AN IMPLEMENTATION OF FHMA FOR HONEY ENCRYPTED DATASETS IN WIRELESS SENSOR NETWORKS

M. Rajalakshmi[1] and C. Parthasarathy[2]
[1]Department of Computer Science and Engineering, SCSVMV, Tamil Nadu, India
[2]Department of Information Technology, SCSVMV, Tamil Nadu, India
E-Mail: rajidmi@gmail.com

ABSTRACT

This paper proposes source encryption and channel encryption of input data sets to improve the data security in Wireless Sensor Networks (WSN). It is the implementation of honey encryption for the information bits as a source encryption and includes Gaussian Frequency Shift Keying (GFSK) for the honey encrypted data to perform Frequency Hopping Spread Spectrum (FHSS) as a channel encryption and the output of FHSS is propagated with the help of Frequency Hopping Multiple Access (FHMA) in WSN. So, it is impossible to intrude through channel by the hackers and also there are no possibilities to detect or decode the information by Brute force attack because of honey encryption. It provides dual security to protect the information.

Keywords: honey encryption (HE), Gaussian frequency shift keying (GFSK), wireless sensor networks (WSN), frequency hopping multiple access (FHMA), frequency hopping spread spectrum (FHSS).

1. INTRODUCTION

The encryption is a process of hiding the plain text with the help of a specific key to obtain the cipher text. However, security maintained in the encrypted text has been easily cracked by the hackers to decode the plain text by using brute force attack. The honey encryption is implemented to overcome the brute force attack. The sequential process of GFSK, FHSS and FHMA are processed in WSN to avoid the channel intruders. The wireless sensor networks follows IEEE 802.11b/g standard to communicate within 100m range with 0 - 20 dbm antenna power in both indoor and outdoor communication and also follows IEEE 802.11n for larger range of communications. It has a bandwidth of 11 Mbps and operating over 2.4 GHZ, 3.6 GHZ and 5 GHZ range of frequencies and also has 600 Mbps throughput and 150ms latency. It has in build security like Wireless Equivalent Privacy (WEP) and Wireless Protected Access (WPA) to authenticate the users.

In pass band communication, the data constellation must be included to implement digital modulation scheme. After mapping the constellation, the GFSK scheme is implemented. The channel encryption process begins with the implementation of FHSS scheme. The Pseudo Noise (PN) Sequence is needed to spread the output of GFSK to perform the FHSS. The FHSS performs 1600 frequency hops per second and also assign specific pattern for the connected nodes. The data sets from FHSS are propagated by FHMA technique. The transmitted datasets are received using frequency diversity. The FHSS data is despreaded with the same PN sequence and perform constellation demapping by using Armstrong method to get the original transmitted data. After that, the decryption process is done for corresponding honey encryption. The information received with synchronization.

2. EFFICIENT ENCRYPTION METHOD

2.1 Honey encryption

The honey encryption is mainly used to overcome the brute force attack. The process of encryption initiates with describing the number of Hash Functions (HF) N going to be implemented for encryption [1]. Generally the value of N is 10K and compiled the hash functions with N times with the OR operation of password with salt to produce the key. The salt can be evaluated by number of bits used as a message. Then the exclusive OR operation performed with message and key to produce cipher text [2]. The encryption and decryption steps are following:

Encryption

```
1. Salt ← S {0,1}^128
2. Key ← HF^N(Pass code || Salt)
3. Cipher Text ← Key (Ex-Or) Message
4. Return {Salt, Key}
```

Decryption

```
1. Key ← HF^N(Pass code || Salt)
2. Message ← Key (Ex-Or) Cipher Text
3. Return {Message}
```

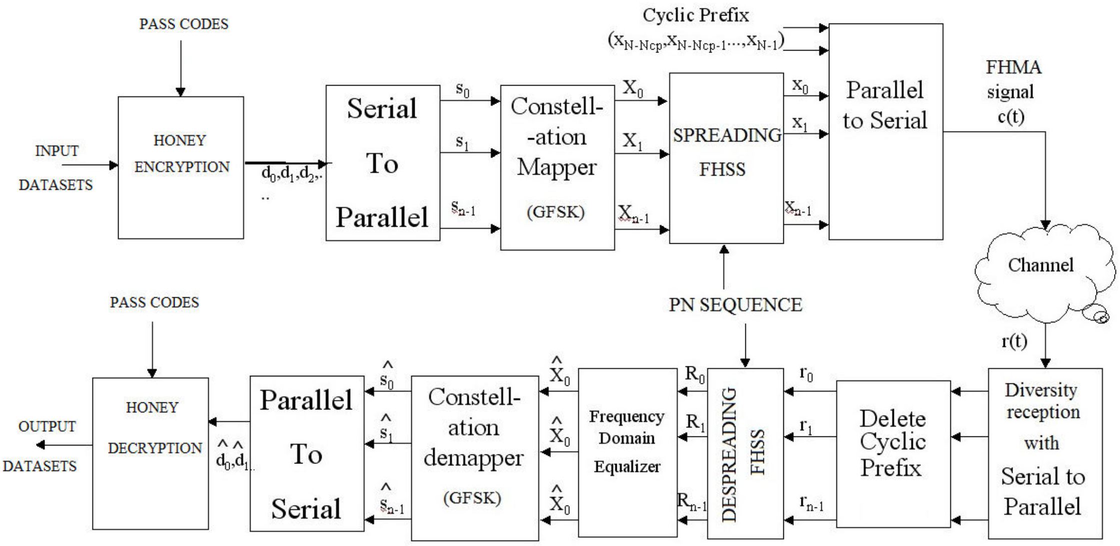

Figure-1. Block diagram of the efficient encryption method.

2.2 GFSK

As opposed to straightforwardly tweaking the frequency with the computerized information symbols, "promptly" changing the frequency toward the start of every symbol period, Gaussian frequency-shift keying (GFSK) channels the information pulses with a Gaussian channel to make the advances smoother. [3] This channel has the benefit of decreasing sideband control, diminishing interference with neighboring channels, at the cost of expanding intersymbol interference. The transmitter and receiver of GFSK is clearly shown in Figure-2 and Figure-3.

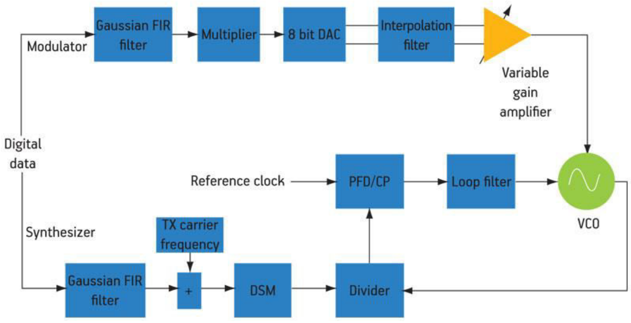

Figure-2. GFSK Transmitter.

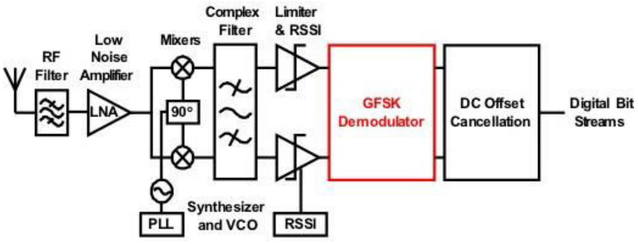

Figure-3. GFSK receiver.

A GFSK modulator contrasts from a straightforward frequency-shift keying modulator in that before the baseband waveform (levels -1 and +1) goes into the FSK modulator, it is gone through a Gaussian channel to make the changes smoother so to constrain its phantom width. Gaussian sifting is a standard path for diminishing phantom width; it is called "pulse shaping" in this application. [4] Here, it uses three bits as symbols. So, the circular constellation is used which is shown in Figure-4.

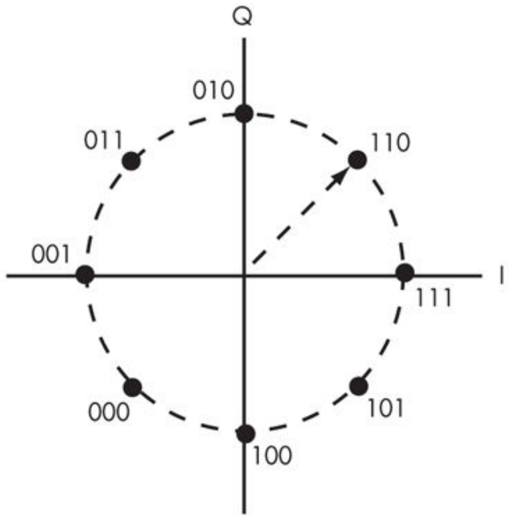

Figure-4. GFSK signal constellations.

2.3 FHSS

Frequency hopping spread spectrum is a strategy for transmitting information remotely, utilizing a wide range of frequencies. After a given time, the transmitter and beneficiary change the frequency on which they transmit the flag. [5] They do this in an apparently arbitrary manner; however both have concurred on the request in which they utilize the frequencies. The process of including Pseudo Random Sequence (PRS) is called spreading and the process of removing the PRS is called Despreading which is shown in Figure-5.

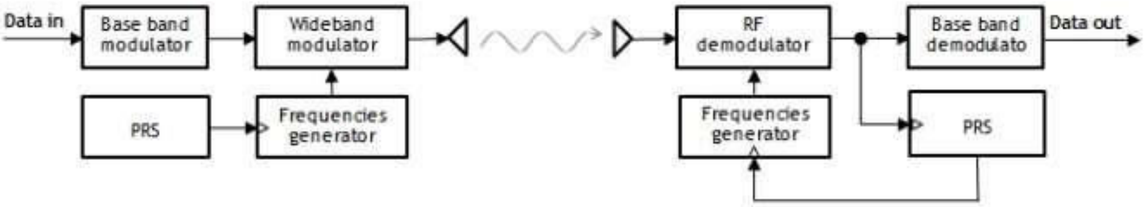

Figure-5. Frequency hopping spread spectrum transmitter and receiver.

2.4 FHMA

It uses different carrier frequencies for different datasets and periodically changing the carrier frequency to transmit over the pass band channel. It is clearly shown in Fig.6.

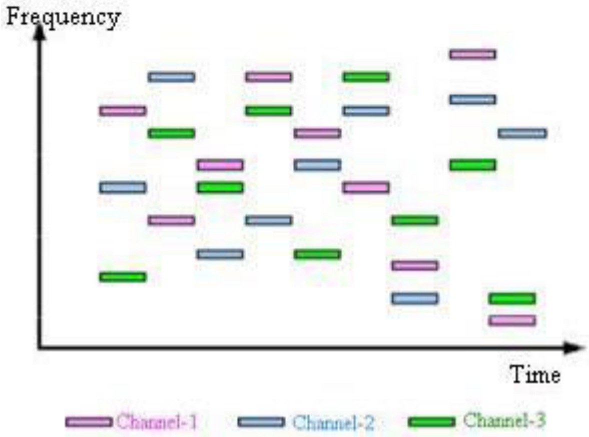

Figure-6. Frequency hopping constellations.

2.5 Frequency diversity

It receives the signals which are modulated with different frequencies and separated the datasets to the corresponding users. It is the counter process for FHMA. The illustration of frequency diversity is shown in Figure-7.

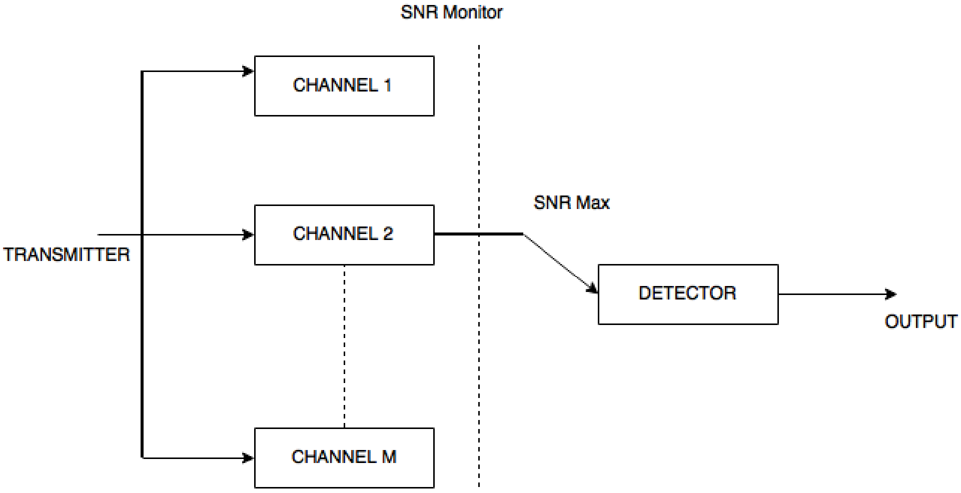

Figure-7. Frequency diversity reception.

3. PERFORMANCE ANALYSIS

The process of honey encryption consumes some time period to encrypt datasets. However, the security is very high. It is compared with other encryption standards and illustrated in the Table-1. The Code Breaking Probability (CBP) of the Efficient Encryption method is very less (approximately equal to 0) when compared to the other standards. The CBP is normalized to unity. The CBP is the ratio between successful attacks into number of attack attempts.

CBP = Successful Attacks / Number of Attack Attempts

Table-1. Comparative analysis of various encryption standards.

ESTEEMS	DES	AES	RSA	3 FISH	RC 5	Efficient encryption method
Key Length (Bytes)	8	16,32	Variable	32,64,128	256	128,256
Block Size (Bytes)	8	2	Variable	32,64,128	4,8,16	16
CBP	1/2	1/3	1/0.5	1/10	1/100	1/∞
Attacks	Linear Crypt Analysis	Sidwe Channel Attack	Brute Force Attack	Boomerang Attack	Timing Attack	No Successful Attacks
Security	Less	Less	Good	Secure	Highly Secure	Highly Secure
Speed	Slow	Fast	Average	Fast	Slow	Average

The frequency hopping spread spectrum multiple access provides high security, because the frequency changes with respect to time period. It is impossible to intrude channel and attacks by the hackers.

4. CONCLUSIONS

Thus the protection of data can be provided by honey encryption and the channel safety is confirmed by the Frequency hopping spread spectrum in the wireless sensor networks. The source encryption and channel encryption of input data sets to improve the data security in Wireless Sensor Networks is achieved by the Efficient Encryption method.

REFERENCES

[1] Mimoso and Michael. 2014. Honey Encryption Tricks Hackers with Decryption Deceiption. in Threat Post.

[2] Simonite and Tom. 2014. Honey Encryption Will Bamboozle Attackers with Fake Secrets. in MIT Technology Review.

[3] D. Sweeney. 2002. An introduction to bluetooth a standard for short range wireless networking. in Proceedings 15th Annual IEEE International ASIC/SOC Conference, Rochester, NY, US. pp. 474-475.

[4] Nordic Semiconductor. 2011. Preliminary Product Specification v1. 2 Archived. At the Wayback Machine.

[5] Radovan Vrana. 2014. Access to digital information resources as a support to academic achievement. in Central European Conference on Information and Intelligent Systems. pp. 144-151.

[6] J. Allwood and R. Schroeder. 2000. Intercultural communication in a virtual environment. in Intercultural Communication. 4: 1-15.

[7] N.G. Bagdasaryn. 2011. Intercultural communication in the context of new media. Website http://www.itas.fzk.de/eng/esociety/preprints/mediaculture/Bagdasaryan.pdf.

[8] D.M. Boyd and N.B. Ellison. 2007. Social network sites: Definition, history, and scholarship. in Journal of Computer-Mediated Communication. 13(1): 210-230.

[9] G.M. Chen and K. Zhang. 2010. New media and cultural identity in the global society. In R. Taiwo (Ed.), Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction), Hershey, PA: Idea Group Inc. pp. 801-815.

[10] W. Chen. 2010. Internet-usage patterns of immigrants in the process of intercultural adaptation. in Cyber psychology, Behavior, and Social Networking. 13(4): 387-399.

[11] Cheong P. H. and Gray. K. 2011. Mediated intercultural dialectics: Identity perceptions and performances in virtual worlds. in Journal of International and Intercultural Communication. 4(4): 265-271.

[12] C.Y. Chiang. 2010. Diasporic theorizing paradigm on cultural identity. in Intercultural Communication Studies. 19(1): 29-46.

[13] Rajdeep Bhanot and Rahul Hans. 2015. A Review and Comparative Analysis of Various Encryption Algorithms. in International Journal of Security and Its Applications. 9(4): 289-306.