International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 14 (2018) pp. 11454-11460

A Novel Wireless Sensor Networks Anti-jamming Technique Based on a Hybrid DS-CDMA/ OFDM/ FH

Mariam Yasin[1], Prof Adwan Yasin[1], Dr Amjad Abu Jazar[1], Dr Mohammad Hamarsheh[1]

[1]Engineering and Information Technology Faculty, Arab American University Jenin, Jenin, Palestine.

Abstract

This paper utilizes the combination of DS-CDMA with OFDM and FH in order to enhance anti-jamming technique in wireless sensor networks (WSN). The DS-CDMA component provides user isolation and protection whilst preserving the ability of many users to use the same carrier frequency simultaneously. The OFDM component removes ISI and enhances resistance to multipath effect. The FH component solves the near-far problem inherent in DS-CDMA. The proposed technique complicates the jammer task by expanding the number of randomly generated and used frequencies. The suggested technique can be adapted to be used in different transmission data rate and different jamming levels.

Keywords: WSN, jamming attacks, CDMA, OFDM, Frequency hopping.

INTRODUCTION

Wireless sensor network (WSN) can be described as a group of small devices which we call them nodes connected wirelessly with each other in order to collect data from specific field. These nodes are self organized and transmit data to the neighbor node until it reaches the destination. WSN's are being used in many different applications like observing the environment and monitoring it [1-3].

WSN's have some challenges that must be taken into consideration because of its broadcasting nature during data transition in addition the ability of being reached from the outside world. Jamming attacks are one of the most main challenges that WSN's face. Jamming attacks [4] are physical layer attacks that target the communications between nodes and prevent the node from receiving data by interrupting the transmitted signal.

Jamming has different types that have been proven to be effective [5]: 1) The Constant jammer, jammer continuously emits random bits to the used channel between nodes so the legitimate node will find the channel busy every time it tries to send a packet; 2) Deceptive jammer, this type of jammer tries to deceive communicator to believe that there is a legitimate packet being transmitted in the channel by sending regular packets instead of random ones; 3) Random Jammer, this type sends either random bits or regular packets trying to save energy specially in situations when the jammer doesn't has enough power; the mentioned types of jamming are called active jamming which tries to keep the channel busy all the time, there is another type of jamming that jams the channel only when its active, it remains idle as long as the channel is idle so whenever it senses any activity in the channel it starts jamming, this type called the reactive jamming.

Jamming algorithms have been developed during the years causing performance degradation, loss of packets and many other issues. In order to defend these harmful attacks the need of developing new anti-jamming techniques has become a must. Many algorithms have been proposed, like detecting the jammer location, channel surfing and frequency hopping mechanisms. For detecting jammer location [6] jamming devices must be localized in the wireless network to avoid any distraction caused by the jammers, taking into account that any algorithm must use minimum network resources. Channel surfing technique [7] depends on changing the communication channel between sensor nodes every time it senses a jamming attack. Finally the frequency hopping (FH) techniques which used for transmitting radio signals by switching between different frequency channels based on a random sequence known between transmitter and receiver [8]. This technique is widely used because it has small probability of detection. Even though FH considered an efficient way for preventing jamming attacks, it fails to overcome the problem when it faces an intelligent jammer that updates his own jamming mechanism. In this paper a new algorithm has been proposed that combines FH with Orthogonal Frequency-Division Multiplexing (OFDM) and Direct Sequence- Code Division Multiple Access DS-CDMA.

RELATED WORK

Nejla Rouissi et al. [9] suggested a new intelligent algorithm for avoiding denial of service attacks (DoS) in wireless sensor networks (WSN's), which is a type of jamming attacks. The proposed algorithm combines Direct Sequence Spread Spectrum, Time-Hopping Spread Spectrum and Frequency Hopping Spread Spectrum techniques, authors tried to combine all these techniques in order to overcome disadvantages from each one alone and maximize their features together. Even though security has been improved to defend DoS attacks, the performance of this algorithm has not proven yet also it's just specialized in DoS attacks not Jamming attacks in general.

The authors in [10] proposed an anti-jamming technique for wireless sensor networks based on the idea of generating the hopping pattern in a way such that it's hard for the jammer to identify the hopping sequence. The generator matrix provides many advantages compared with the existed techniques, for example, high security, less memory used in the sensor nodes since it has a very limited one, less complex and others. All sensor nodes contain the generator matrix to achieve

synchronization by generating exactly the same hopping pattern.

A new anti jamming algorithm has been proposed in [11] based on optimal decision rule. This algorithm takes into consideration the individual decision for each node, whether to switch frequency or not. Then it makes best decision for the whole network which tries to find best fit of all. The goal is to maximize the throughput in all over the network and minimize energy consumption since the used algorithms consume much energy. This algorithm is applicable on the static wireless sensor network and static jammers; it hadn't proven its effectiveness on the dynamic networks.

Jeongyoon Heo et al. [12] proposed a new anti-jamming model for low-power and lossy networks called (Dodge-Jam). The proposed model tries to avoid sneaky jammers and also tries to restore the packets from the jammed transmissions. Several mechanisms were used, the combination of 'multi-ACK channel hopping', 'ACK channel hopping' and 'multi-block data shift'. Experimental results showed better packet delivery ratio. This technique only defeated three types of jamming attacks so it's not a general method to be used for all types.

P. Bhavathankar et al. [13] discussed a new method in topology control that has been proposed for wireless sensor networks in order to avoid jamming. The proposed model TC-JAM verifies packet delivery integrity, also guarantee less energy consumption and increase network lifetime during jamming. Each node chooses the level of power transmission while covering the optimal group of neighbours. So, as the sink node identifies the jamming nodes the rest of nodes modify power transmission in order to minimize power consumption. The results showed less energy consumption and increasing in network life time compared with existing schemes. The algorithm hasn't ensured QoS of the network.

The authors in [14] suggested a new anti-jamming technique for wireless sensor networks in order to improve quality of the affected links by jammers. Network users try to work together by giving the jammed one higher access probability to the channel so they get bigger share of its utilization, also using shared communication techniques the throughput in the jammed links are improved. The results showed some achievements compared with existed non-cooperative algorithms

Kai Zeng [15] discussed physical layer key generation process in order to overcome the security challenges that wireless sensor networks (WSN) face like jamming attacks. By analyzing the strength of the security in the existed key generation models, the authors proposed a new model that suggests a random probing signal in order to cover the information about channel state, also a secret key will be generated in this process. The results showed that proposed model has higher security strength compared with the existed models.

The authors in [16] suggested a new model for detecting jamming attacks using swarm intelligence, in particular the artificial bee colony. Distance, packet loss and energy are the performance parameters that affect the decision making in the proposed model. Network conditions caused can be separated, either it's by jammers or it's by natural source. The simulation results showed the effectiveness of the model but haven't been tested in a real world.

A new range-free model (PSO) has been proposed in [17] to locate jamming attack source in the wireless sensor networks. The algorithm depends on each node position whether it's jammed or not jammed, it takes the smallest covering circle of the jammed positions and jammer locations will be in the center of the circle. The results showed higher accuracy compared with other existed range-free models also the model gives lower localization error.

A security algorithm for wireless sensor networks has been proposed in [18]. This model deals with Denial of Service Attacks (DOS) by making a strong authentication against it. Watchdog technique is being used in this model in order to monitor the intruder node in the network, every time the watchdog node notice a malicious node it immediately give information about it. The network is divided into cluster and assigned with cluster head which will be the watchdog node. The results showed some improvements in the throughput. The algorithm deals with DOS attacks and isn't tested on other attacks.

The authors in [19] tried to minimize jamming by using combination of frequency hopping (FH) and transmission rate adaptation (RA) techniques. Using this model the transmitter is able to avoid jammers by modifying the channel and also changing its rate. The paper takes into consideration one type of jammers "reactive-sweep" that aims to degrade throughput in the wireless network. The interaction between transmitter and jammer in the proposed algorithm was modeled as zero-sum Markov game. The used policy helps the transmitter to decide when to hop to another channel and gives the best transmission rate to be used. The results showed an improvement in the throughput.

Meng Zheng et al. [20] a new theoretical framework has been proposed based on Adaptive frequency hopping approach instead of Blind frequency hopping approach, so instead of switching the frequency in blindness way; the new frequency will be chosen by the network manager carefully in order to maximize the transmission reliability by using a fixed control channel to communicate. This method has successfully achieved their goal, but they didn't take into consideration the consequences of losing the connection with the network manger or with the control channel.

Matthew Hannon et al. [21] has proposed a new frequency hopping pattern generation technique to maximum transmission data rate and minimizes the bit error ratio during data transition. The proposed method depends on prior statics about the number of times each channel has been jammed to generate best sequence of frequency channels with minimum probability to jam in the future. The simulation results showed that described method offers a better performing than random frequency hopping generators.

A code tree scheme has been discussed in [22] that help to avoid jammers, this system works in all spread spectrum communications scheme. The receiver works together with the transmitter in order to identify jammers, that's because the

transmitter has more information than others. The proposed scheme tries to lessen the jamming attack though the transmitter is allowed to continue transmitting less code than number of users. The simulated results showed improvement on transmitting.

Marco Tiloca et al. [23] concentrate on a particular sort of selective jamming, such that the jammer tries to interrupt communication to single specific sensor node. This type of attack is easy to do on TDMA-based WSN since the node on this type use the same slot for data transmission for many repeated superframes. To avoid this problem, the authors proposed a new method to avoid such attack called "JAMMY"; at the end of every super-frame a utilization pattern is computed for the next slot to make it unpredictable for the jammer. The results showed that the JAMMY method has no overheads.

Anthony D. Wood et al.[24] proposed a novel Medium Access Control (MAC) protocol 'DEEJAM' tries to solve the problem of the stealthy jammers, the suggested protocol conceal communication from the jammer, by evading its search to minimizes the effect. The protocol aims to reduce packet loss while the network is operating or during jammer attack. DEEJEM has major computational and energy cost.

A new model for detecting DDOS attacks in WSN has been suggested in [25], the algorithm senses the attack at early phases in order to minimize the data loss and save more energy. By dividing the network into grids, each grid is assigned with an examiner node; this node is responsible for distinguishing between normal nodes and malicious ones. Examiner node depends on number of neighbours as a threshold and if any node sends packets more than the threshold, the examiner node will mark this node as a malicious node.

Balamurugan Gopalakrishnan et al. [26] proposed chaotic frequency hopping (CFH) model as an anti jamming technique for wireless sensor networks (WSNs). The proposed model uses a chaotic signal in order to confuse the jammer by its chaotic behavior. The chaotic signal is responsible about selecting the hop for transmitting without using a pre shared key. The results showed that the CFH model is more secure than the normal FH especially for reactive jammer.

Sukumaran A.N et al. [27] proposed a novel algorithm that uses twenty hopping patterns and in each pattern it uses six hopes. For each generated pattern there are three odds and three evens frequency channels. All nodes store all patterns and all seed values, from the pattern table ten patterns are chosen based on the seed values. Each node has to store many of seed values and this is memory costly.

Yadong et al. [28] suggested a frequency hopping (FH) algorithm for defending jamming attacks in wireless sensors networks (WSNs). The proposed model tried to increase the network reliability, by switching the frequency while the packet drop rate becomes beyond a pre-decided threshold. Results showed increasing in network reliability comparing with the slotted frequency hopping.

PROPOSED SYSTEM MODEL

The overall block diagram of DS-CDMA /OFDM/FH system is shown in Figure 1.

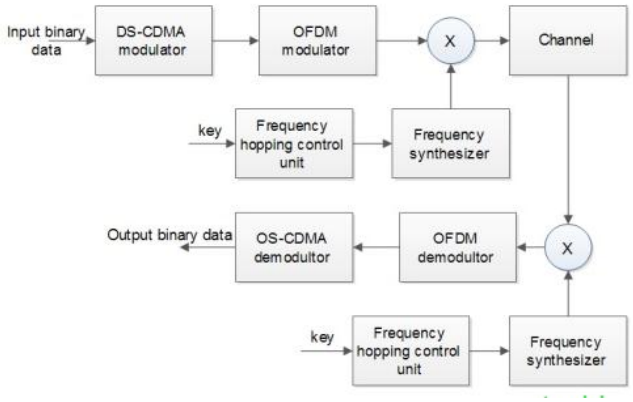

Figure 1. Block Diagram of DS-CDMA /OFDM/FH System

The generation of DS-CDMA /OFDM/FH signal is considered as three sequential phases see Figure 1. The input binary data is first spread with a unique spreading code of length N and when applied to OFDM modulator which uses multiple subcarriers, equal in number to the length of the spreading code. The output of the OFDM modulator is applied to frequency hopping section which consists of multiplier, frequency synthesizer and frequency hopping control unit.

There are few points to be noticed:

Bandwidth and number of OFDM sub-channels

Orthogonal frequency-division multiplexing (OFDM) is used in this model in order to increase number of sub-channels in the 2.4 band that is been used in the WSN, as shown in Figure 2 the IEEE 802.15.4 has a standard division for the used channel. The number of sub-channels that IEEE proposed is 16 sub-channels, and channels capacities are defined as 2 MHz for each.

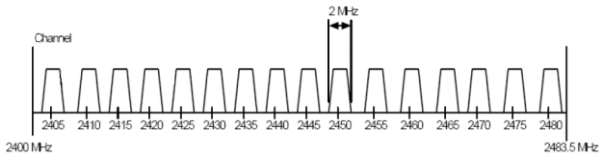

Figure 2. IEEE 802.15.14 Channel Selection

OFDM divides the channels into many sub-channels that are orthogonal to each other; previously the division of the channel was done using normal FDM, which caused using lots of guard bands in order to prevent interference between transmitted signals. By using OFDM we can double the number of channels of original FDM and by this we save great bandwidth and spectral effectiveness in addition mitigation ISI and delay.

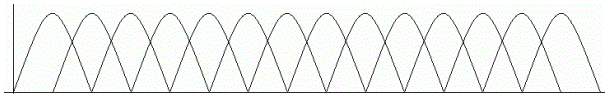

Figure 3. OFDM Orthogonal Sub-Channels

In case of frequency hopping that has been used to avoid jamming, 16 channel to hope among them have large probability to be exposed by the jammer, so probability P for jammer to guess the used channel will be $P=\frac{1}{\text{number of channels}}$, in IEEE case $P=\frac{1}{16} \cong 0.06$, this number make lots of troubles during data transmission and makes lots of data loss. To overcome this issue our proposed model aims to minimize P to minimum in order to increase the complexity of our suggested anti-jamming technique by increasing number of channels. In order to achieve this goal we employed OFDM, and we decrease the capacity of each sub-channel to satisfy the required data transmission rate in most WSN's.

In this paper, we are interested in the unlicensed frequency band (2.4 GHz-2.5 GHz) with a total bandwidth of 100 MHz. The number of OFDM sub-channels is determined by the channel coherence bandwidth (Bc) which in turn is determined by the rms delay spread (Trms). Suppose that the rms delay spread Trms =0.266 ms which is suitable for open area and suburban area.

The coherence bandwidth is determined as:

$$Bc=\frac{1}{5\ Trms} \quad (1)$$

$$Bc=\frac{1}{5 \times 0.266} = 750\ KHz$$

Usually the OFDM sub channel bandwidth (Bsc) is much less than the coherence bandwidth

$$Bsc << Bc \quad (2)$$

$$Bsc \approx 0.1\ Bc$$

$$Bsc = 0.1 \times 750\ KHz = 75\ KHz$$

Suppose the signal to noise ratio $(\frac{S}{N})$ is equal to 0.8, then according to Shannon capacity theorem, the channel capacity (C) is determined as:

$$C=BW \log_2 (1+\frac{S}{N}) \quad (3)$$

$$C= 75\ KHz \log_2 (1+0.8) = 64\ Kbps$$

The number of sub channels for sub carriers (Nsc) is equal to:

$$Nsc=\frac{100\ MHz}{75\ KHz} \cong 1328 \text{ sub channels}$$

In this paper we will take the Nsc= 1024 for data because according to IFFT, the number of IFFT points must be equal to a number that is a power of 2.

The rest of sub-channels will be divided as shown in Figure4, 256 sub-channels will be used as control channel and the rest will be left without particular use as guard channels in case of interference while transmitting high data rate. The sub channels are not fixed, for example, data can be transmitted at any channel from the 1328 sub-channels but number of channels that is used to transmit data mustn't exceed 1024 sub-channels.

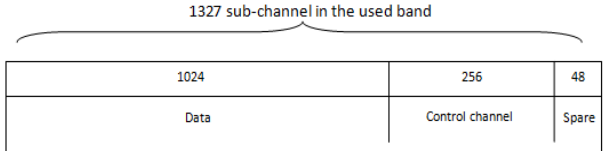

Figure 4. Set of Used Frequencies

Modulation

Any type can be used for modulating CDMA sequence, in our case; it's modulated in the OFDM transmitter as M-QAM.

CDMA multiplexing technique is used to make large number of users access the network in the same time by giving each user a unique code sequence called pseudo noise (PN), this code will be like a signature for any transmitted data bit.

This technique doesn't divide the transmission according to time or other methods; instead the division will be done by using the assigned code for each user. The code is transformed in a wide band signal collecting user's signals. The user code is used to extract the user's signal from the wide band signal, in order to recover his data.

CDMA suffers mainly from near-far problem where the signal travels in different paths in order to reach the destination, but combining it with proposed FH technique solves this problem. This makes sure that there are no two sensors operating in the same frequency.

Since jamming attacks may have different levels of complexity we adapt our proposed model to deal with all jamming levels. In CDMA technique we suggest using different Walsh code size where each bit of data will be sent along with the used code. Size of Walsh code depends on the level of jamming, suggested model divides the jamming attack level into four categories: low jamming level (J_0), medium jamming level (J_1), high jamming level (J_2) and very high jamming level (J_3). Where we use 8, 16, 32 and 64 bits sequentially Walsh code on each data bit takes. Number of sub channels (NSC) needed to transfer data throughput of 8 Kb/s will be defined according to the following Equation 4.

$$NSC=\frac{\text{data T} \times \text{chips}}{\text{SC}} \quad (4)$$

Such that

Data T = 8 Kb

Chips= number of Walsh code bits will be used according to the jamming level

SC= Sub channel bandwidth and it equals 64 Kb/s

For example, if the network suffered from jamming attack from level j_3, number of sub channels needed to transfer 8 Kb/s will be= $\frac{8 \times 64}{64}$ = 8 sub- channels

Frequency Sequence Generator

Synchronization is achieved by using cyclic prefix in OFDM modulator.

In order to generate frequencies, a random number generator (RNG) has been used; it generates a sequence of numbers that represents sub-channels, which are used in order to hope among the frequencies. Every channel band width will be given a number from {0,1,2, …., 1327}, taking into consideration that our suggested bandwidth will be 75KHz, so number 0 will express the 2.400 MHz channel bandwidth, number 1 will express the 2,400075 MHz channel bandwidth and so on. Each number will be converted into carrier i using the following Equation 5.

$$\text{Carrier } i = i * f_0 + \text{base} + \frac{f0}{2} \qquad (5)$$

Such that

i: the output number from the random number generator

f_0: 75 KHz, sub-channel bandwidth

Base: 2.4 MHz

At the beginning a special key that exists in each authorized node is used to generate the initial frequency sequence using the random number generator, when all frequencies in the sequence is used, the synch node sends a new seed to be used as an input instead of the key for the RNG as shown in Figure 5.

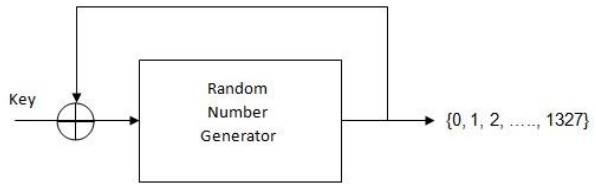

Figure 5. Frequency Generator

In order to deal with the case of repetitions among the output random numbers, the following steps are done:

- After the sequence is generated each node finds the repeated numbers.
- The repeated numbers are excluded and the output is arranged
- Search for the missing numbers and add them to the generated sequence.

Synchronization is mainly needed when we add a new node to the WSN, adding a new node to the network will make confusion to the new node since the used frequency is not fixed and the nodes keep hopping among the channels.

We solve this problem by using key dependent random number generator that uses a predefined secret key in all authorized nodes see Figure 5, any new node can guess and produce the sequence of used frequencies at any time which enable it to start transmitting data on the right channel as soon as it joins to the network.

PERFORMANCE EVALUATION

Performance of DS-CDMA

It is believed that there are K active users. Each user has a PN sequence with L chips per message symbol period Ts such that Ts= LTc, where Tc is the chip duration. The output of DS-CDMA modulator can be expressed as:

$$Sk(t) = \sqrt{\frac{2Es}{Ts}}\, mk(t)\, pk(t) \cos(2\pi fct + \emptyset k) \qquad (6)$$

Where:

Es is the signal energy per symbol

pk(t) for the kth users, it is the PN code sequence

mk(t) for the kth users, it is the data sequence

and ∅k the kth modulator spreader introduce it as the phase angle.

The probability average of bit error is given by:

$$Pb = Q\left(\frac{1}{\sqrt{\frac{k-1}{3L} + \frac{N0}{2Eb}}}\right) \qquad (7)$$

Where:

K: number of users

L: number of chips

No: the noise spectral density

Eb: the signal energy per bit

For the interference limited case where thermal noise is not a factor, $\frac{Eb}{N0}$ tends to infinity and the probability average of bit error is given by :

$$Pb = Q\left(\sqrt{\frac{3L}{k-1}}\right) \qquad (8)$$

Performance of OFDM-FH

The bit error probability for M-QAM is given by:

$$Pb = [\,2\,(1-\tfrac{1}{\sqrt{M}})/\log 2\,\sqrt{M}\,] \,.\, Q\left(\sqrt{[(3\log\sqrt{M})/(M-1)\;\; \tfrac{2Eb}{N0}]}\right) \qquad (9)$$

M → stands for M-QAM inside OFDM modulator.

Performance of the hybrid DS-CDMA/ OFDM/ FH system is the same as OFDM/ FH as basically the transmission and reception are carried out by the OFDM-FH system, DS - CDMA component is responsible for generating data stream in

complex way. So the suggested system is an OFDM-FH system.

The Final proposed model is illustrated in Figure 6.

CONCLUSION

We proposed a model that integrates CDMA/OFDMA/FH in order to increase jamming resistance; we extend the number of used frequencies by reducing the sub-channels bandwidth to 75 KHz which is sufficient in many applications for WSN. As a result we achieved 1327 sub-channels that can be used during the frequency hopping which make it very difficult for jammer to predict the used frequency during data transmission. We developed a frequency generator which is key dependent that enables the nodes to synchronize and coordinate frequencies.

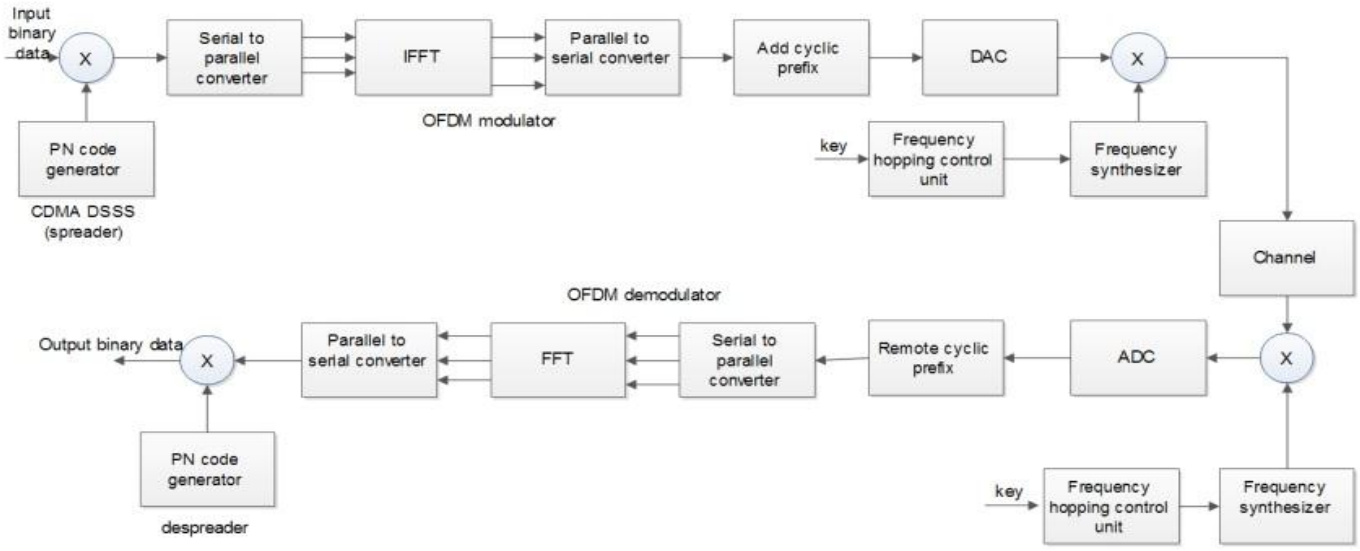

Figure 6. Expanded Proposed System Block Diagram

REFERENCES

[1] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, "Detection, classification, and tracking of targets," IEEE Signal Processing Magazine, vol. 19, no. 2, pp.

17 –29, Mar. 2002.

[2] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, and S. S. Sastry, "Distributed control applications within sensor networks," Proceedings of the IEEE, vol. 91, no. 8, pp. 1235 – 1246, Aug. 2003.

[3] F. Zhao, "Wireless sensor networks: a new computing platform for tomorrow's Internet," in Proceedings of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, 2004, 2004, vol. 1, pp. I – 27 Vol.1.

[4] Adam, M. M., & Shehu, N. M. (2016). Wireless Sensor Networks: Security Issues. Science [ETEBMS-2016], 5, 6.

[5] Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. IEEE network, 20(3), 41-47.

[6] Koh, J. Y., & Zhang, P. (2017, December). Localizing Wireless Jamming Attacks with Minimal Network Resources. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (pp. 322-334). Springer, Cham

[7] Xu, W. (2007, April). Channel surfing: defending wireless sensor networks from interference. In Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on (pp. 499-508). IEEE.

[8] Hu, C., Kim, J. Y., Na, S. Y., Kim, H. G., & Choi, S. H. (2017). Compressive Frequency Hopping Signal Detection Using Spectral Kurtosis and Residual Signals. Wireless Personal Communications, 94(1), 53-67.

[9] Rouissi, N., Gharsellaoui, H., & Bouamama, S. (2016, June). A hybrid DS-FH-THSS approach anti-jamming in Wireless Sensor Networks. In Software Engineering Research, Management and Applications (SERA), 2016 IEEE 14th International Conference on (pp. 133-139). IEEE.

[10] Achuthan, E., & Kishore, R. (2014, April). A novel anti jamming technique for Wireless Sensor Networks. In Communications and Signal

Processing (ICCSP), 2014 International Conference on (pp. 920-924). IEEE.

[11] Bhavathankar, P., Sarkar, S., & Misra, S. (2017). Optimal decision rule-based ex-ante frequency hopping for jamming avoidance in wireless sensor networks. Computer Networks, 128, 172-185.

[12] Heo, J., Kim, J. J., Bahk, S., & Paek, J. (2017, June). Dodge-jam: Anti-jamming technique for low-power and lossy wireless networks. In Sensing, Communication, and Networking (SECON), 2017 14th Annual IEEE International Conference on (pp. 1-9). IEEE.

[13] Bhavathankar, P., Mondal, A., & Misra, S. (2017). Topology control in the presence of jammers for wireless sensor networks. International Journal of Communication Systems, 30(13).

[14] Zhang, L., Guan, Z., & Melodia, T. (2016). United against the enemy: anti-jamming based on cross-layer cooperation in wireless networks. IEEE Transactions on Wireless Communications, 15(8), 5733-5747.

[15] Zeng, K. (2015). Physical layer key generation in wireless networks: challenges and opportunities. IEEE Communications Magazine, 53(6), 33-39.

[16] Sasikala, E., & Rengarajan, N. (2015). An intelligent technique to detect jamming attack in wireless sensor networks (WSNs). International Journal of Fuzzy Systems, 17(1), 76-83.

[17] Pang, L., Chen, X., Xue, Z., & Khatoun, R. (2017, September). A Novel Range-Free Jammer Localization Solution in Wireless Network by Using PSO Algorithm. In International Conference of Pioneering Computer Scientists, Engineers and Educators (pp. 198-211). Springer, Singapore.

[18] Raja, K. N., & Beno, M. M. (2014). On securing wireless sensor network-novel authentication scheme against DOS attacks. Journal of medical systems, 38(10), 84.

[19] Hanawal, M. K., Abdel-Rahman, M. J., & Krunz, M. (2016). Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems. IEEE Transactions on Mobile Computing, 15(9), 2247-2259.

[20] M. Zheng, B. Yang, W. Liang, H. Yu, and L. Chen, "Adaptive frequency hopping in industrial Wireless Sensor Networks: A decision-theoretic framework," 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2015.

[21] Hannon, M., Feng, S., Kwon, H., & Pham, K. (2016, November). Jamming statistics-dependent frequency hopping. In Military Communications Conference, MILCOM 2016-2016 IEEE (pp. 138-143). IEEE.

[22] Chiang, J. T., & Hu, Y. C. (2007, September). Cross-layer jamming detection and mitigation in wireless broadcast networks. In Proceedings of the 13th annual ACM international conference on Mobile computing and networking (pp. 346-349). ACM.

[23] Tiloca, M., De Guglielmo, D., Dini, G., Anastasi, G., & Das, S. K. (2017). JAMMY: a Distributed and Dynamic Solution to Selective Jamming Attack in TDMA WSNs. IEEE Transactions on Dependable and Secure Computing, 14(4), 392-405.

[24] Wood, A. D., Stankovic, J. A., & Zhou, G. (2007, June). DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. In Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on (pp. 60-69). IEEE.

[25] Kaushal, K., & Sahni, V. (2016). Early Detection of DDoS Attack in WSN. International Journal of Computer Applications, 134(13), 0975-8887.

[26] Gopalakrishnan, B., & Bhagyaveni, M. A. (2017). Anti-jamming communication for body area network using chaotic frequency hopping. Healthcare Technology Letters, 4(6), 233-237.

[27] Sukumaran, A. N., Kishore, R., & Radha, S. (2014). A Novel Frequency Hopping Spread Spectrum Technique using Random Pattern Table for WSN. Adhoc & Sensor Wireless Networks, 23.

[28] Wan, Y., Wang, Q., Duan, S., & Zhang, X. (2009, September). RAFH: reliable aware frequency hopping method for industrial wireless sensor networks. In Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on (pp. 1-4). IEEE.