Smart and Secure Monitoring of Industrial Environments using IoT

Shruthi Puranik
Department of Computer Science and Engineering
National Institute of Technology
Karnataka, Surathkal, India
shruthi3093@gmail.com

Jayashree Mohan
Department of Computer Science and Engineering
National Institute of Technology
Karnataka, Surathkal, India
jayashree2912@gmail.com

K Chandrasekaran
Department of Computer Science and Engineering
National Institute of Technology
Karnataka, Surathkal, India
kch@nitk.ac.in

ABSTRACT

The Internet of Things (IoT) standard is giving rise to complex smart systems where in it has been made conceivable to captivate objects we experience in regular life, to interact and exchange information over a wireless network. The steep surge in industrialization and poor strategies used in controlling industrial pollution has resulted in degradation in the quality of environment around us. Negligence of leakage within an industry can result in massive hazards like the Bhopal Gas Tragedy. This paper proposes a secure IoT framework to smartly connect industrial surroundings. Our proposed framework helps in monitoring the level of pollutants, particulate matter and effluents released into the environment, notifying concerned authorities whenever their permissible level surpasses. Also we smartly connect the houses in close vicinity, so that precautionary measures can be taken to evacuate people in times of unexpected leakages. Our paper also discusses the various technologies and the security assessments being done to make it a complete secure system.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

Keywords

IoT, Wireless Sensor Networks (WSN), RFID, Gas sensors, Pollution, Secure IoT

1. INTRODUCTION

Internet of Things (IoT) [1] has undoubtedly rendered an overwhelming change to the lives of people, ranging from smart watch to smart cities [2]. Although the perception of IoT varies highly, in aggregate, it can be thought as an interconnection of physical and virtual objects which are capable of exchanging data or information with each other. In order to achieve the lateral, upward and downward communication between the "things" in the system, they are equipped with sensors, software, etc. Though constrained by the resources, communication can be set up between the objects to an appreciable extent. Some of the well known applications of IoT lie in the areas of health care, home automation, logistics, etc [3].

Increasing capabilities and reducing costs of the Radio Frequency Identification (RFID) [4] technology has motivated the development of IoT frameworks for applications of all sorts. In this paper RFID plays a vital role in identifying those factories contributing to higher industrial pollution.

The growing field of Wireless Sensor networks (WSN)[5] ,underwater sensor network [6] and gas sensors [7], few of which are though in its infancy have been considerably used in our framework to monitor pollution. There are high precision sensing technologies that are expensive for deployment, hence the emergence of a cost efficient WSN can be harnessed and readings of multiple sensors can be compared to obtain a near accurate value.

Since IoT is still in the growing phase, ensuring security of data exchanged in the wireless networks is a difficult task [8]. Because of the inherent wireless nature of IoT, it is susceptible to a wide range of attacks. Our framework deals with the transmission of sensitive information pertaining to industries. Hence it is important to ensure security of data in this matter.

This paper presents a framework to detect and monitor the level of industrial pollution and leakages anywhere over the city under consideration using sensor data. Active RFID tags, combined with sensors, form the proposed wireless sensor network based on IEEE 802.15.4.

The main objectives and requirements identified for our framework are:

- Design an architecture and describe the interaction of nodes.
- Ensure collaboration among the various nodes located at various geographical locations.
- Represent the data collected over the WSN graphically, by means of tables and charts.
- Notify the concerned authorities about exceeding levels of pollution in real time.

WCI '15, August 10 - 13, 2015, Kochi, India

DOI: http://dx.doi.org/10.1145/2791405.2791553

- Generate reports on a regular basis to provide an overview on how environment friendly every factory is.
- To enumerate the security requirements of the system like access control.
- To identify security vulnerabilities and risks and provide a solution to each of those.

The rest of the paper is organized as follows. Section III depicts the work that has been done in this area so far. In Section IV, we explain the proposed framework in detail. In Section V, we assess the possible threats to our framework and Section VI analyzes the security requirements of the system. The conceivable enhancements to the proposed system, that can be incorporated in future are described in Section VII.

2. MOTIVATION

Although industrialization has positively impacted the lives of people, on the other hand, environment is facing heavy degradation in the form of air and water pollution. The rate at which the pollution level is rising up is alarming. And, a substantial share of this pollution is attributed to the industrial wastes [9]. A recent report says that India spends $80 billion per year which amounts to 5.7% of its economy due to the environmental degradation [10]. So, it is really necessary to monitor the pollution level all the time and take measures to control the pollution. In this regard, we make an attempt to automate the process of monitoring pollution level by designing an IoT framework for the "things" involved and affected by the industrial pollution.

3. RELATED WORK

Surveys and studies conducted in different countries reveal that industrial waste is one of the major contributors to the degradation of the ecosystem [11, 12, 13]. It has hence become vital to address this issue of industrial pollution and leakage, and take necessary steps to curb them.

RFID technology [4] is a noteworthy achievement in the embedded communication paradigm which enables design of microchips for wireless data communication. They help in automatic identification of anything that is attached to it, acting as an electronic barcode. We harness this nature of RFID to tag each unit of the factory to monitor their emission levels.

Various applications of IoT have been developing rapidly over the past few years namely, Smart cities, logistics, medicine, fitness devices, transport and so forth [3].

IoT is now focusing on intelligent interactive applications, distributed systems and so on. This provokes the need for development of new methodologies to meet the reliability, security and privacy requirements [14]. Security for IoT must be enforced in each of the four layers of any IoT model, namely perceptual layer, network layer, support layer and application layer [8].

As the IoT deals with a huge number of things and their relevant data, many security challenges have to be addressed. For example, many attacks can occur such as message modification, traffic analysis, Denial of Service, eavesdropping, Sybil attack and so on [8]. In order to avoid these threats and to permit authorized use only, current research efforts have been focusing on the following areas: protocol and network security, data and privacy, identity management, trust and governance, fault tolerance, dynamic trust, security, and privacy management.A systemic and cognitive approach to IoT security has been proposed in [15].

Taking into consideration all these available technologies, their constraints and strengths, we propose a novel secure framework to curb industrial pollution using IoT, aiming to help prevent environmental degradation.

4. PROPOSED FRAMEWORK

In this section we propose a framework that effectively utilizes the concept of IoT to handle industrial pollution, by continuously monitoring the pollutant levels in an automated manner. We propose to utilize a mix of Wireless Sensor Network (WSN), for quick and dependable transmission of information, Electrochemical Toxic Gas Sensors (for various gases like Carbon monoxide, sulphur oxides, methane, oxides of nitrogen etc) to recognize the level of lethal gasses released by the factories, and the utilization of a Radio Frequency Identification (RFID) labeling framework to screen every factory from anyplace on the planet.

4.1 Technologies used

4.1.1 Radio-frequency identification (RFID)

RFID, which is a part of Automated Data Collection (ADC) technology makes use of electromagnetic waves in order to send and receive data with the intention of easy identification and tracking of the things to which the RFID tags are attached. In particular, radio-frequency waves are used between the reader and the objects. The two important components of RFID are RFID tags and RFID tag reader. RFID tags have both radio transmitters and receivers embedded in them and RFID reader or interrogator is a device which works in coordination with antenna to send data to the tags.

4.1.2 WSN

Wireless sensor networks (WSN) is a network of nodes or sensors distributed spatially used to check the environmental and physical conditions such as temperature, pressure, pollutants level and so on. The data collected by the sensors are transferred to the sink through network. The sink in turn might be connected to some other networks through a gateway. Sensors are usually small, portable and light-weighted. Sensors are provided with a transceiver, microcontroller and power source.

4.1.3 Electrochemical Gas Sensors and Underwater sensors

Electrochemical gas sensors are used to detect the gases and measure their concentration by the process of oxidation or reduction of target gas at an electrode and the current obtained from that is measured. Under water sensor networks find a great use in monitoring pollution by keeping track of the varying pH and temperature of water. This technology is used in our framework to keep track of water pollution by industries.

4.2 Architecture

Each unit or equipment dealing with the main functionality in the industry (i.e. the core unit of the industry) and

the chimney which serves as the outlet, is furnished with a passive RFID tag. The RFID readers detecting the RFID tag for the setup described above is depicted in Fig. 1

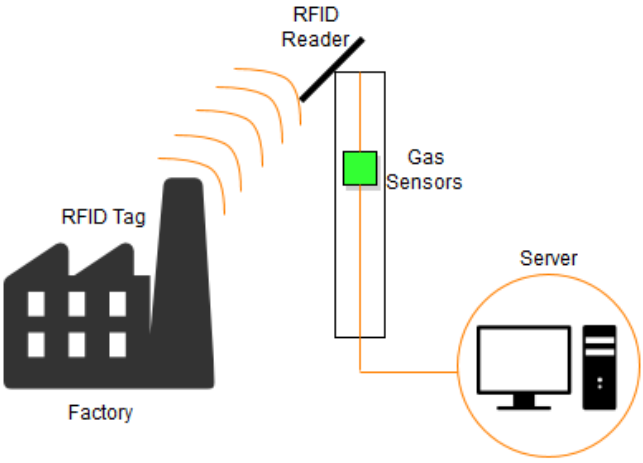

Figure 1: Working of RFID Readers

Sensor nodes, which are composed of gas sensors, are placed at key areas within the factory, especially near the major production units which are vulnerable to leakages. These sensor nodes serve to continuously gather data related to the level of harmful gases within the working area, which help in detecting unexpected leakage of gases. In addition to the sensors within the industrial workplace, we place another sensor node externally, in proximity to the chimneys, to monitor the level of pollutants released into the atmosphere by that particular industry. Also,we make use of underwater sensor networks to monitor the temperature and pH of the water body into which the effluents from the factory are being discharged.These sensor nodes help to monitor if there are any increasing variations from the normal conditions of water, which imply an aberration in the level of toxic effluents let into the water by factories. We propose to deploy sensor nodes at regular spans within the water body, depending on the nature and area covered by it.

4.3 Sensor Node Deployment Strategy

We categorize the Wireless sensor nodes into three main types:

- **Gas sensors:** These are the sensor nodes that are placed either inside the factory, near the processing units, to detect leakages or in the surrounding, to monitor pollution of air and water.
- **Collector Nodes:** These nodes form the second level of hierarchy. Their job is to collect information from the sensor nodes, aggregate the information and send it to the main server.
- **Aggregator Node:** We intend to place one aggregator node just before sending the sensor information to the main server, to aggregate the information coming from various collector nodes spread across the city. The aggregated data is then passed on to the Server for processing.
- **Server:** The main server processes the data forwarded by the aggregate node, testing if the levels exceed the permissible value.

The hierarchy of arrangement of these nodes are as depicted in Fig. 2.

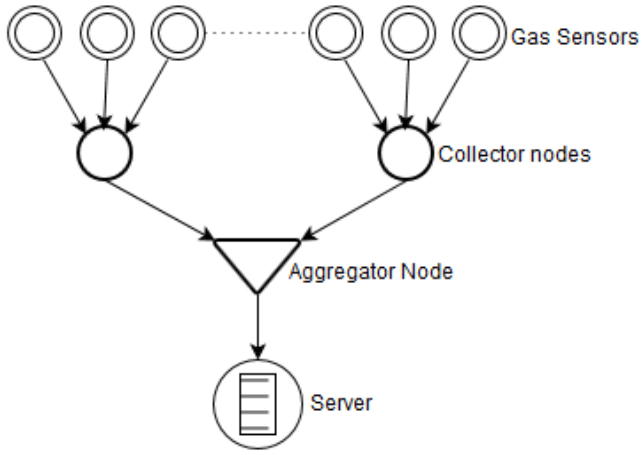

Figure 2: The heirarchy of Nodes

4.3.1 *Node Placement Strategy*

- These gas/underwater sensor nodes are placed at random positions, taking into consideration the position of main processing units, chimneys or effluent outlets.
- We partition the huge city under consideration, with a number of factories, into smaller areas, such that each area approximately has same number of factories and spans similar space in geography, namely, A1,A2,...An as shown in Fig. 3
- We place one collector node in each of these identified areas, to aggregate the data and pass on to the server.
- Finally we place the aggregator node and server in a fixed location, where computing and processing technologies are available to interpret the collected data and disseminate warning signals or alarms in case of emergencies.

4.4 Working

The sensor nodes may be recognized by special IP addresses. These hubs assemble sensor information consistently and send it remotely to the server. At whatever point the sensor hubs sense sudden climb in levels (than the ordinary level expected), quest is launched for concerned RFID labels, i.e. the chimney/unit bringing about contamination/spillage are recognized with the aid of the RFID tag appended on them. The mechanical unit which is identified with this RFID tag is accordingly distinguished and the concerned authority for that industry is alarmed about this issue in the event of exceeding contamination level. The permissible level of each of the toxic gas is fixed in accordance to the limits prescribed by the Pollution Control Board for that Country.

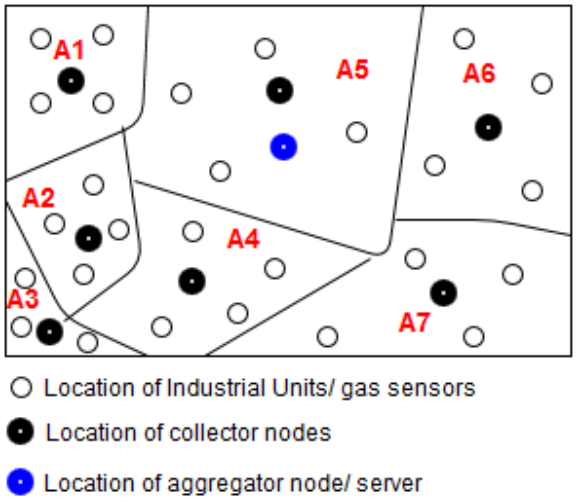

Figure 3: Node placement Strategy.

Over a period of time, if the emission levels pertaining to a particular industry is on rise, the authorities responsible for quality check are notified, and necessary actions can be initiated. On the other hand, if the sensors detect a sudden surge in the level of toxic gases within the premises of the industry, then this is interpreted as a leakage. In cases of leakage, alongside alarming the concerned authorities, the valves that are smartly connected shuts down automatically and a siren rings in the factory. To improve the construction modeling, we propose to smartly connect all houses in the close vicinity of any industry, so that when a siren rings at the processing plant, all houses are alarmed and individuals can take essential precautionary measure, such as abandoning the spot briefly.

The model of our framework is depicted in Fig. 4.

5. POSSIBLE THREATS TO THE SYSTEM

For a IoT framework like the one proposed, some of the main security aspects to be taken care of are authentication, authorization, identification and integrity of information exchanged.

It is difficult to achieve authentication in a IoT because of the nature of the RFID tags. RFIDs are known to have energy management issues which gets reflected in sensor networks. Due to this, the exchange of information between the external server and the RFID tags might fail, resulting in practical difficulties with authentication of users over the network. These factors make authentication one of the serious threats in our framework.

Ensuring integrity of data is another issue in our Framework. As a huge amount of confidential data is exchanged over the wireless network, it is important to ensure the integrity of messages and avoid attacks such as Man in the Middle Attack (MITM). An attack such as MITM can cause disruption in the working of our framework leading to improper analysis and interpretation of pollutant data.

Thus it is important to use secure and efficient protocols and other security measures to overcome these possible threats to our system. A in depth security analysis of the proposed framework and various security measures that could be employed to overcome these threats, have been explained in the following section.

6. SECURITY ANALYSIS

In the pace of automating the process of monitoring pollution level, we should not sideline the consideration and the assessment of the security issues, without which the IoT framework cannot endure. Several Worldwide organizations, like the European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF) and others have proposed several Standards for IoT [16], some of which have been enumerated in Table 1. However these Standardization approaches do not guarantee the security of exchanged information. IoT, due to its remote nature, is greatly defenseless against diverse attacks which has been on rise these days. Some of the security measures undertaken in our framework are discussed here.

Table 1: Standardization Efforts by Various Organizations

Standard	Objective	Data rate (kbps)	Comm. Range (m)
EPCglobal	Integration of RFID technology into the electronic product code (EPC),framework,which allows for sharing of information related to products	$\sim 10^2$	~ 1
GRIFS	European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the Internet of Things	$\sim 10^2$	~ 1
6LoWPAN	Integration of low-power IEEE 802.15.4 devices into IPv6 network	$\sim 10^2$	10-100
NFC	Definition of a set of protocols for low range and bidirectional communications	Up to 424	$\sim 10^2$
Wireless Hart	Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices	$\sim 10^2$	10-100
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	$\sim 10^2$	10-100

6.1 Role based access control model

One of the prominent concerns in security is access control. It is very much necessary to check whether the users are authorized to carry out a particular action or not. In order to meet this requirement, the authentication in our system would be based on role based access control model in which the access permissions are dependent on the roles

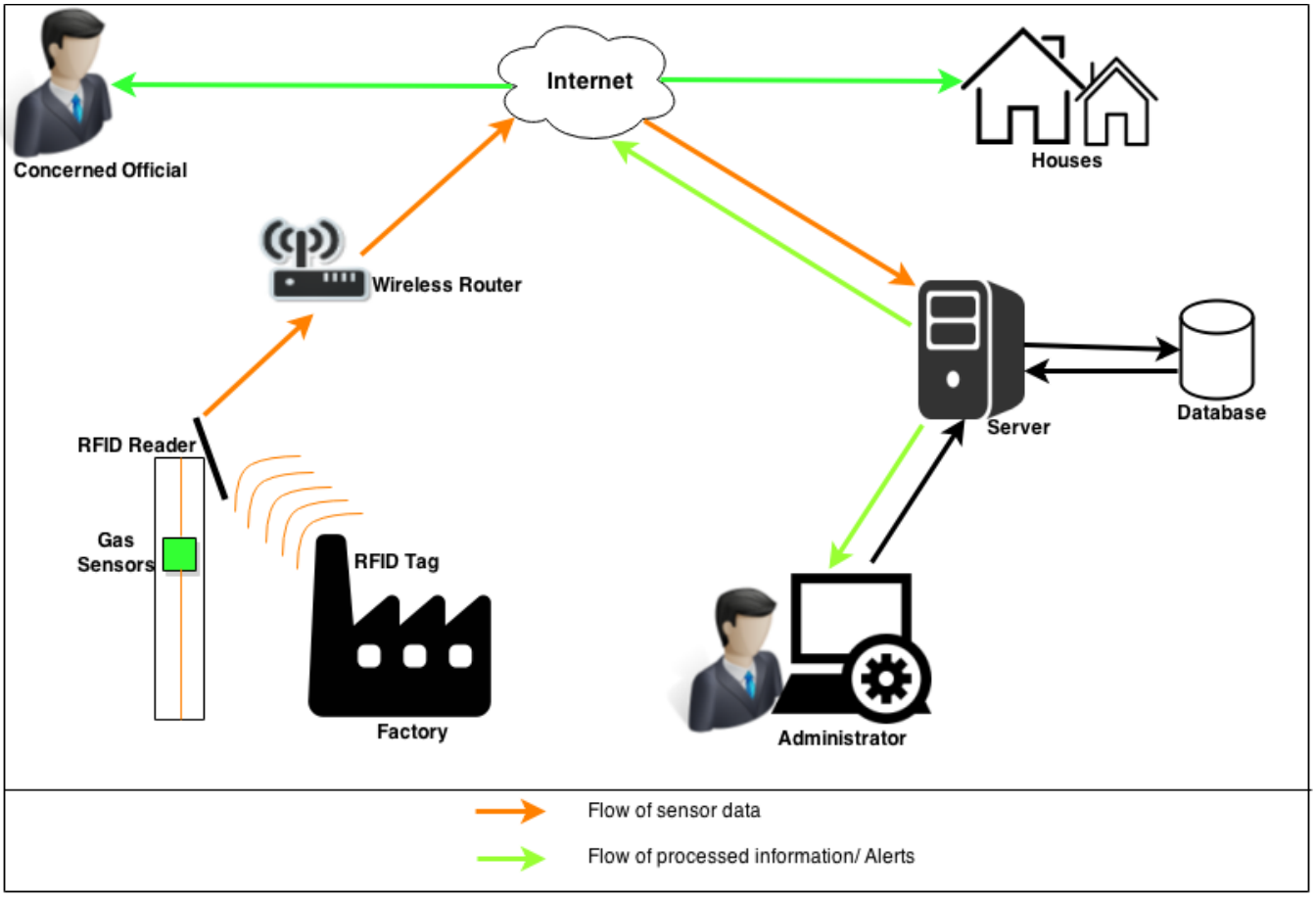

Figure 4: The proposed Framework

played by the actors in the system. The actors in our system are administrators, pollution control in-charge in the industries, concerned officials of the pollution control board and the residents in the nearby locality. Each actor in the system is assigned few roles which in turn are assigned permissions. For example, consider a role which is assigned the permission to explicitly notify the pollution control board about the aberrant rise in the waste discharges of industries. It is possible that this role would be assigned to many such permissions. And, the administrator would be assigned this role alongside few others.

6.2 IPv6 adoption

As we all know, the world is making a gradual transition from IPv4 to IPv6. And, we would consider adoption of IPv6 as ideal to our system. The objects in our system are always growing which demands for a larger address space. Also, IPv6 has data encryption in built which would server good purpose in our system.

6.3 RFID security

RFID makes use of radio signals for identifying and tracking the objects. These radio signals are susceptible to eavesdropping which would result in the disclosure of the identities of the industries and this is a loss of privacy which is undesirable. Also, attackers can clone the tags wherein the eavesdropped information would be used for unauthorized access permissions. So, it is very much evident that without proper security measures, the system cannot be maintained fairly. Some of the cryptographic techniques used in this regard are rolling codes, challenge-response authentication and so on. Also, the RFID signals should be protected by using appropriate encryption algorithms. However, RFID demands for lightweight protocols because of the energy management issues. Therefore, even after using the above mentioned cryptographic techniques, some of the problems would still remain.

6.4 Physical security

The devices in the system form the vital part in the proper functioning of the system as a whole. So, the security of these devices should be given utmost importance. Special care should be taken while building the nodes and the antennas of the system. The wiring inside the sensors should be as accurate as possible. And, these devices should be protected to prevent attackers from tampering or destroying them. At the same time, this protection should not affect the process of data collection and transmission. Most importantly, during the installation of the electrochemical toxic gas sensors, we have to make sure that the physical security is not compromised in any way. Suitable methods like CCTV installation can be made use of to monitor the sensor nodes in the industries.

6.5 Trade-off between cost and performance

One of the desired features in any IoT framework is that the sensor nodes should be able to capture data in a comprehensive manner. The electrochemical toxic gas sensors used to detect the leakage or the excess discharge of toxic effluents should be capable of collecting the data to the maximum extent. Otherwise, the very purpose of this system would fail. But the high performance sensors are associated with high costs. So, there exists a trade-off between cost of the sensors and their performance.

7. CONCLUSION

In the last decade, the deployment of IoT has faced many challenges due to many concerns. The limited computing capabilities of some of the devices in the IoT system degrade the overall performance. Also, some objects are constrained by their low battery capacity. In spite of taking the above mentioned security measures, the proposed system might be posed with new problems. And these problems would prevail in any IoT system, not particular to ours. So, some enhancements to the security of the proposed system can be done as the field of Internet of Things advances. Also, some functionalities can be added to it to customize the system based on many factors such as the rules and the regulations set by the pollution control board and so on. In aggregate, the proposed system would bring about a positive change in the environment we are living in and result in a healthier world.

8. REFERENCES

[1] De-Li Yang, Feng Liu, and Yi-Duo Liang. A survey of the internet of things. In *Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010),*. Atlantis Press, 2010.

[2] Elias Z Tragos, Vangelis Angelakis, Alexandros Fragkiadakis, David Gundlegard, Cosmin-Septimiu Nechifor, George Oikonomou, Henrich C Pohls, and Anastasius Gavras. Enabling reliable and secure iot-based smart city applications. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*, pages 111–116. IEEE, 2014.

[3] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 2013.

[4] Quan Z Sheng, Xue Li, and Sherali Zeadally. Enabling next-generation rfid applications: solutions and challenges. *Computer*, pages 21–28, 2008.

[5] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.

[6] Ian F Akyildiz and Mehmet Can Vuran. Wireless underwater sensor networks. *Wireless Sensor Networks*, pages 399–442, 2010.

[7] E Comini, G Faglia, G Sberveglieri, Zhengwei Pan, and Zhong L Wang. Stable and highly sensitive gas sensors based on semiconducting oxide nanobelts. *Applied Physics Letters*, 81(10):1869–1871, 2002.

[8] Xu Xiaohui. Study on security problems and key technologies of the internet of things. In *Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on*, pages 407–410. IEEE, 2013.

[9] Jiming HAO and Guowen LI. Air Pollution Caused By Industries. http://www.eolss.net/sample-chapters/c09/E4-11-02-01.pdf.

[10] Jiming HAO and Guowen LI. India: Green Growth - Overcoming Environment Challenges to Promote Development. http://www.worldbank.org/en/news/feature/2014/03/06/green-growth-overcoming-india-environment-challenges-promote-dev 2014.

[11] Daniel Rosenfeld. Suppression of rain and snow by urban and industrial air pollution. *Science*, 287(5459):1793–1796, 2000.

[12] Yajie Ma, Mark Richards, Moustafa Ghanem, Yike Guo, and John Hassard. Air pollution monitoring and mining based on sensor grid in london. *Sensors*, 8(6):3601–3623, 2008.

[13] Kavi K Khedo, Rajiv Perseedoss, Avinash Mungur, et al. A wireless sensor network air pollution monitoring system. *arXiv preprint arXiv:1005.1737*, 2010.

[14] Kai Zhao and Lina Ge. A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pages 663–667. IEEE, 2013.

[15] Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou, and Abdelmadjid Bouabdallah. A systemic approach for iot security. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*, pages 351–355. IEEE, 2013.

[16] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.