN	Local Area Network
LoWPAN	Low power Wireless Personal Area Network
LR-WPAN	Low-rate Wireless Personal Area Network
M2M	Machine to Machine
NFC	Near Field Communication
PAN	Personal Area Network
P2P	Peer-to-Peer
QoS	Quality of Service
RFID	Radio-Frequency Identification
SOA	Service Oriented Architecture
TCP/IP	Transmission Control Protocol / Internet Protocol
TETRA	Terrestrial Trunked Radio
UMTS	Universal Mobile Telecommunications System
UWB	Ultra-Wide Band
WAN	Wide Area Network
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network
WSAN	Wireless Sensor Actuator Network
6LoWPAN	IPv6 over Low power Wireless Personal Area Network

1 INTRODUCTION

The subject of this Bachelor's thesis is Internet of Things (IoT) in logistics. The Idea for the subject came from a company in the industry. Specifically, interest was to look into the possibilities to utilize the functionality of a wireless IoT device to improve its own logistics process and if the data collected by the device could be used to improve customer experience.

Internet of things is a rapidly growing industry and IoT technologies are widely utilized also in logistics processes. There is a lot of new research done in this area, but the rising popularity and constantly emerging new applications of IoT technology leaves a lot of questions fairly unexplored.

In this thesis the focus is in finding the technologies and practices currently used for tracking goods in logistics processes and what kind of new technologies are being developed to that end. The communication capabilities of wireless IoT devices are also explored.

Research questions for the thesis are:

1. How are IoT technologies used for tracking in logistics processes?

2. What is the potential for a wireless IoT device to interface with the tracking systems used in its own delivery process?

The research is done by literary study of recent articles and the specifications of the technologies involved. The communication technologies that are utilized by wireless IoT devices and logistics systems are identified and focused on. The possible synergies and restrictions are discussed. The goal is to find where in the supply chain from device manufacturer to the customer there is potential to benefit from communication between the delivered wireless IoT device and the logistics system, and where more detailed research on the matter should be encouraged.

2 INTERNET OF THINGS

2.1 Overview of IoT

The concept of Internet of Things has its origins in 1999 work done by researchers in Massachusetts Institute of Technology (MIT). The idea was put forth by Neil Gereshenfeld from the MIT Media Lab in his book "When Things Start to Think". The former head of Auto-ID Center at the same institute, Kevin Ashton, is quoted as the first person to use the term "Internet of Things" in the title of a presentation he made at Procter & Gamble in 1999. (Sachs et al. 2010)

Höller et al. (2014) describe the paradigm of IoT in contrast to the older and broader concept of Machine to Machine (M2M) communication in the following way: *"In contrast to M2M, however, IoT also refers to the connection of such systems and sensors to the broader Internet, as well as the use of general Internet technologies. In the long term, it is envisaged that an IoT-ecosystem will emerge not dissimilar to today's Internet, allowing things and real world objects to connect, communicate, and interact with one another in the same way humans do via the web today."*

Atzori et al. (2010) have a similar take on the generality of the communication technologies in IoT: *"In fact, "Internet of Things" semantically means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols". This implies a huge number of (heterogeneous) objects involved in the process."*

2.1.1 Ubiquitous Computing

A concept closely related to Intenet of Things is the paradigm of "Ubiquitous Computing". The term coined by Weiser (1991) describes the phenomenon that human awareness of computers disappear due to the seamless integration of computers into the world at large, which is in contrast to personal computing. When mostly machine to machine interaction is concerned, Ubiquitous Computing (UbiComp), also known as "Pervasive Computing", is also used similar to Internet of Things in literature. (Satyanarayanan, 2001)

2.1.2 Industrial internet

The originators of the term “Industrial internet”, Evans and Annuziata (2012), approach the theme from the perspective of smart entities, their data, and the analytical systems optimizing the smart entities. World Economic Forum has defined industrial internet as “A short-hand for the industrial applications of IoT, also known as the Industrial Internet of Things, or IIoT” (WEF, 2015). The term “Industrial internet” comprehends the non-consumer side of IoT, and in an industrial setting these terms are often used interchangeably.

2.2 IoT architecture

There is not one unified architecture for IoT applications. Different models have been proposed and there is a multitude of practical solutions already implemented. Gubbi et al. (2013) divide IoT in three components that enable seamless Ubiquitous Computing: “(a) Hardware—made up of sensors, actuators and embedded communication hardware (b) Middleware—on demand storage and computing tools for data analytics and (c) Presentation—novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications”. They further identify the most important enabling technologies for IoT as Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Addressing schemes, Data storage and analytics, Visualization.

Similar three level generalized descriptions take many forms in literature, with an application at the top connected by some kind of middleware to the physical layer, often named “things”, “objects” or “devices” that perform the function of indentification, sensing and communication. In addition to these functions, actuation in the form of Actuator Networks or combined Wireless Sensor and Actuator Networks (WSAN) can be part of IoT system, for interaction with physical world. (Gubbi et al. 2013, Atzori et al. 2010)

2.2.1 Middleware

For middleware of IoT, the Service Oriented Architecture (SOA) approach is gaining popularity. The adoption of the SOA principles allows for decomposing complex and monolithic systems into applications consisting of an ecosystem of simpler and well-

defined components. According to Atzori et al. (2010): *"The se of common interfaces and standard protocols gives a horizontal view of an enterprise system. Thus, the development of business processes enabled by the SOA is the result of the process of designing work-flows of coordinated services, which eventually are associated with objects actions. This facilitates the interaction among the parts of an enterprise and allows for reducing the time necessary to adapt itself to the changes imposed by the market evolution. A SOA approach also allows for software and hardware reusing, because it does not impose a specific technology for the service implementation."*

Figure 1. is describes the proposal by Atzori et al. (2010) for the general architecture of the middleware that tries to encompass all the functionalities, that address the problems previous proposed models have not: abstracting the devices functionalities and communications capabilities, providing a common set of services and an environment for service composition.

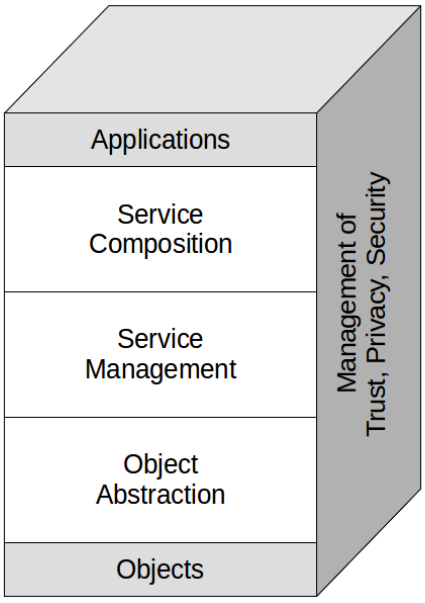

Figure 1. SOA-based architecture for the IoT middleware (adapted from Atzori et al. 2010).

Another future vision by Spiess et al. (2009) for an architecture in the enterprise setting is depicted in Figure 2. In this vision, future infrastructures are seen as service-oriented:

"As such, new functionality will be introduced by combining services in a cross-layer form, i.e. services relying on the enterprise system, on the network itself and at device level will be combined. New integration scenarios can be applied by orchestrating the services in scenario-specific ways. In addition, sophisticated services can be created at any layer (even at device layer) taking into account and based only on the provided functionality of other entities that can be provided as a service]. In parallel, dynamic discovery and peer-to-peer communication will allow to optimally exploit the functionality of a given device. It is clear that we move away from isolated stand-alone hardware and software solutions towards more cooperative models."

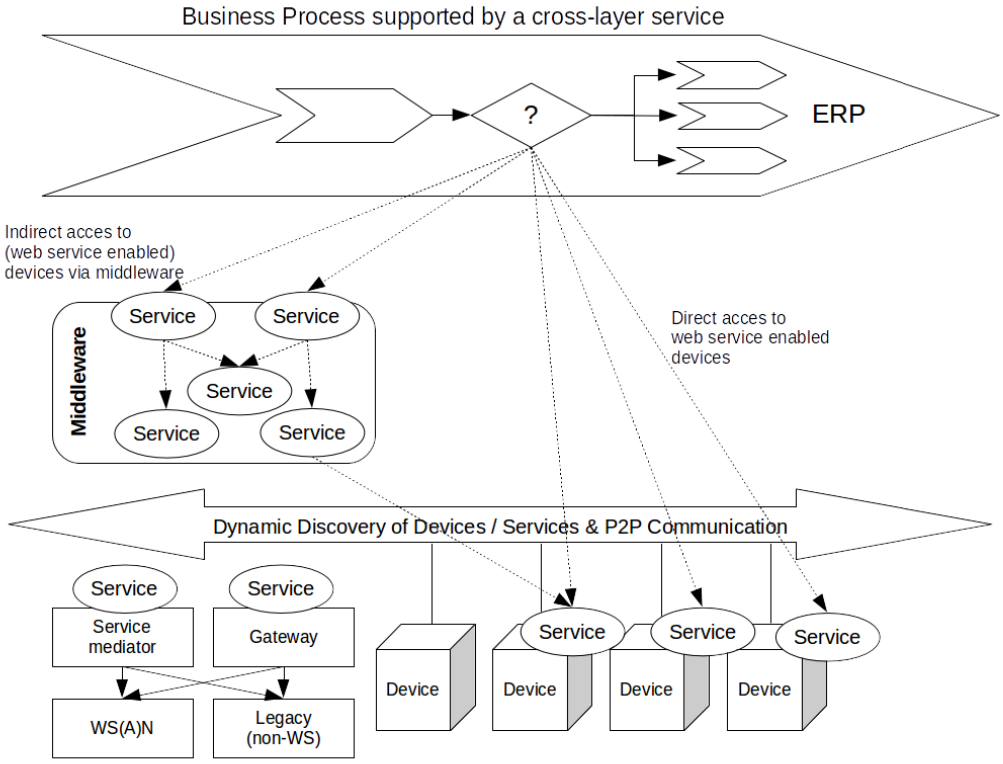

Figure 2. A vision of web service mashups (adapted from Spiess et al. 2009).

2.2.2 Future directions

The five-layered architecture of current Internet, running with TCP/IP protocols faces problems with the new requirements that come from adoption of IoT. Billions of connected objects create much larger traffic and need a lot more data storages. Also considerations like security and governance need to be addressed. A redesign of a new architecture is a very complex project, which needs to consider many factors like reliability, scalability, modularity, interoperability, interface, QoS, etc. As more devices

are connected, Internet of Things could also be divided to different application systems to restrict excessive traffic between devices that do not have the need to be connected with some other types of devices.

Muhonen (2015) predicts that, in the future, there will be some official Industrial internet and IoT standards, but some will be de facto standards, agreed by industry forums or alliances or dictated by companies in decisive roles. The most widely used and the strongest standards will be in communications and networking. Due to technical and business reasons, properties such as data and semantic interoperability, software platforms and data-analysis, will see more domain specific standards and proprietary solutions. Especially, software platforms are currently under a lot of competition by multiple players in the field, and customer interests drive towards open interfaces.

2.3 Wireless communication technologies in IoT

Internet of Things utilizes various communication technologies. Most of the communication in IoT is wireless. Long-range technology includes Cellular Networks (GSM, UMTS, LTE), Worldwide Interoperability for Microwave Access (WiMAX), and Terrestrial Trunked Radio (TETRA). Satellites are also utilized in Global Positioning System (GPS) and Digital Video Broadcasting-Return Channel via Satellite (DVB-RCS). In this work the focus is on short-range wireless and sensing technology. Some of the most relevant of such technologies, which were found to be used in harbor environment are presented. (Cimino et al., 2015)

2.3.1 RFID

The development of Radio-Frequency IDentification (RFID) tags is where IoT started and it persists as the most used IoT technology today. RFID technology enables design of microchips for wireless data communication over radio waves. Compared to its predecessors, barcode and magnetic strip, it has the benefit of not needing to be visible or in contact. Depending on the type of the chip it can be read-only, write once - read many or read-and-write. The communication can also be encrypted. The RFID tag can be active, passive, semipassive or semiactive. Passive RFID tags are not battery powered and they use the power of the reader's interrogation signal to communicate the ID to the RFID reader. Active RFID tags are battery powered, have one or more antennas, one or more transponder and may operate on different frequencies. They also

have longer operating distance up to 200m. Of the several applications, the main application of active RFID tags is in port containers for monitoring cargo. Semipassive RFID tags have an on board power supply to power the controller or microchip and can contain additional devices, such as sensors. Semiactive RFID tags have active (powered) transceiver, but no active (powered) receiver, and can be used over long distances or in high interference environments. (Cimino et al. 2015, Gubbi et al. 2013, Yan, 2008).

2.3.2 Bluetooth

Bluetooth is an industrial data transmission technology for WPAN (Wireless Personal Area Network). It provides a standard, economical and safe way to exchange information between different devices through a secure short-range radio frequency. The Bluetooth specification has been designed with the primary goal of getting low power consumption, a short range (1-100m depending on the device class) and a low-cost production for compatible devices. The Bluetooth protocol works in the free frequencies of 2.45 GHz and utilizes frequency hopping to counteract interference problems. Bluetooth device is able to search for other Bluetooth devices covered by the radio signal within a radius of a few tens of meters. There is a new version (Bluetooth Low Energy (LE), Bluetooth Version 4.0+ or Bluetooth Smart), that is designed for IoT use and notably less power than the previous versions (with the same traffic sent). A lot of the saved power is gained from the utilization of a very low power sleep mode, where the device can be woken up very quickly if needed. Bluetooth LE also uses different channels and different modulation compared to Bluetooth “Classic”, but they can utilize the same antenna. A software radio implementation can provide compatibility with the Bluetooth LE and previous versions, but peripherals generally support only one or the other. (Bluetooth.com 2016, Cimino et al. 2015, Yick et al. 2008)

Bluetooth can form wireless LANs with less power dissipation and lower cost hardware compared to Wi-Fi. However, since Bluetooth is connection oriented, a master and slave connection must be established before data is exchanged. Master (or “central“) devices scan for other devices and Slave (or “peripheral“) devices advertise and wait for connections. This simple "one hop" network is called a piconet, and may include up to seven active slaves connected to one master. There is no limit on the maximum number of slaves connected to one master but only seven of them can be active at time, others have to be in so called parked state. The master unit of a piconet controls the traffic

within the piconet by means of polling the slaves according to any preferred algorithm. (Bluetooth.com 2016, Cimino et al. 2015, Mbientlab.com 2014, Suri and Rani 2007, Yick et al. 2008)

2.3.3 Wi-Fi

Wi-Fi is a telecommunication technology that enables end users to connect with each other through a local network wirelessly (WLAN) based on IEEE 802.11 standard. Wi-Fi is developed to provide high speed transmission with large radius (100m). To be able to cover the desired area, several Access Points (and related cell coverage) are cabled together in the local network, although they can also be connected wirelessly with a loss in spectral efficiency of the system. The local network can be connected to the Internet via a router and can use all the connectivity services offered by an Internet Service Provider (ISP). The basic cell of a Wi-Fi LAN is called a basic service set (BSS), which is a set of mobile or fixed stations. They can be interconnected to other BSSs through an architectural component called distribution system (DS) to form an arbitrary size and complexity extensive service set (ESS) network, which is often referred to as an infrastructure network. Independent basic service set (IBSS) configuration allows Wi-Fi stations to communicate directly without any AP. This type of LAN is often formed without pre-planning for only as long as it is needed. This type of operation is often referred to as an ad hoc network. (Cimino et al. 2015, Lee et al. 2007)

2.3.4 ZigBee

Lee et al. (2007) give a very comprehensive description of the properties of a ZigBee network in both available topologies: *"ZigBee over IEEE 802.15.4, defines specifications for lowrate WPAN (LR-WPAN) for supporting simple devices that consume minimal power and typically operate in the personal operating space (POS) of 10m. ZigBee provides self-organized, multi-hop, and reliable mesh networking with long battery lifetime. Two different device types can participate in an LR-WPAN network: a full-function device (FFD) and a reduced-function device (RFD). The FFD can operate in three modes serving as a PAN coordinator, a coordinator, or a device. An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor. They do not have the need to send large amounts of data and may only associate with a single FFD at a time. Consequently, the RFD can be*

implemented using minimal resources and memory capacity. After an FFD is activated for the first time, it may establish its own network and become the PAN coordinator. All star networks operate independently from all other star networks currently in operation. This is achieved by choosing a PAN identifier, which is not currently used by any other network within the radio sphere of influence. Once the PAN identifier is chosen, the PAN coordinator can allow other devices to join its network. An RFD may connect to a cluster tree network as a leave node at the end of a branch, because it may only associate with one FFD at a time. Any of the FFDs may act as a coordinator and provide synchronization services to other devices or other coordinators. Only one of these coordinators can be the overall PAN coordinator, which may have greater computational resources than any other device in the PAN."

2.4 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are a network of devices that collect data from the surrounding environment and communicate the information forward. Usually they are characterized by a distributed architecture, where the devices function in a relatively autonomous manner. They form a hierarchical or homogenous topology. In homogenous topology device nodes provide same functionality and in hierarchical topology specialized nodes perform specific functions. Such a division can be when some nodes are specialized to processing and routing, while other nodes are monitoring and collecting data. Hierarchical topology gives the advantage to optimize nodes for the tasks (for example data processing capabilities and energy consumption). Advantages of a homogenous topology is the resiliency of the network and the ease of replacing a node. Clustered structure, a hybrid topology, is often used, where the tasks of a node is dependent on its spatial and topological location. WSNs can be further classified to dynamic and static networks depending on if the nodes can arbitrary move or not, and to centralized or distributed depending on the allocation of tasks between the nodes. For example, a base station can take care of data processing in a centralized network. (Cimino et al. 2015)

Gubbi et al. (2013) list the following as the components of WSN monitoring network:

- ***"WSN hardware*** *— Typically a node (WSN core hardware) contains sensor interfaces, processing units, transceiver units and power supply. Almost always,*

they comprise of multiple A/D converters for sensor interfacing and more modern sensor nodes have the ability to communicate using one frequency band making them more versatile.

- ***WSN communication stack*** *— The nodes are expected to be deployed in an ad-hoc manner for most applications. Designing an appropriate topology, routing and MAC layer is critical for the scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base station. Node drop outs, and consequent degraded network lifetimes, are frequent. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet.*
- ***WSN Middleware*** *— A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner. This is based on the idea of isolating resources that can be used by several applications. A platform-independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture (OSWA). OSWA is built upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method (SWE) by the Open Geospatial Consortium (OGC).*
- ***Secure Data aggregation*** *— An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors. Node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important."*

2.4.1 Technology standards in WSN

There is a number of technology standards used in the formation of Wireless Sensor Networks. Here is a list of some of the most relevant with some main characteristics explained.

6LoWPAN IPv6-based Low power Wireless Personal Area Networks is designed for applications with low data rate devices that requires Internet communication. (Rawat et al. 2013, Yick et al. 2008).

IEEE 802.15.3 is a physical and MAC layer standard for high data rate WPAN, designed to support real-time multi-media streaming of music and video. The standard is used in devices such as, portable video electronics, wireless speakers and wireless connectivity for gaming, televisions, cordless phones and printers. (Yick et al. 2008).

IEEE 802.15.4 specifies media access control and the physical layer for low-rate wireless personal area networks (LR-WPANs). Wireless sensor applications using IEEE 802.15.4 include industrial, residential and environment monitoring, automation and control focusing on low complexity, low cost of deployment, and low power consumption. Devices in the star topology communicate with a central controller while in the peer-to-peer topology ad hoc and self-configuring networks can be formed. (Rawat et al. 2013, Yick et al. 2008).

ISA100.11a is targeted at industrial processing monitoring and control market, where loss of data can be costly for operators. Network behavior must be predictable, reliable, and tolerant of RF interference and harsh environmental conditions. It offers both meshing and star network topologies. (Wagner & Barton 2012, Yick et al. 2008).

WirelessHART is a wireless sensor networking technology based on the one of the most popular industrial protocols in use (Highway Addressable Remote Transducer Protocol) that is designed to support mesh, star, and combined network topologies. Compatibility with installed legacy and new wired HEART devices is the main reason for its utilization. (Yick et al. 2008, En.hartcomm.org, 2016)

ZigBee is targeted primarily at the home and office automation market, with instant and effortless network setup and affordable radio processors as key properties. ZigBee devices can form mesh networks connecting up to thousands of devices together. The devices use very little power and can operate on a cell battery for many years and due to these factors it is likely the most used technology in WSN use currently. (Karan et al. 2015, Wagner & Barton 2012, Yick et al. 2008).

Bluetooth is more known for its use in connecting peripherals to consumer devices for which it was originally designed. The connection orientation used to be an obstacle for forming a Bluetooth WSN with the previous versions of Bluetooth. According to Yic et al. (2008): *"Experimental results indicate that Bluetooth-based sensor networks using BTnodes are suitable for applications that are active over a limited time period with a*

few unpredictable traffic bursts. BTnodes can achieve high throughput; however, they consume a lot of energy even when idle. Connection maintenance is expensive and dual radios are needed to support multi-hop routing. Hence, Bluetooth can only serve as an alternative to broadcast radios."

However, more recent studies have shown that utilization of new kind of network topology can eliminate the need of two radios for a node. Multiple piconets connected to each other is called a scatternet. A scatternet consists of two or more piconets with a shared slave node. A slave node cannot simultaneously connect to multiple masters, but it is possible to switch between two of them. In such a hybrid topology of star and mesh topologies each piconet conducts intra-piconet communication autonomously, while inter-piconet communication is routed through a shared slave. The resulting power consumption of the network is less than that of a more common Zigbee network when Bluetooth LE nodes are utilized this way. Bluetooth LE also connects faster than Zigbee and is gaining popularity as an option for WSN. (Karan et al. 2015).

2.4.2 Multi-party WSN

Recent development in the field is multi-party Wireless Sensor Networks. Being a multi-party environment means that the ecosystem comprises multiple administrative domains or parties, which have interest in the same sensor data. At the moment, in most solutions, third parties have only access to a data repository supplied by the WSN owner, but in the future third parties may be given direct access to the nodes. WSN owner can then collect fee for this service. WSNs are also multi-application environments, since they usually are not single purpose. WSNs are also considered dynamic environments, because both the nodes and the applications that utilize them change. Nodes disappear and new appear, new applications are created and old applications updated. (Maerien et al., 2015).

For the purpose of providing a secure way to share a WSN, developers of SecLooCI WSN middleware, Maerien et al. (2015) propose a role model for multi-party WSNs, that can be used to develop a middleware to support the sharing of nodes. In the model three roles are described:

- The Application Owner (AO), who wants to use the WSNs to perform actuation or gather sensor data. The applications require certain resources from the sensor

node, such as sensing and storage capabilities. The use of the shared resources can be reimbursed from the AO by the PO.

- The Platform Owner (PO) is the owner of the sensor node platforms. PO can get faster Return on Investment on the deployment of a WSN from other parties that will pay for the use of the services provided by the nodes.
- The Network Owner (NO) manages the wireless network. The role of NO is to provide network and Internet capabilities to local nodes, much in the same way that currently Wi-Fi connections are provided to visitors by organizations in a specific location.

The relationship between these roles is clarified in Figure 3.

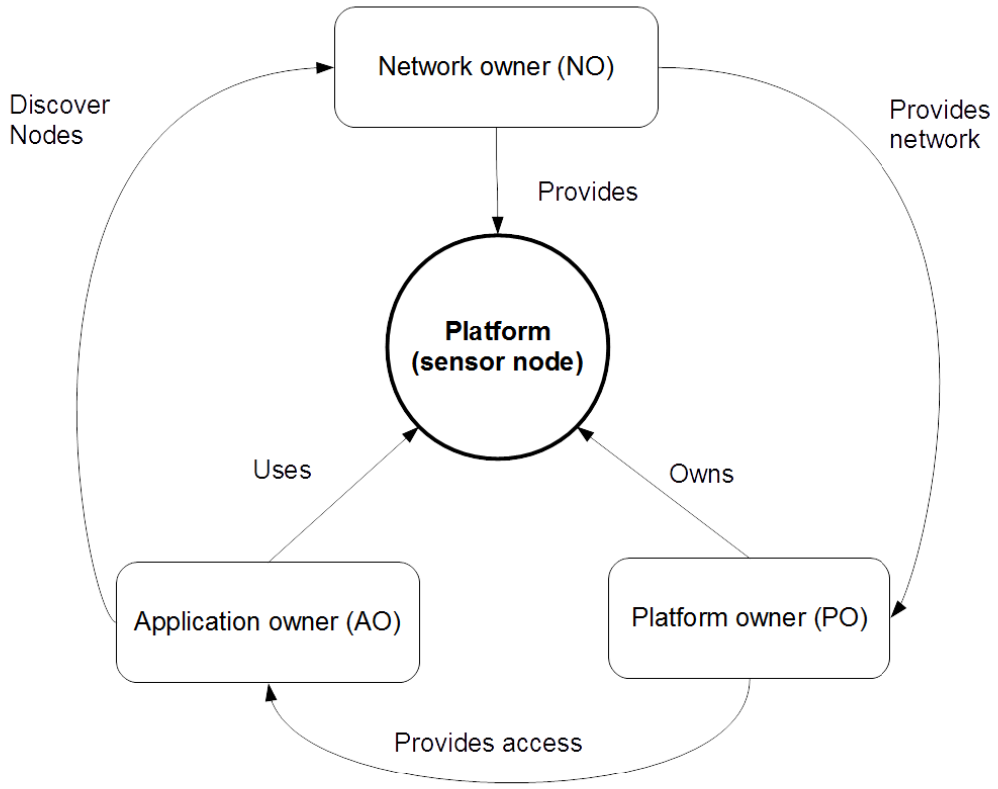

Figure 3. Overview of different roles in WSN (adapted from Marien et al. 2015)

Motivation for a AO to use a multi-user WSN is to avoid the costs of deploying a WSN of their own. PO and NO can collect revenue from the use of their services, or receive

services from the other parties in return. Marien et al. (2015) provide an example on how the roles can also be in the hands of a single entity:

*"**Combining roles** Each party can perform one or more of these roles depending on the situation. For example in the harbour context: the PO of the container nodes is likely also an AO since he will have an application monitoring the current state of the containers. The harbour authorities likely fulfil all three roles simultaneously: they provide networking to all containers currently in the WSN (NO), they have some static node infrastructure to allow for example localisation services (PO), and they have a monitoring application running on both their own nodes and foreign nodes to track all containers currently present in the harbour (AO)."*

3 IOT IN LOGISTICS

3.1 Logistics processes

The background of logistics is in the military. The term “logistics” appeared in literature as early as 1898 in the context of French military processes, and is later adopted into business usage relating essentially to the movement and transmittal of goods, services and information (Lummus et al. 2001). Cristopher (2011) defines logistics as essentially a planning orientation and framework that seeks to create a single plan for the flow of products and information through business. Figure 3. illustrates the total systems concept of linking marketplace and supplier base through the organization.

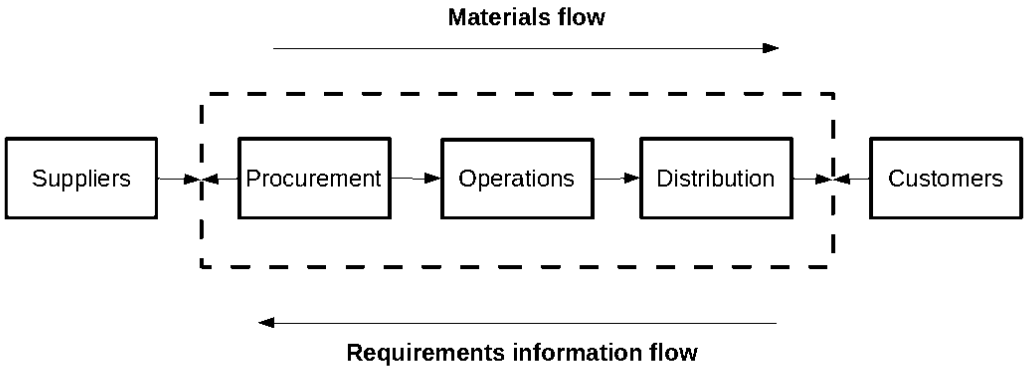

Figure 4. Logistics management process (adapted from Christopher, 2011)

Logistics is viewed as essential part of supply chain management. It involves planning, implementing and controlling efficient, effective flow and storage of goods and services from the beginning point of external origin to the company and from the company to the point of consumption for the purpose of conforming to customer requirements. The view in logistics is generally within a single company although it also manages flows between the company and its suppliers and customers. (Lummus et al. 2001).

Inbound and outbound logistics are included in Porter’s (1985) value chain concept as primary activities that are responsible of value creation. Porter does not describe what

value is created by said activities, but according to Lambert et al. (2008) logistics function is involved in creation of value through eight cross-functional processes identified by The Global Supply Chain Forum: customer relationship management, supplier relationship management, customer service management, demand management, order fulfillment, manufacturing flow management, product development and commercialization, and returns management.

3.2 Role of IoT in logistics

Logistics industry is a key player to benefit from IoT revolution. Logistics is a typically fragmented and low-margin industry, with tens of thousands of different suppliers with varying operating standards for local, domestic, and international operations. Being such a networked business, it will be necessary to adjust entire networks before implementing new solutions, which means substantial investments for any developments. However improvements in transportation and logistics will benefit all economic activities which rely on shipping of goods and on the reliability and efficiency of supply chains. Despite the costs involved in the investments, logistics industry has been the early adopters of IoT technologies, and many logistics vehicles today are already brimming with sensors, embedded processors, and wireless connectivity. The adoption of pallet or item-level tagging with RFID or other low cost technology is at the center of many applications of IoT. (www.dpdhl.com 2016, Evans and Annunziata, 2012).

DHL and Cisco (www.dpdhl.com, 2016) see the following driving forces for logistics providers to adopt IoT at an accelerating rate:

Technology push

- Mobile computing growing steadily with more mobile phones expected in 2020 than people in the world
- Due to the consumerization of IT, sensor technology has become more mature and affordable to be used for industry purposes in logistics
- With the move towards 5G, wireless communication will reach a new level of maturity connecting everything anytime
- Cloud computing and big data technologies will enable new data-based services

Need for logistics solutions

- High need for transparency and integrity control (right products, at the right time, place, quantity, condition and at the right cost) along the supply chain
- End consumers are asking for detailed shipment tracking to have transparency in real time
- Business customers are asking for integrity control especially for sensitive goods
- Logistics companies need transparency of networks and assets being used for ongoing optimization of efficiency and network utilization

DHL and Cisco (www.dpdhl.com, 2016) also have found a number of realized and potential use-cases in three different parts of logistics industry:

Warehousing operations

- Smart inventory management is possible when whole inventory is tagged
- Damage detection by pallet scanning with IoT connected cameras
- Real time visibility into inventory levels and conditions prevent out-of-stock situations and quality management of the stored material
- Accurate inventory control is possible when outbound gateway scans and ensures that correct items in correct order leave the storage.
- Optimal asset utilization is made possible by IoT connected machinery and vehicles.
- Predictive maintenance is made possible with sensors that measure physical stress of machinery in the transport systems.
- Health and safety improvements can be gained by reducing accidents by collisions with vehicles.
- Connected workforce can benefit from augmented reality interactions with machines with opt-in wearables, scanners and smartphones connected to the IoT system. Human performance and well-being can also be analyzed and improved.
- Smart warehouse energy management is made possible when lightning and devices can be switched off when not needed resulting in saved energy.

Cargo

- Location and condition monitoring. Information such as temperature, humidity, light, shock is collected and can tell a lot about the current state of a shipment.
- Theft prevention through clear vision on movement of goods allows fast reaction and prevents loss through inventory delays and the value of stolen goods.
- Fleet and asset management allows the analyzation of idle time and optimization of asset use.
- Health and safety benefits can be gained by alerting drivers about need to rest.
- Predictive asset lifecycle management. A truck can monitor itself for degradation and damages and the maintenance can be planned accordingly.
- End-to-end supply chain risk management benefits from the data collected by the system, which can be analyzed to enable automatic reaction to events like natural disasters and worker strikes.

Last-mile delivery

- Optimized collection is made possible by smart mail boxes, which inform end customer and logistics provider of deliveries and the conditions of the shipment.
- Automatic replenishment and anticipatory shipping reduce lead times. Automatic replenishment requires monitoring inventory levels at a retail store. Anticipatory shipping cuts lead times by moving goods closer to the customer by analyzing customer data before confirmation of a purchase is made.
- Monetizing and optimizing the return trip by connecting delivery people and vehicles with people who may have need for delivery and packing services.
- Next generation visibility on products is possible by monitoring items throughout the delivery for example for cold chain integrity of perishables.

3.2.1 IoT in container transport

Almost 90% of the world trade is transported in containers, which are delivered using different means of transportation including ships and trains. The container trade faces a lot of challenges comprising of container tracking, real time monitoring and intrusion detection, real time theft reporting mechanism, and status reporting of shipment items. Different IoT solutions are utilized to address these challenges. (Mahlknecht and Madani, 2007).

Shamsuzzoha et al. (2011) noticed in their pilot tracking project the difficulties communicating with GPRS-radio signals from within a container in ship transport. Interference from other signals and the contents of the container, not to mention the variable distances and angles to base station make this kind of connection very unreliable. Most proprietary systems had been mounted only on container doors without monitoring the inside of the container. Mahlknecht and Madani, (2007) proposed a hierarchical system to tackle this issue. In their model, an intra-container WSN nodes, called internal monitors (IM) would function as sensor nodes and connect to the container monitor (CM). There is one CM mounted on each container, and they have GSM and GPS connectivity that is used connecting directly to global communication, but if available, are connected to a prime monitor (PM). The PM is an infrastructure node on a ship or a train, and most energy-intensive communication goes through it. The general description of the model is depicted in Figure 5.

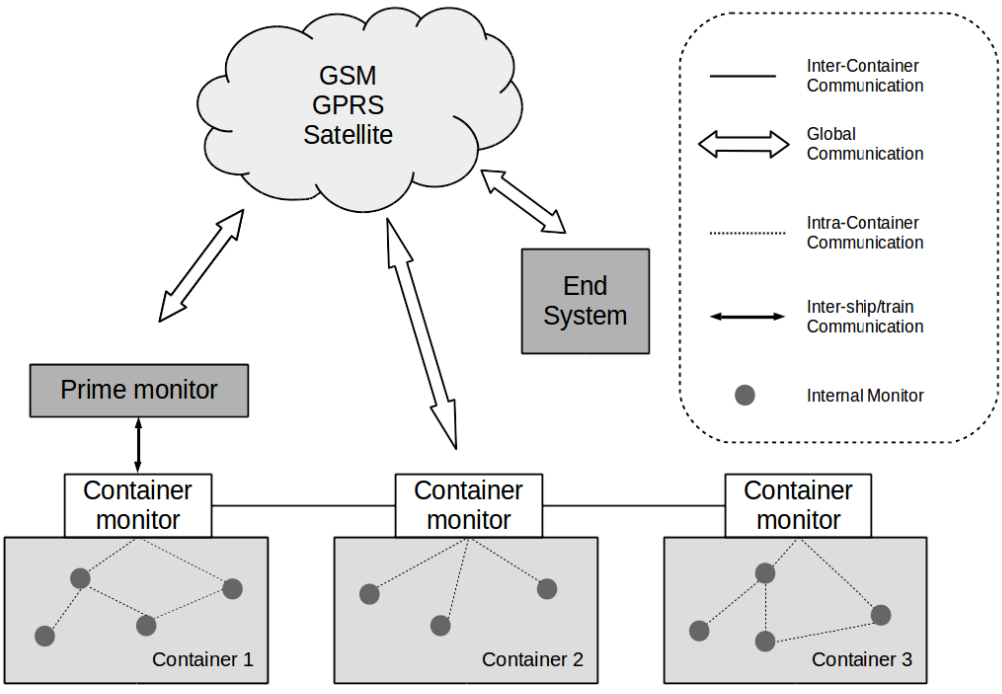

Figure 5. Overall system architechture for a container tracking WSN (adapted from Mahlknecht and Madani, 2007)

Maerien et. Al (2014) present a use case for the role model of a multi-party WSN, described in section 2.4.2. The case shows the reuse of existing sensor deployment for different uses by different parties in logistics context:

"For example, logistics providers install a fairly heavy weight sensor in their containers with performance similar to a smart phone to perform supply chain monitoring, with smaller sensors and actuators across the container. These sensors allow visibility of container status for all parties in the supply chain, assuming the logistics providers shares the sensor node data.

Many parties want to interact with the sensors of the containers: (1) the owners of the goods want to know the containers location and to ensure the goods are transported in a correct manner (limited shocks, no extreme temperatures, etc.), (2) harbour owners and customs require node access to enable localisation, monitor container access and ensure correct handling of goods, and (3) governments require access, temperature and location data for security reasons: in order for easy customs processing, it is necessary to prove container integrity and ensure supply chain visibility, as for example required by the US C-TPAT treaty (Customs-Trade Partnership Against Terror) or the European Authorised Economic Operator certificate. All these parties prefer live data to ensure freshness, integrity and the ability to immediately respond to potential issues. Retrieval of this data is assimilated in the sensor network to ensure the required freshness and integrity of data, requiring deployment of custom configurations and multi-party direct node access."

4 DISCUSSION

The purpose of this thesis was to look into these two research questions.

1. How are IoT technologies used for tracking in logistics processes?

2. What is the potential for a wireless IoT device to interface with the tracking systems used in its own delivery process.

Internet of Things is very widely used in logistics processes, which was very evident in the recent report by DHL and Cisco. The tracking with IoT begins with using affordable RFID tags or other wireless means at product item or palette level. Warehouses, logistic hubs, containers and vehicles can be equipped, and often are, with a wireless sensor network to monitor variables such as temperature, humidity, light and shock. At least the information of the location of the shipment is shared usually with the involved parties, and more use-cases are developed for the other data sensor networks can provide. Systems used for the tracking are usually proprietary and very diverse. The lack of global standards is currently somewhat limiting the progress in this area.

There is potential for a wireless IoT device to interface with the tracking system of its own delivery process. Basic requirement for such is that the device is using the same communication standards that logistics provider is using. Since the basic identification is mainly done with passive RFID tags, the best potential is to interface with wireless sensor networks. It seems that WSN:s are present at warehouses and logistic hubs, like harbors. Even inside of a container there can be some kind of WSN present. Bluetooth Low Energy and ZigBee appear to be the most viable communication technologies for such a thing, due to their low energy consumption in WSN use and wide adoption for this reason. However, also the software architecture has to be compatible. It appears that some kind of service oriented architecture is most likely implemented as middleware in a WSN. In the absence of any standard for it, object abstraction for the device in question needs to be implemented in it.

Stakeholders also need to be identified and the role of the device defined. Depending on the properties of the WSN, the device can be considered as a single sensor node in a wider sensor network or the devices can form a sensor network of their own connecting

to a local network owner. Since the logistics processes are already well equipped with sensors the device might not have any valuable data to provide to other stakeholders in the process. If the device cannot provide any valuable data, some cost for the energy use and the implementation costs to comply the device will possibly need to be compensated by some kind of fee. The motivation to interface with the device with some part of logistics system is mostly to gain internet access to deliver the own sensor data of the device for real time tracking by the device owner.

5 CONCLUSIONS

Internet of Things is a paradigm that is gaining popularity in many industries. The various aspects of IoT are not yet very well standardized although IoT is already widely in use. Many IoT implementations use service oriented architecture for middleware, which makes easier to produce applications for different purposes in a complex multi-device system. Wireless Senor Networks are the part of IoT that provide the sensory function that enables IoT to connect with real world. WSN can be dynamic, multi-party and multi-application systems, and its different roles can be owned by different entities.

Logistics industry can be seen as early adopters of IoT technology, and many of the processes involved are already utilizing IoT. There is a potential for various new use-cases, but the technology and its standardization is not yet mature enough for everything that is visioned. Products can be tracked at any point in the delivery process using IoT. WSNs can even convey real time data on different variables from inside cargo containers.

A IoT device that is being delivered, can potentially interface with the WSNs of the logistics system. The exact implementation details and costs involved are unknown, but the level of standard technologies will have great impact on it. Further research on the matter could be done by surveying the systems and standards logistics service providers are using in their processes to find out if there are some de facto standards in the industry. In the future, logistics service providers might provide connections to delivered devices much in the same way airports provide to travelling humans today.

REFERENCES

Atzori, L., Iera, A. and Morabito, G. 2010. The Internet of Things: A survey. *Computer Networks,* 54(15), pp.2787-2805.

Bluetooth.com. 2016. *Bluetooth Low Energy | Bluetooth Technology Website*. [online] Available at: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy [Accessed 27 May 2016].

Cimino, Mario GCA, et al. 2015. Wireless communication, identification and sensing technologies enabling integrated logistics: a study in the harbor environment. *arXiv preprint arXiv:1510.06175*.

Christopher, M. 2011. *Logistics and supply chain management.* 4th ed. London: Financial Times Prentice Hall.

www.dpdhl.com. 2016. *Internet of Things in Logistics: A collaborative report by DHL and Cisco on implications and use cases for the logistics industry*. [online] Available at: http://www.dpdhl.com/content/dam/dpdhl/presse/pdf/2015/DHLTrendReport_Internet_of_things.pdf [Accessed 29 May 2016].

En.hartcomm.org. 2016. WirelessHART Overview. [online] Available at: http://en.hartcomm.org/hcp/tech/wihart/wireless_overview.html [Accessed 28 May 2016].

Evans, P. and Annunziata, M., 2012. *Industrial internet: Pushing the boundaries of minds and machines*. General Electric, 21.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems,* 29(7), 1645-1660.

Höller J., Tsiatsis V., Mulligan C. 2014 *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence.* Oxford: Academic Press.

Karan N., Janhavi K., Mansi W., Zalak D., Vedashree R., Ganesh G., Jonathan J. 2015. Optimizing Power Consumption in IoT based Wireless Sensor Networks using luetooth Low Energy. Green Computing and Internet of Things (ICGCIoT), *2015 International Conference on, Isksue* Date: 8-10 Oct. 2015.

Lambert, D., García-Dastugue, S. and Croxton, K. 2008. The role of logistics managers in the cross-functional implementation of supply chain management. *Journal of Business Logistics,* 29(1), pp.113-132.

Lee, J. S., Su, Y.W., Shen, C.C. 2007. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*. IEEE, 2007. p. 46-51.

Lummus, R., Krumwiede, D. and Vokurka, R. 2001. The relationship of logistics to supply chain management: developing a common industry definition. *Industr Mngmnt & Data Systems,* 101(8), pp.426-432.

Maerien, J., Michiels, S., Hughes, D., Huygens, C., Joosen, W. 2015. SecLooCI: A comprehensive security middleware architecture for shared wireless sensor networks. *Ad Hoc Networks*, 25, pp.141-169.

Mahlknecht, S. and Madani, S. A. 2007. On architecture of low power wireless sensor networks for container tracking and monitoring applications. *Industrial Informatics, 2007 5th IEEE International Conference on*. IEEE, 2007. p. 353-358.

Mbientlab.com. 2014. *Bluetooth Low Energy Introduction | MbientLab Blog*. [online] Available at: http://mbientlab.com/blog/bluetooth-low-energy-introduction/ [Accessed 27 May 2016].

Muhonen, T. 2015. *Standardization of industrial internet and IoT (Internet of Things) – Perspective on condition based maintenance.* Thesis (MSc). University of Oulu.

Porter, M. 1985. *Competitive advantage.* New York: Free Press.

Sachs, K., Petrov, I. and Guerrero, P. 2010. *From active data management to event-based systems and more.* Berlin: Springer.
Rawat, P., Singh, K., Chaouchi, H., Bonnin, J. 2013. Wireless sensor networks: a survey on recent developments and potential synergies. *J Supercomput*, 68(1), pp.1-48.
Satyanarayanan, M. 2001. Pervasive computing: vision and challenges. *IEEE Pers. Commun.*, 8(4), pp.10-17.
Shamsuzzoha, A. H. M., Addo-Tenkorang R., Phuong D., Helo P. 2011. Logistics tracking: An implementation issue for delivery network. In: *Technology Management in the Energy Smart World (PICMET), 2011 Proceedings of PICMET'11:*. IEEE, 2011. p. 1-10.
Spiess, P. et al. 2009. SOA-based integration of the internet of things in enterprise services. *Web Services, 2009. ICWS 2009. IEEE International Conference on*. IEEE, 2009. p. 968-975.
Suri P. and Rani S. 2007. Bluetooth network-the adhoc network concept. *Proceedings 2007 IEEE SoutheastCon*.
Tan L., Wang N. 2010. Future internet: The internet of things. In: *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on* (Vol. 5, pp. V5-376). IEEE.
Wagner R. S., Barton R. J. 2012. Performance comparison of wireless sensor network standard protocols in an aerospace environment: ISA100. 11a and ZigBee Pro. In *Aerospace Conference, 2012 IEEE* (pp. 1-14). IEEE.
Weiser M. 1991. The Computer for the 21st Century. *Sci Am*, 265(3), pp.94-104.
World Economic Forum Working Group (WEF)., 2015. Industrial internet of things: Unleashing the potential of connected products and services. *World Economic Forum,* January 2015.
Yan, L. 2008. *The Internet of things: from RFID to the next-generation pervasive networked systems*. New York: Auerbach Publications.
Yick J., Mukherjee B., Ghosal D. 2008. Wireless sensor network survey. *Computer Networks*, 52(12), pp.2292-2330.