CHAPTER I

INTRODUCTION

1.1 RESEARCH BACKGROUND

Wireless Sensor Network (WSN) is a collection of few to thousands of WSN nodes that are randomly spread in the area to monitor environmental changes, like temperature and humidity (Wang, 2015). Figure 1.1 shows a WSN topology example of a wireless sensor network used for monitoring the marine environment, where a base station acts as a focal point for the WSN network. (XU, 2014).

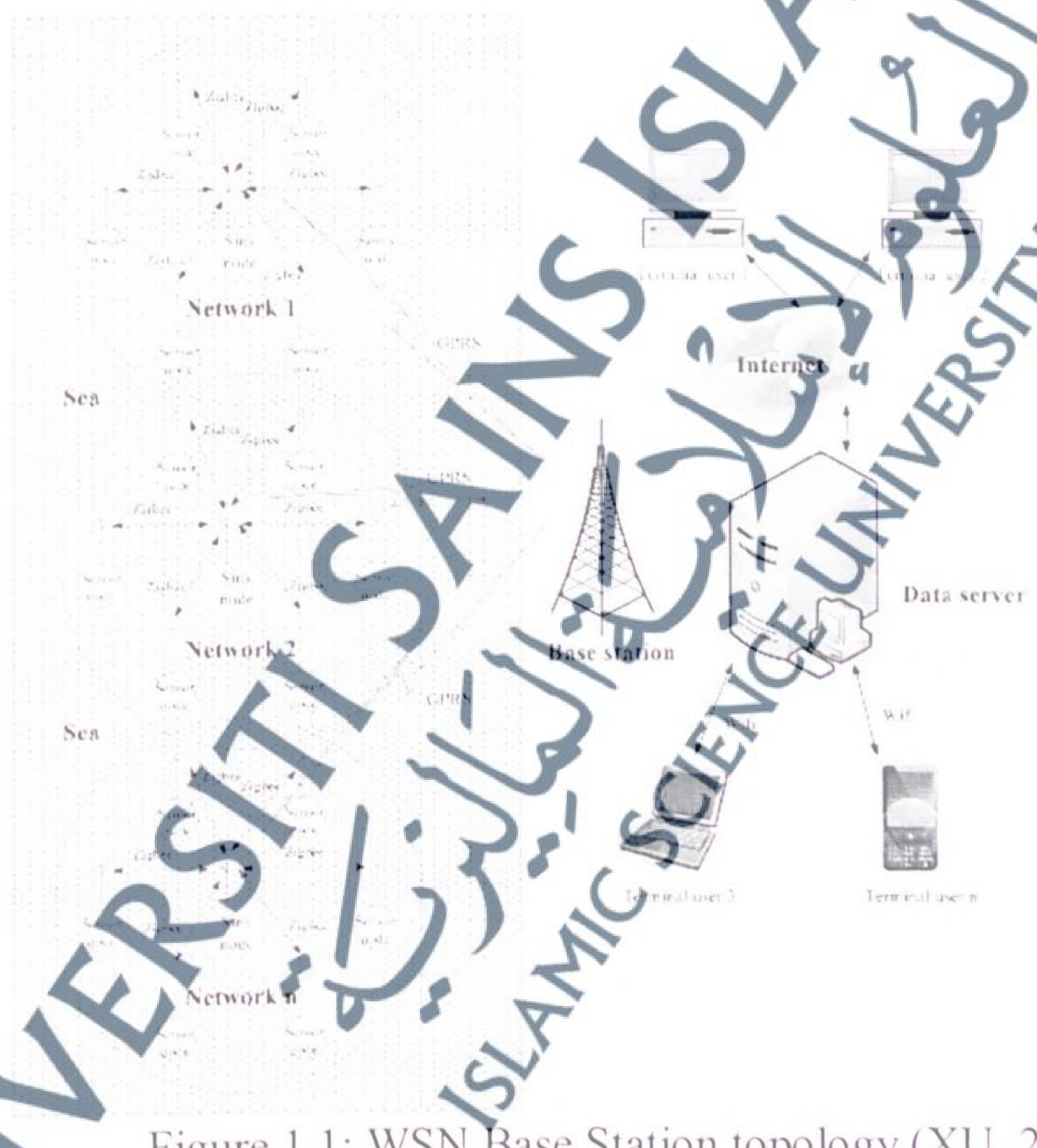

Figure 1.1: WSN Base Station topology (XU, 2014).

Recent projects and applications for Wireless Sensor Network (WSN) are expanding, especially with the appearance of low cost, credit card size, open source

computer systems (e.g. Raspberry Pi, Arduino and BeagleBone) that are equipped with multiple add-ons for communication, humidity, temperature, smoke and other sensors that opened WSN to new possibilities for building a low cost WSN (Fisher, 2015).

But such expansion is still facing distance as a main obstacle. WSN nodes are hard to manage in remote areas, and in other areas, they are implemented in places that are hard to reach, like woods and country borders, or even marine world (XU, 2014). AS GSM or CDMA signals fade when moving to remote areas. Such cases make it hard to make sure that keys and ciphered data are safely delivered and exchanged if pre-implemented, and are hard to be sent by the available wireless solutions because of their lack of reachability, especially on large scale WSN environment.

Figure 1.2: Raspberry Pi Zero, a 5$ computer.

On the other hand, key management faces several types of vulnerability between WSN nodes. In most cases WSN keys are pre-implemented (or pre-shared key). However, the main issue is, by reverse engineering, one node key will compromise the whole WSN network (Dimitrievski, 2011).

Another issue for pre-implement keys is that WSN nodes are small in factor, so they have a limited energy source, storage and processing power. In this case, storing keys need more storage, more energy and more processing power. However, one of the main priorities while designing WSN nodes is saving WSN resources for a better performance (Walters, 2006).

Sometimes for the sake of saving resources, keys are sent in raw to WSN nodes to save energy, storage and processing power, but in this case, the key will be vulnerable, since a sniffer can be used to get the keys while exchanging between WSN nodes. Another solution for WSN nodes is, therefore, needed to solve these issues.

Commercial FM stations are spread all around the country, and they have a wide coverage. Commercial FM broadcasts audio (e.g. Talk show), along with Radio Data System (RDS) which provides program name and time. And in Japan and some parts of Europe they are using Data Radio Channel (DARC) along with RDS for updating traffic status and bus station terminals. Figure 1.3 shows RDS information for FM station displayed on car radio.

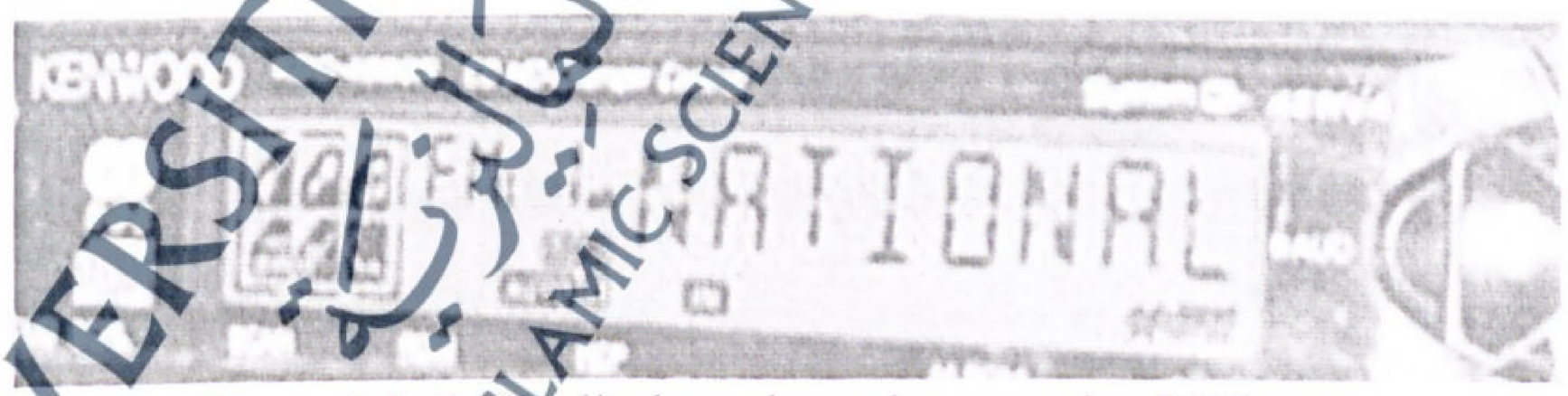

Figure 1.3: Radio displays channel name using RDS.

Commercial FM stations can be used to send the key to remote sites by injecting the key within the commercial FM station and broadcasting it to the WSN Base Station in remote areas. FM stations are covering all the country so there is no need to set up a new

project to reach WSN Nodes. And because the key is hidden in FM band, it's hard to be sniffed. To listeners, it's just another talk show or a song, but the fact is that the key is hidden in the broadcasted channel along with that talk show or song. Figure 1.4 shows Canadian Broadcasting Corporation (CBC) FM stations coverage along canadian east coast.

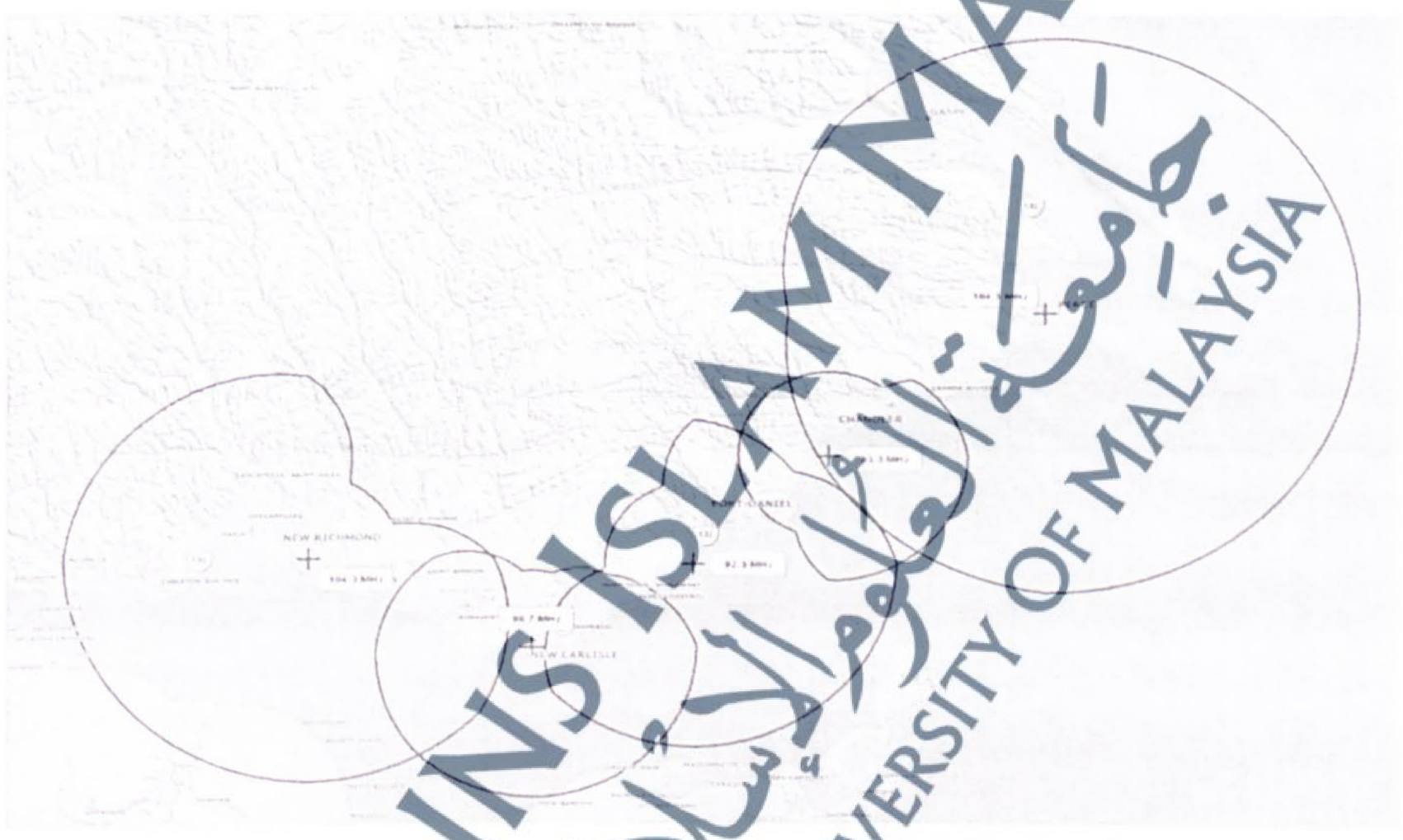

Figure 1.4: Alternate Frequency coverage, CBC/Radio-Canada.

(Cbc.radio-canada.ca, 2015)

This research will solve the symmetric key management, and long distance issues by using commercial FM radio stations. The solution will provide the three primary information security aspects along with secrecy:

Confidentiality: the term for keeping symmetric key and data safe and not available for unauthorized entity, users or process.

Integrity: to maintain and assure the accuracy of the symmetric key data, and that it cannot be altered by an unauthorized user.

- Availability: to make sure that the information must be available the time it's needed. Figure 1.5 shows the primary information security aspects triangle.

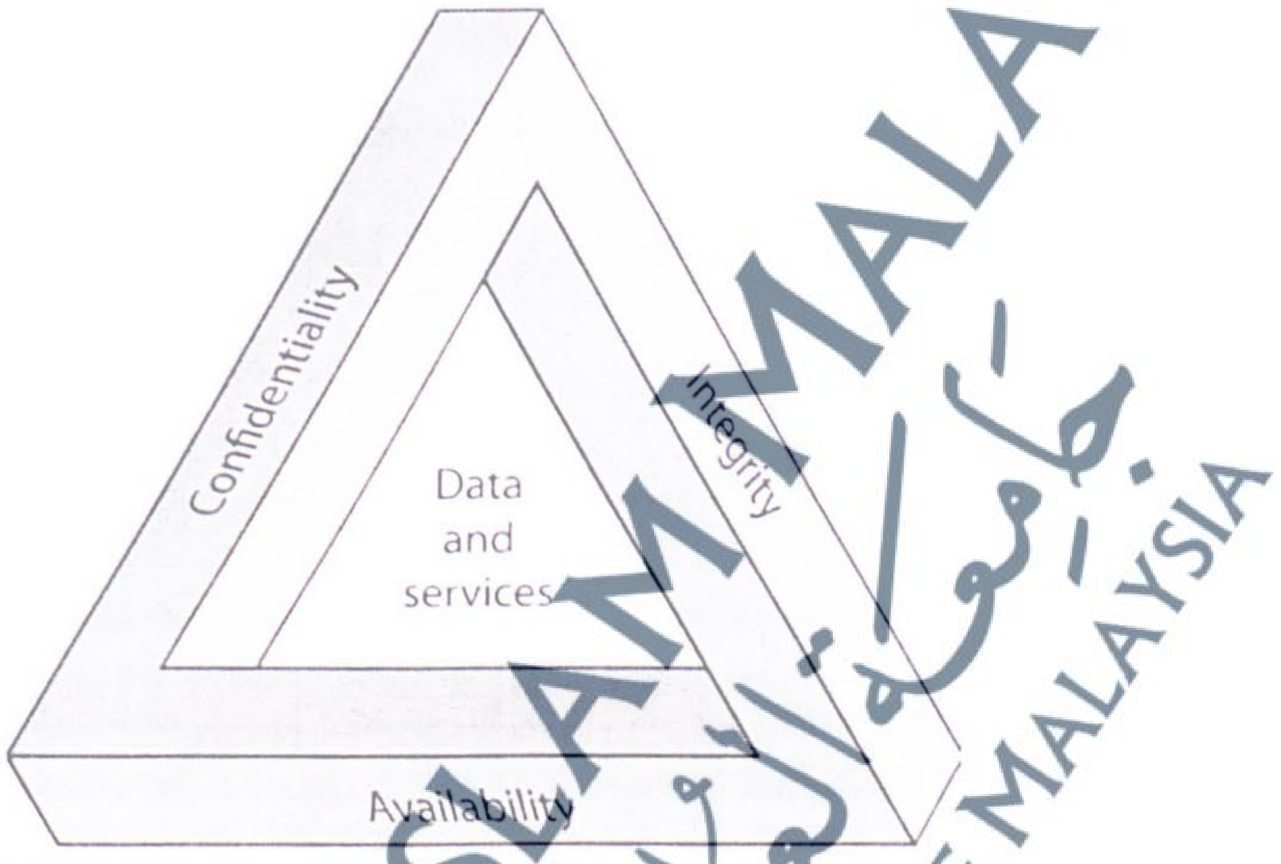

Figure 1.5: Primary information security aspects.

1.2 PROBLEM STATEMENT

To deliver data, without being compromised, using a long range wireless solution to send the secret key for WSN modes in remote areas and provide secure communication using asymmetric key distribution for the secret key. However, the symmetric key is highly sensitive, as it's used to protect WSN data. This explains why asymmetric cryptography is used to protect the secret key (symmetric key) while being exchanged between the sender and the receiver in contrast to the current wireless transmission methods that have a lot of limitations, e.g. Short distance.

FM broadcasting method can be used to solve secure communication and symmetric key distribution issues, by using ECC to encrypt and send the secret key using commercial FM stations. As FM, stations have a wide coverage within the

whole country, and because the symmetric key is hidden within the FM wave, it is hard to discover the key; also FM has a wide coverage around the country unlike other wireless techniques that have a limited coverage.

The main problem is how to build a system that can encrypt and then securely embed the secret key using asymmetric key in an FM transmission and send it to the WSN base station to recover the secret key and send it to the WSN nodes. Figure 1.6 shows an example of commercial FM station communicate with base stations in remote areas.

Figure 1.6: An example of a commercial FM, WSN Base Station in remote areas.

1.3 RESEARCH QUESTIONS

- How to study the parameters in key management related to FM system along with SDR system to provide the CIA concept along with reachability and availability for the TX and RX systems.
- How to design and implement a software defined radio (SDR) system that acts as an alternative method for delivering the secret key to WSN base station.

- How to understand and implement a secure key transfer using ECC along with Spreading, Fake code encapsulation and XOR encryption techniques to build the TX and RX systems.
- How to evaluate the performance of the TX and RX systems for the key management technique to make sure that key can be transferred and received from TX system to RX system.

1.4 RESEARCH OBJECTIVES

1. To study the parameters in key management related to EM system along with SDR system to provide the CIA concept along with reachability and availability for the TX and RX systems.
2. To design and implement a software defined radio (SDR) system that acts as an alternative method for delivering the secret key to WSN base station.
3. To understand and implement a secure key transfer using ECC along with Spreading, Fake code encapsulation and XOR encryption techniques to build the TX and RX systems.
4. To evaluate the performance of the TX and RX systems for the key management technique to make sure that key can be transferred and received from TX system to RX system.

1.5 RESEARCH SCOPE

The scope of work will be as follows:

1. This research will be built using GNURadio, a software used to build SDR systems.
2. HackRF One, an open source SDR platform that will be used to build an FM station.
3. RTL-SDR dongle that will be used to build a WSN base station.
4. The study is limited to encrypt and decrypt the WSN keys, imbed it to fake code and transmit it within the FM band.
5. The system must be secure and cost efficient.
6. Both systems will be constructed in a secure lab to not affect the commercial FM bandwidth. Results will then be collected and analyzed.

1.6 THESIS STRUCTURE

The thesis contains six chapters that are structured as follows:

- Chapter 1: the chapter includes a brief background about the study, research question, research scope and research objectives that will be done in this research.
- Chapter 2: the chapter will highlight current studies related to this study, explaining the need for such study from many angles, like current wireless coverage issues, why using ECC for WSN, benefits of using FM and discuss why other solutions are not good enough in emergency cases.
- Chapter 3: this chapter contains the research methodology implemented in this research, it contains the development model for the FM solution and the materials and tools used.
- Chapter 4: provides a full description of the system design and implementation, it describes the system structure design and system implementation for the TX and RX systems.
- Chapter 5: the chapter highlights the system testing and evaluation of the FM TX and RX systems.
- Chapter 6: includes the conclusion of the research, contribution and study limitations.