CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter will discuss current problems and solutions that are provided for WSN key management. The chapter will highlight these bulletins:

- Is Encryption enough for WSN key management?
- Current wireless methods reachability issues.
- FM as a solution for WSN coverage.
- Techniques used to embed data within the FM band.
- Using ECC as a strong, small key size encryption technique.
- Using software defined radio in current WSN implementations.

2.2 IS ENCRYPTION ENOUGH FOR WSN KEY MANAGEMENT?

Encryption alone is not enough for Key management in WSN so it is better to have another layer of security. Laskar (2012) explains how implementation and design of key management for WSN is hard because of the vulnerabilities of WSN nodes and its resource limitations.

While Zhang (2010) paper discusses the symmetric KMS algorithms needed for the security of WSN nodes, though, such implementation will make a heavy burden for calculating and saving the symmetric key, in time that WSN nodes should be as light as possible.

Another paper for KIM (2006), talks about key management issues for large wireless sensor networks, and how a shared secret key is exchanged to provide the CIA

concept, so that the location of remote nodes are hard to be determined. It also explains how hard it is to use public key cryptography due to the limitation of WSN nodes as the Pre-implemented secret key is used within them.

Using FM to embed and hide the symmetric key will solve both issues, the pre-implemented key needs more energy, and because keys are not pre-implemented they will be protected from reverse engineering that can extract keys from WSN nodes. While symmetric key generated by WSN nodes needs more memory and processing power.

2.3 CURRENT WIRELESS METHODS COVERAGE ISSUES

A research for (Kang, 2008) discussing the lack of available wireless solutions to reach WSN's in remote areas, reveals that without a stable wireless connection between remote areas the data may be lost or intermittent. The research mentions satellite communication as an example of long range wireless solution, and how rain, fog and snow can affect it and have a non-negligible impact upon the connection.

Another research Chasmai (2011) discusses the implementing WSN in the Indian Himalayas. It observes that modern theoretical solutions for WSN connectivity are hard to be applied in real case scenarios, especially in snowy weather. Hence, another solution is needed.

A research for Sayin (2013) tries to promote using the 144 MHz band (VHF) and the 434 MHz band (UHF) frequencies instead of current wireless methods for reaching the remote WSN's. However, the main issue is that this is a point to point solution (line of sight). In addition, the range was for about 1.3 miles only. While FM stations

broadcast is spread all around the country and commercial FM stations have a wider coverage.

2.4 FM AS A SOLUTION FOR WSN COVERAGE

In this section we will discuss why to choose FM stations to communicate with remote WSN rather than common ways (e.g. GSM, Wi-Fi) especially for remote WSN where it's too hard to make a new wireless setup, or in emergency cases where wireless services are down and as a solution for coverage issues.

A research for Barca (2013) proposes a system that can use a special RDS encoder within FM stations to send messages to groups in emergency cases as an alternative method of communication when regular communications are unavailable. But RDS has a low speed and it's not secure enough because RDS system is well known and can be reversed engineered.

A research for Campos (2014) shows that IEEE 802.11 based wireless multimedia sensor network has three major problems: bad performance, throughput unfairness, and energy inefficiency. In trying to solve these issues, they presented a technique called Wi-Fi Network Infrastructure extension (WiFiX) to resolve the energy efficiency problems.

The paper proposes a broadcast solution (point-to-multipoint) to control the Wi-Fi interfaces for the MWSN to save energy, because a working FM adapter needs much less energy than Wi-Fi one in its sleep mode.

Another research for Chen (2012) that relates to fingerprint-based indoor localization, highlights the issues related to Wi-Fi, which include fading due to operating frequency, multipath and the issue that it's susceptible to human presence.

The paper proposes using FM as an alternative solution for these issues, as it is "less susceptible to human presence, multipath and fading, it exhibits exceptional indoor penetration, and according to the experimental study FM has much less fading over time when compared to Wi-Fi signals. In addition, "accuracy increased to 83% more when compared to Wi-Fi solutions.

A paper for Ahmed (2005) discusses coverage of the hole problem in WSN area because of the numerous amount of WSN nodes, and that some applications need a better coverage to have a better accuracy relating to fault tolerance or redundancy Figure 2.1. The paper also shows that having no holes which figure (right) shows, is impossible because of the coverage has many limitations when it comes to accuracy.

Figure 2.1: Unit disk sensing model with coverage gap (left), sensor node will be added for more coverage (right).

The paper also notes how Mobile Sensor Networks technique is intended to have the maximum coverage, though it needs a long time for installation, and how complex

the protocol is, and the maximum distance that WSN nodes can be deployed in relation to the coverage.

Wireless solutions need design, time and man-power to have a new establishment, and they have a lack of reachability. On the other hand, commercial FM stations are already covering all the country, Figure 2.3. And each radio station has a wide coverage that can reach more than 40, Figure 2.4 shows a commercial FM stations that can be used to send an encrypted key to remote WSN's.

A document for Sprint (2005) explains the lack of GSM and CDMA services in times of emergencies (e.g. floods, storms, snow), the document shows that there are four points of failure. The main single point of failure is Power that feeds the cell site and cellular base stations.

The second risk exposure is Damage, as the average wind speed around cell towers is about 160 – 200 KM/h, while most of the damage is accrued because of flying objects at that speed, especially in ice storms that can cause severe damage to cell towers.

The third risk is Capacity, as cellular sites have a specific capacity to handle, and can be easily filled in emergency cases, because of heavy usage of mobile services seeking help, and once the capacity is filled, service will be blocked.

The fourth exposure is the Public Switched Telephone Network (PSTN) capacity, the capacity of PSTN depends on the call destination that the user wants to reach, that capacity will be bottle nicked in emergencies as one PSTN switch maybe used to control calls in the entire region. Figure 2.2 shows single points of failure in case of emergencies.

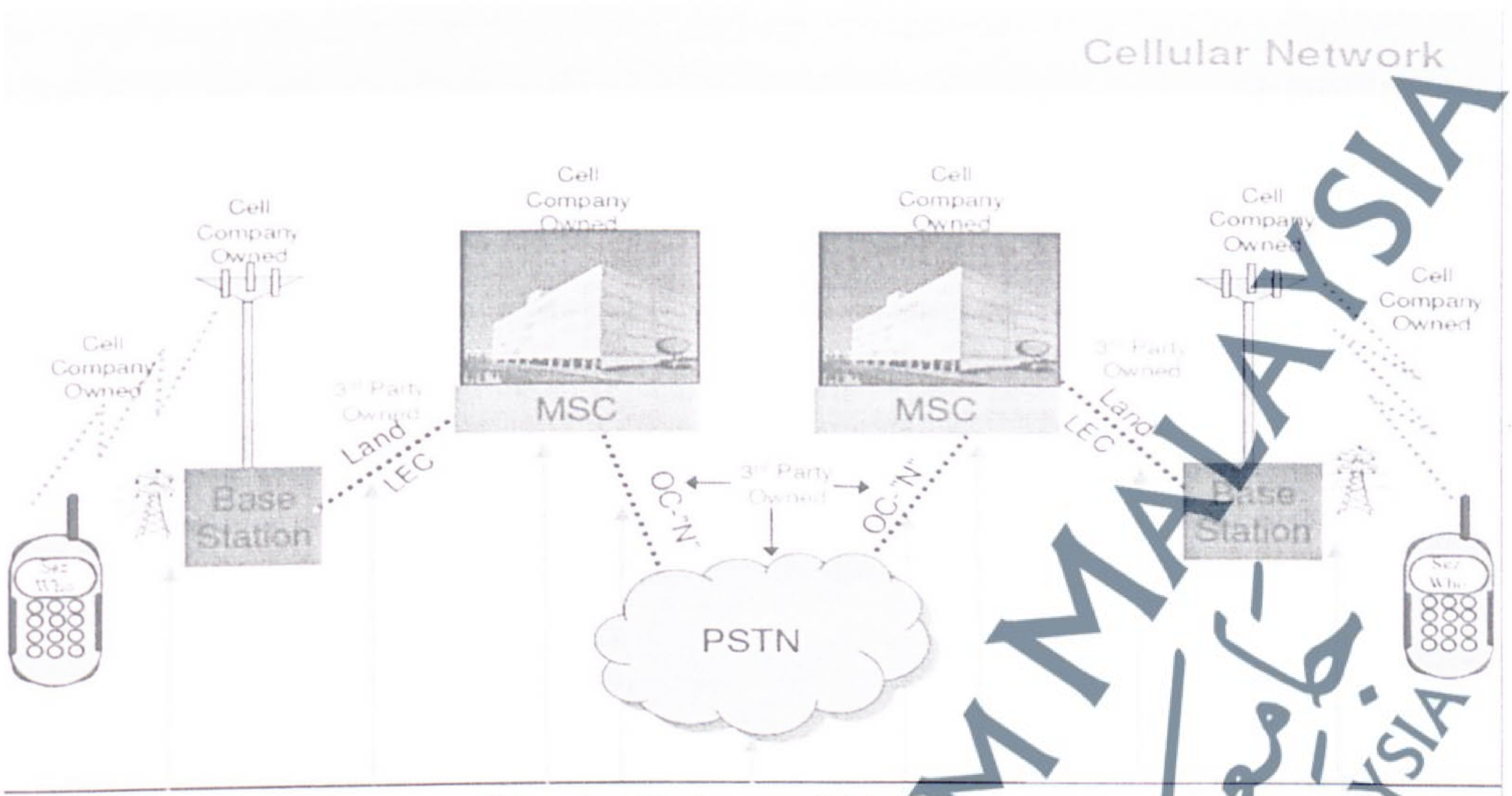

Figure 2.2: GSM/CDMA single points of failure in emergency case (Sprint, 2005).

FM stations have a wide coverage in urban and remote areas that cover indoor and outdoor and can provide a private service that has a low cost and low power consumption hardware that can gain service from commercial FM stations that are spreading all around the country (Youssef, 2005).

Figure 2.3 shows an example of FM station coverage for talk show stations around the USA. While Figure 2.4 shows an example of a single station that has a coverage of 40 miles (~64.37 KM). Commercial FM stations can be used to send the key securely with no capacity limitations, no coverage issues, and no setup time and is free of charge.

Figure 2.3: A coverage map example for radio stations around USA.

(Radio-locator.com, 2014).

Figure 2.4: an example for a commercial radio channel broadcast range.

(Radio-locator.com, 2014).

2.5 TECHNIQUES USED TO EMBED DATA WITHIN THE FM BAND

There are three main types of data communication protocol sent over commercial FM radio stations:

2.5.1 RADIO DATA SYSTEM (RDS)

RDS is a communication protocol standard used for embedding small amounts of digital information in FM radio broadcasts. The embedded information can be a station's name, time and even traffic information. RDBS is the American name for the RDS. RDS or RDBS in North America, has a data transfer rate of 1,187.5 bits per second on a 57-kHz subcarrier as shown in Figure 2.5 (RDS Basics, 2015).

2.5.2 MICROSOFT DIRECTBAND

Discontinued in 2006, DirectBand was a Microsoft technology product used in North America that was a high-rate (12 Kbit/s) standard. DirectBand used commercial FM radio stations to deliver traffic and weather information, sports scores and more in over 100 cities to constantly transmit data to a variety of devices, including portable GPS devices, wrist watches and home weather stations. The MSN SPOT watch in Figure receives digital data from FM station and filters it depending on user customization as shown in Figure 2.6 (Youssef, 2005).

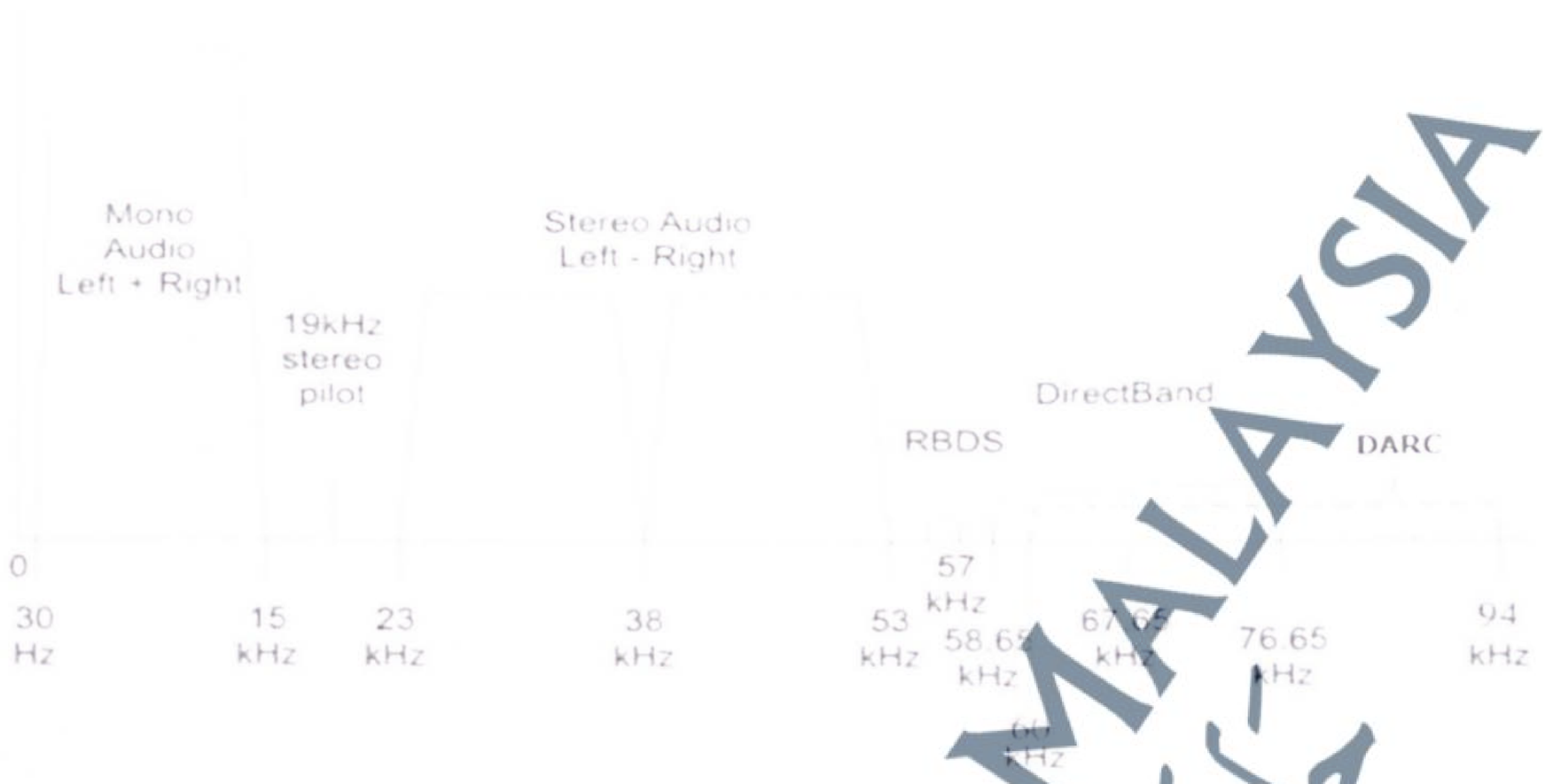

Figure 2.5: The RDS and DirectBand and DARC spectrum of an FM pilot tone system.

Figure 2.6: MSN SPOT watch data gain.

2.5.3 Data Radio Channel (DARC)

DARC is a high-rate, (16 Kbit/s) standard is used to encode data in a subcarrier over radio station broadcasts. Because of its high speed DARC is used for disseminating traffic information. In the USA, it was utilized to deliver stock market quotes. In Japan and France, DARC has been used for traffic information (Torrieri, D. 2011).

Figure 2.7 shows bus terminal displays that reveal the Estimated Time of Arrival

(ETA) for the next bus. The bus terminal display in Helsinki, Finland uses DARC to update its data.

Figure 2.7: Bus terminal display in Helsinki, Finland.

Table 2.1: spectrum of an FM pilot tone system.

KHz	H	Expected	Observed	Data Rate
0-15	-	Mono signal (L+R)	Mono signal (L+R)	-
19	1st	Stereo pilot tone	Nothing on 1st harmonic	-
23-37	-	Stereo sideband (L-R)	Missing stereo sideband (L-R)	-
38	2nd	Stereo center	Nothing on 2nd harmonic	-
39-53	-	Stereo sideband (L-R)	Missing stereo sideband (L-R)	-
57	3rd	RDS Center	RDS Center	1.1875 Kbit/s
67.65	4th	DirectBand Center	Digital Signal	12 Kbit/s
76	4th	DARC Center	Digital Signal	16 Kbit/s

RDS had a small data rate comparing to DirectBand and DARC, but both DirectBand and DARC are property standards. And then we ask to deliver a new solution so we can embed on the 4th harmonic of the FM band to deliver the WSN key securely.

Table 2.2 shows a comparison between various types of communications techniques and the advantage and disadvantages for each of them.

Table 2.2: comparison between current communication solutions.

No.	Communication type	Max Speed	Max. Coverage	Capacity	Advantage	Disadvantage
1	Wi-Fi	1.3 Gbps	limited	limited	Good for day to day use for small area coverage especially indoor.	Limited capacity and coverage, high cost for long distance range and needs time to setup.
2	Wi-Max	1 Gbps	65 KM	1000	High speed connection.	Point to Point connection that is resilience to weather and tower capacity.
3	GSM	2 Mbps	70 KM	100	Very good coverage in urban areas.	Faded in remote areas.
4	3G	7.2 Mbps	70 KM	100	High speed, good coverage in urban areas.	Faded in remote areas.
5	4G/LTE	1 Gbps	70 KM	100	Very high speed, good coverage in urban areas.	Faded in remote areas.
6	ZigBee	250 Kbps	50 m	limited	Low power consumption, good for near communication.	Low speed, low coverage.
7	FM	11 Mbps	107 KM	Broadcast	Wide coverage with broadcast, no setup time, no extra cost, good for small applications.(Lan, 2010)	Limited speed.
8	SATELLITE	1 Gbps	6000 KM	4000	Wide coverage, High speed	Too costly, needs heap setup time, resilience to weather conditions specially snow.

2.6 USING ECC AS A STRONG, SMALL KEY SIZE ENCRYPTION TECHNIQUE

For symmetric key encryption, US National Institute for Standards and Technology (NIST) recommends to migrate from public key algorithms to Elliptic Curve Cryptographic (ECC). Because most of the key systems nowadays are using 1024-bit parameters, such as AES and Diffie-Hellman NIST considered this to be sufficient for use until 2010 only, after that, systems must use parameters more than 1024-bit, that means more processing power. The next table compares keys sizes needed between DES and AES with RSA and Diffie-Hellman and elliptic curve that are expected to give identical security as shown in Table 2.3.

Table 2.3: NIST Recommended Key Sizes (NIST.gov, 2009).

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

ECC's additionally are computationally more productive than the original open key frameworks, RSA and Diffie-Hellman. The accompanying table demonstrates the degree of DH processing versus ECC calculation for each of the key sizes recorded in Table 2.4.

Table 2.4: Relative Computation Costs of Diffie-Hellman and Elliptic Curves (NIST.gov, 2009).

Security Level (bits)	Ratio of DH Cost : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

That means using ECC for WSN will save a great deal of processing power, energy, and memory to encrypt and decrypt the key.

ECC has multiple usage in real IT world for key exchange in several internet services like Bitcoin internet currency. Elliptic Curve Digital Signature Algorithm (ECDSA) is used for user private key to transfer the ownership of a bitcoin from one owner to another. ECC is also used in Secure Shell (SSH-2), an encrypted network protocol used to allow secure key exchange between remote users and servers (Bos, 2014).

A Global Security concept that was introduced by Lenstra (2013) comparing the energy needed to break a cryptography algorithm and check the amount of water that energey will boil. The study shows that breaking a 228-bit RSA can boil a teaspoon of water, while energy needed to break a 228-bit ECC key can boil all the water on earth.

We will use Elliptic Curve Crypto Utility for Reliable Encryption (SECCURE) version 0.5 (SECCURE Elliptic Curve Crypto Utility for Reliable Encryption, 2015), a

toolset that offers public key encryption/decryption that is compatible with python. Though our method is using ECC as a secure encryption, and though its proven that it is impossible to hack the key, ECC is still vulnerable to be timed by an attacker (Time Attack).

ECC is not the only crypto system that is vulnerable to time attack, as time attack can affect any type of crypto system, from webserver, to KMS server, even ATM smart cards (Brumley, 2005). Time attack can be done by having precise calculations for the cpu input, so the attacker can reverse engineering back to the input time – a threat that justifies the need for a remote KMS service with a key hiden within FM to prevent the time attack and to diliver the key safely to the WSN base station.

2.7 USING SOFTWARE DEFINED RADIO IN CURRENT WSN IMPLEMENTATIONS

Traditional radio devices are constructed from physical components that are hard to be modified without a physical intervention, that's where SDR comes. IEEE defines SDR as "Radio in which some or all of the physical layer functions are software defined". In other words, replacing some of the radio physical components and/or functions are done using a software instead of hardware, so the hardware will just obtain the raw signal and then SDR system will handle the signal process phase. That gives radio design higher flexibility with lower cost. Figure 2.8 shows SDR block design.

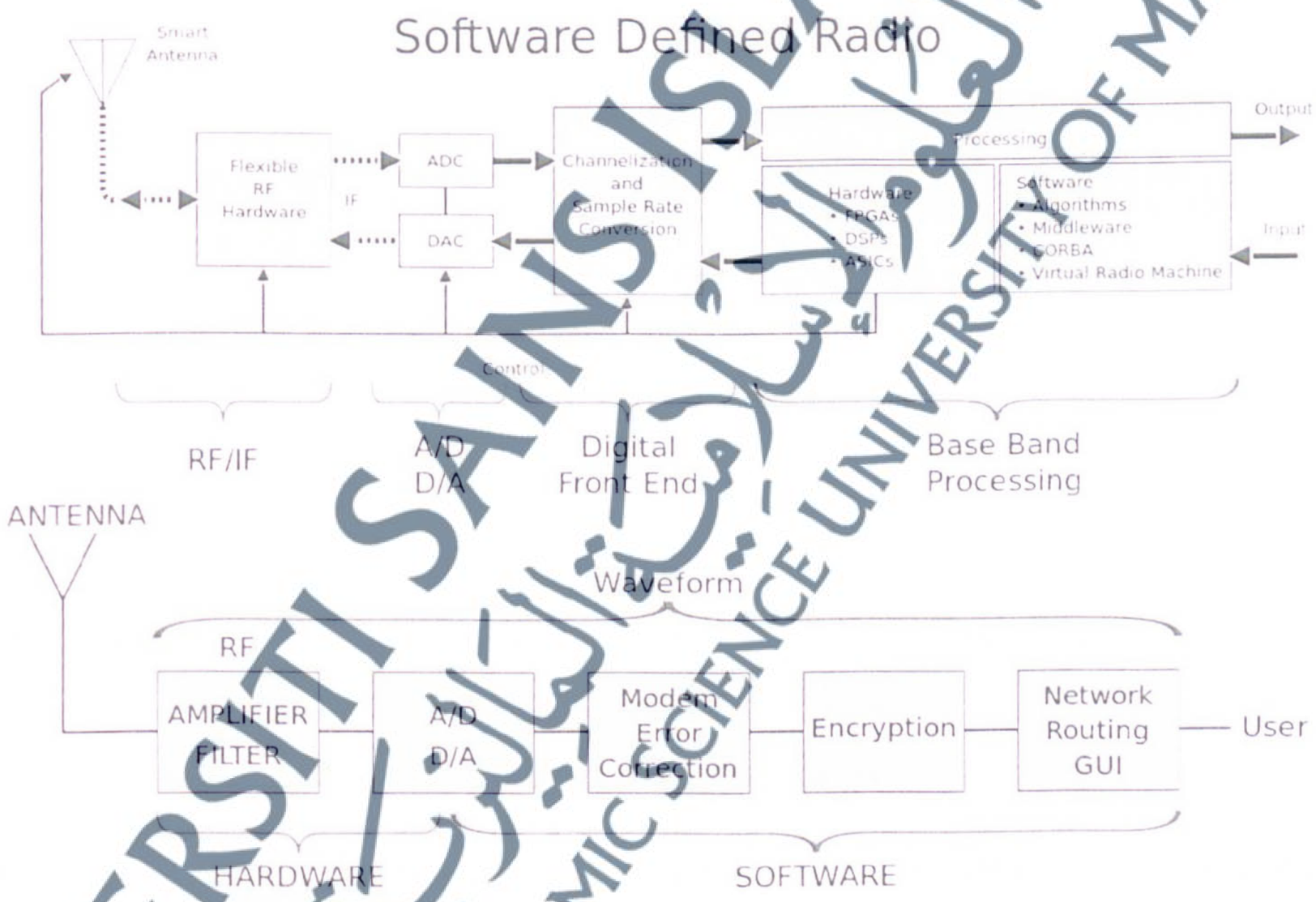

Figure 2.8: Software Defined Radio Structure.

SDR has been used in many implementations in WSN projects lately, some uses SDR as an early design tool for WSN. A paper for Kong (2010) shows that SDR can

be used as an initial design phase for WSN inside the car to elimintate wired sensors that have complex data and power cables route inside the car body.

Another paper for Vannucci (2008) presents a new way for building WSN nodes to save energy that is used for transmitting. The study proposes a Backscatter radio; the transmitter WSN node is simplified to a transistor and an antenna, while SDR is used as a transceiver to transmit the carrier.

Another study used SDR to create a wireless communication monitor using SDR to enhance the link quality and to verify link quality estimation in WSN's. It used GNU Radio and USRP to calculate the Error Vector Magnitude (EVM) and Packet Reception Rate (PRR) for trasmitting systems (Qin,2011).

A paper for Li (2009) used USRP with GNURadio to overcome the shortage of low throughput and coverage. The researchers have used narrow-band to communicate with a range of WSN platforms using SDR, because using SDR has no specific standard or hardware design constraints, as the biggest part of hardware implementation is done on the software side (GNURadio) while USRP is used for communication.

2.8 CONCLUSION

In this chapter we have discussed several points relevant to the thesis and highlighted the corresponding research papers to demonstrate the current challenges facing WSN design and implementation, especially in real case scenarios.

The investigation shows that the proposed system can overcome these issues by avoiding or taking advantage of each study, to build a multi-layer secure WSN using

commercial FM stations especially in emergency times. Table 2.5 summarizes the literature review papers.

Table 2.5: literature ECC, FM and SDR papers summarization.

Research	Year	Technique	Coverage	Advantages	Disadvantages
Lenstra	2013	ECC	N/A	Comparing the energy needed to break a cryptography algorithm, and check how much water that energy will boil. The study shows that breaking a 228-bit RSA can boil a teaspoon of water, while energy needed to break a 228-bit ECC key can boil all the water on earth.	ECC is security is proven, though it is still like other encryption techniques vulnerable to be timed by and attacker (Time Attack). So KM server must be kept safe from time attackers.
Barca	2013	RDS/FM	100 KM	Wide coverage especially to remote areas.	RDS main issues is low speed, and RDS techniques is well known so that messages can be reverse engineered.

Research	Year	Technique	Coverage	Advantages	Disadvantages
Sayin	2013	VHF/UHF	2 KM	An alternative solution for common long range wireless communication techniques using VHF/UHF.	The main issue that's this is a point to point solution (line of sight). In addition, the range was for about 1.3 miles only. So it needs a special setup.
Sprint	2005	GSM/CDMA	70 KM	Wide urban coverage, easy setup, secure communication.	A Technical document explains the lack of GSM and CDMA services in times of emergencies (e.g. floods, storms, snow), the document shows that there are four point of failures. The main single point of failure is Power that feeds the cell site and cellular base stations. The second risk is the flying objects that can hit the cell towers. The third risk is Capacity, as cellular sites has a specific capacity. The fourth exposure is PSTN capacity that can be easily filled at emergency cases.

Research	Year	Technique	Coverage	Advantages	Disadvantages
NIST	2009	ECC	N/A	ECC is an a small secure key that symmetric key size of 256 bits needs an RSA and DH key size of 15360 bit while in ECC key size is 521.	Still new and needs time to be implemented as alternative solution for RSA and DH.
Bos	2014	ECC	N/A	ECC has multiple usage in real IT world for key exchange in several internet services like Bitcoin internet currency, Elliptic Curve Digital Signature Algorithm (ECDSA) is used for user private key, this is used to transfer the ownership of a bitcoin from one owner to another.	Still new and needs time to be implemented as alternative solution for RSA and DH especially for small applications.

Research	Year	Technique	Coverage	Advantages	Disadvantages
Li	2009	SDR	In Lab	Used USRP with GNURadio to overcome the shortage of low throughput and coverage. The researchers have used narrow-band to communicate with a range of WSN platforms using SDR, because using SDR has no specific standard or hardware design constrains, as the biggest part of the hardware implementation are done on the software side (GNURadio) while USRP used for communication	No specific standard, though because of regulations SDR must be only used in a secure lab to not overlap with other frequencies.

Table 2.5 shows a summarization for FM, ECC and SDR papers that were included in literature review, the table compares technique used and the coverage for each technique (if applicable) and the advantages and disadvantages for each technique.

From the table we can conclude that ECC is an excellent encryption technique that can be used to encrypt the WSN symmetric key. While FM is a long range, low cost and easy to setup wireless solution that can be used to deliver the encrypted symmetric key to the remote WSN nodes using SDR.