International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 6673~6681
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp6673-6681

Physical layer security and energy efficiency over different error correcting codes in wireless sensor networks

Mohammed Ahmed Magzoub[1], Azlan Abd Aziz[2], Mohammed Ahmed Salem[3], Hadhrami Ab Ghani[4], Azlina Abdul Aziz[5], Azwan Mahmud[6]
[1,2,3,4, 5]Faculty of Engineering and Technology (FET), Multimedia University, Malaysia
[6]Faculty of Engineering (FOE), Multimedia University, Malaysia

Article Info

Article history:

Received Nov 26, 2018
Revised May 29, 2020
Accepted Jun 6, 2020

Keywords:

Energy efficiency
Error correcting codes
Physical layer security
Reed solomon
Security gap (S_G)
Signal to nose ratio
Wireless sensor networks

ABSTRACT

Despite the rapid growth in the market demanding for wireless sensor networks (WSNs), they are far from being secured or efficient. WSNs are vulnerable to malicious attacks and utilize too much power. At the same time, there is a significant increment of the security threats due to the growth of the several applications that employ wireless sensor networks. Therefore, introducing physical layer security is considered to be a promising solution to mitigate the threats. This paper evaluates popular coding techniques like Reed solomon (RS) techniques and scrambled error correcting codes specifically in terms of security gap. The difference between the signal to nose ratio (SNR) of the eavesdropper and the legitimate receiver nodes is defined as the security gap. We investigate the security gap, energy efficiency, and bit error rate between RS and scrambled t-error correcting codes for wireless sensor networks. Lastly, energy efficiency in RS and Bose-Chaudhuri-Hocquenghem (BCH) is also studied. The results of the simulation emphasize that RS technique achieves similar security gap as scrambled error correcting codes. However, the analysis concludes that the computational complexities of the *RS* is less compared to the scrambled error correcting codes. We also found that BCH code is more energy-efficient than RS.

Corresponding Author:

Azlan Abd Aziz,
Faculty of Engineering and Technology,
Multimedia University,
Melaka, 75450, Malaysia.
Email: azlan.abdaziz@mmu.edu.my

1. INTRODUCTION

The open nature of the wireless communication technologies makes the wireless medium subject to many threats. Due to the increase in the number of attacks against the wireless communication system, a growing interest has developed in securing the information over wireless transmission system [1]. In the TCP/IP model, security algorithms are applied in the upper layers. However, physical layer security (PLS) does not contain any type of security even though it contains features that could provide security from information theory point of view [2].

In PLS, the transmitter and receiver are assumed to be aware of the techniques used for transmission. PLS is achieved when the parties of the communication system aware of the information about the used techniques for transmission yet there is a variation in the quality between wiretap channel and the main channel [3-7]. In addition, it is assumed that the wiretapped channel (eavesdropper channel) is a degraded version of the main channel, this helps the legitimate receiver using the main channel to get back the transmitted data but the eavesdropper node is not able to get back the transmitted data and this is how PLS is achieved. There are several metrics for security performance. In this paper, the selected security

performance metric is the security gap (S_G) because it is practical to be implemented, depends on the bit error rate (BER) and the signal to noise ratio (SNR), and it is simple. Security gap is defined as the difference between the SNR of the intended receiver and the SNR of the eavesdropper [8, 9].

Wireless sensor network (WSN) helps in analyzing and collecting the information. Security is the major challenge to deploy for the WSN. The main reason is the vulnerability of the WSN to several attacks such as wormhole attacks, Hello flood attacks, black hole attack, Sybil attack, attacks the data in transit, and denial of services [10]. Cryptography is an approach to avoid these attacks. However, the algorithms of cryptography are computationally expensive. Researchers proposed several strategies to calculate the quality of the transmitted data, such as bose-chaudhuri-hocquenghem (BCH), reed solomon (RS), and low-density parity check (LDPC). The challenging part is to identify the suitable strategy in terms of power efficiency for error correction [11, 12]. This open research question makes this topic to be the interest of many researchers.

The threats that are facing the WSN leads to implement several works to prevent WSN from some of the attacks. Typically, the energy and computation abilities of WSN are not enough to manage the conventional security methods (sensor network method). To avoid the attacks with less computational energy and power, physical layer security for WSN is an excellent approach to be selected. In [13] demonstrate that the PLS techniques could be applied to WSN to ensure perfect secrecy. The authors of [14-16] claim that the ancryption techniques such as channel aware encryption, and stochastic encryption achive security and realibality. Yet, high computational energy and ability are required.

To the best of the authors' knowledge, the error correction codes benefits in WSN has not been adequately well investigated in terms of PLS. This paper studies the affects of various error correction codes on the security of WSN. In this paper, the S_G metric is used unlike the previous literature works where the maximum equivocation is used as the metric for security. In this paper, a brief explanation on the security and the energy efficiency of the WSNs is presented as well since many previous works only focus on the energy efficiency or the security aspects. Nontheless, there are a few investigations suggesting that the various channel codes affect the energy consumption differently for WSNs [17, 18]. The efficiencies of the code's energy are evaluated with an analytical radio model. The authors of [4] shows that the energy efficiency is changing with the variation of the codes based on the quality of the channel. In otherwords, there are small differences between the codes in terms of energy efficiency in a good quality channel. Since the processing power consumption for the coding technique is high [19], selecting the less complex coding technique is essential mainly with the WSN applications due to the processing and memory constraints [20].

This paper analyzes the PLS by investigating several error corrections codes such as RS t-error correction codes. Moreover, the focus is to study the affect of the t-error correction codes on the PLS. The BCH codes acchives high S_G compared with LDPC codes. Thus, BCH is introduced with additional techniques such as scrambling [21]. Scrambling the data bits is employed as an additional strategy to improve the security by decreasing the gap between the eavesdropper node and legitimate receiver. By scrambling the data bits, the probability of bit error is maintained close to 0.5 with the increasing of SNR [22]. The organization of this paper is as follows. Section 2 presents the system model. Section 3 provides some introduction regarding the scrambled t-error correction codes, RS correcting codes, and BCH code. Section 4 discusses the results of the comparison between scrambled t-error correction codes and the (RS). Finally, section 5 concludes this paper.

The main contributions of this paper are summarized as follow:

- The analysis of error correction codes such as scrambled error correction codes, BCH, and RS are illustrated in terms of S_G.
- The comparison in terms of S_G is investigated between the scrambled error correction codes and the RS.
- The comparison is done in terms of S_G between scrambled BCH and unscrambled BCH.

2. SYSTEM MODEL

In this research, the additive white gaussian noise (AWGN) wire-tap channel is utilized as the main transmission channel between the sender (Alice), the legitimate receiver (Bob) and eavesdropper node (Eve). This system model implemented firstly by [22]. Figure 1 illustrates the typical Wyner wiretap channel. The sender (Alice) uses any suitable transmission technique to send the data message to the legitimate receiver (Bob). The data is received by both Bob and Eve, where both are aware of the transmission technique used by the sender. As a result, the received data message at both Bob and Eve is recovered. However, the recovered messages differences in the channels between Eve and Alice, and Bob and Alice make the difference in the recovered message.

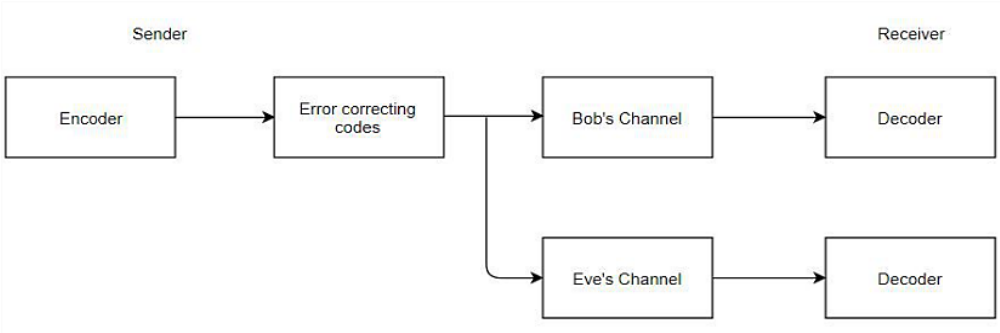

Figure 1. Wire-tap channel's ystem model

3. PERFORMANCE ANALYSIS FOR THE ERROR CORRECTION CODES

This section introduces each t-error correction codes techniques. The scrambled codes and the RS code are compared in terms of PLS.

3.1. Reed solomon (RS)

RS is a common error correcting code technique that is used with various bits. RS provides desirable results for correcting burst errors due to the correction of these errors done in the bits level. RS code is defined as $(n; k)$ code where k denotes the message bits in the codeword and n denotes the number of bits in the codeword. RS codes can correct $(n - k)/2$ errors [11]. The advantages of RS are increasing the SNR and the transmission secrecy rate.

3.1.1. Galois field (GF)

Galois field (GF) is a special field that has a special property, the arithmetic operations addition, subtraction, multiplication, and division on field elements always have results.

3.1.2. Generator polynomial

In RS, the valid codeword can be divided by the generator polynomial. The general polynomial is defined as:

$$g(x)(x - \alpha_i)(x - \alpha_i + 1) \ldots . (x - \alpha_i + 2t) \quad (1)$$

the codeword is defined as

$$c(x) = (x - \alpha_i + 1) \ldots . (x - \alpha_i + 2t) \quad (2)$$

where *g(x), i(x)* and *c(x)* are the generator polynomial, information block, and valid codeword, respectively.

3.1.3. Encoder

The 2t is calculated using:

$$p(x) = i(x).(xn - k) mod g(x) \quad (3)$$

In RS encoder each register holds a symbol that consist of 8 bits.

3.1.4. Decoder

The received message consists of two parts, the transmitted codeword and the errors.

$$r(x) = c(x) + e(x) \quad (4)$$

RS can find up to t error position and correct them. The probability of bit error of RS using hard decision decoding is calculated as,

$$P_P = 1/n \sum_{i=t_{ec}+1}^{\{t\}i} i \binom{n}{i} P^i (1 - P)^{n-i} \quad (5)$$

Where P denotes the probability of the channel bit error, n denotes the bits number in the codeword, and $t_{ec} = (n-k)/2$ is the capability of the RS code to correct errors. RS codes have various decoding strategies. However, the strategy of hard decision-decoding is selected. Figure 2 illustrates the BER of the RS codes with several code-length. Based on Figure 2, the RS codes are observed to be highly imperfect due to the increament of the probability of error with the decrease of the SNR and the codeword. This imperfection is considered as an advantage for security.

3.2. Bose-chaudhuri-hocquenghem (BCH)

BCH is deemed as an error correction codes technique that is able for correcting and detecting several bits error [23-25]. BCH is an error correcting code technique that is suitable for WSNs due to its properties of enhancing the efficiency of the energy by 23% [20]. BCH was selected by [21] to be scrambled to reduce the S_G between the eavesdropper and the legitimate receiver. In this section, BCH has been evaluated without using the scrambling techniques and compared against Reed Solomon without scrambling. Figure 3 indicates the impact of the scrambling on BCH code. The BER improves significantly with scrambling as the SNR increases and outperforms that without scrambling.

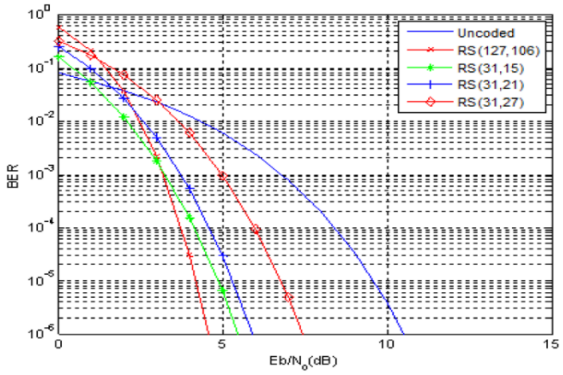

Figure 2. BER of RS codes using BPSK over an AWGN channel

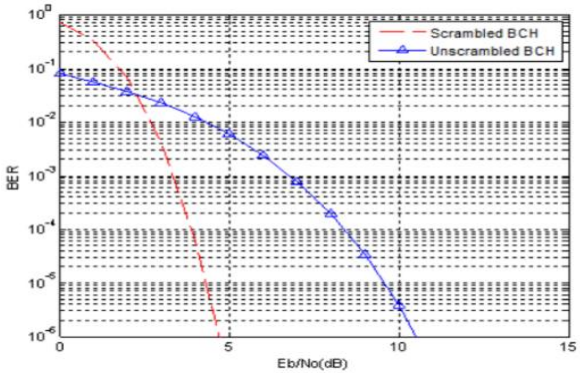

Figure 3. BER of BCH with and without scrambling

3.3. Scrambled t-error correction codes

The implementation of Non-systematic codes is firstly introduced in [22]. The authers of [20] utilize the scrambling techniques to reduce the S_G. Thus, proving that scrambling has a significant impact on the S_G. The scrambling technique assumed that the transmitter is going to encode the message as follow,

$$C = U.S.G \tag{6}$$

where the G is a generator matrix with dimension kxn, and S is scrambling matrix with dimension kxk. The generator matrix G can be written in different ways due to its systematic character. Now G can be written as $G = [I|C]$, I is identity matrix with dimension kxk, and C is $kx(n-k)$ parity check matrix. Now with all mentioned above. The codeword can be written as,

$$c = [U.S|\, U.S.C] = [m_l|m_r] \tag{7}$$

From the above equation, the m_l is the first $kbits$ of the codeword while the m_r is last rbits of the codeword. To ensure the PLS, the BER of the intended receiver should be low as well as the SNR should be high enough to ensure all the errors could be corrected and for that $U_B = u = m_l.S^1$ The bit error probability while theBER for the eavesdropper should be high, as well as the SNR, should be low so that the eavesdropper is not going to be able to decode the message and for that, the output of the descrambler for the eavesdropper can be written as,

$$U_E = u + e_l.S^{-1} \tag{8}$$

where e_l is the left part of the error vector $[e_l|e_r]$ for the perfect scrambling is calculated.

$$P_e^{PS} = 1/2 \sum_{j=1}^{k} \binom{k}{j} \sum_{i=t+1}^{n} \binom{n-k}{i-j} P_o^i (1-P_o)^{n-i} \quad (9)$$

In (9) computes the probability of the bit error for perfect scrambling where k denotes the total message bits in the codeword. The authors of [14] demonstrates the results of (9) using BCH codes. Figure 4 depicts the various level of scrambling as W represents the column weight of the scrambling matrix. The lowest S_G is retrieved with the perfect scrambling diagram.

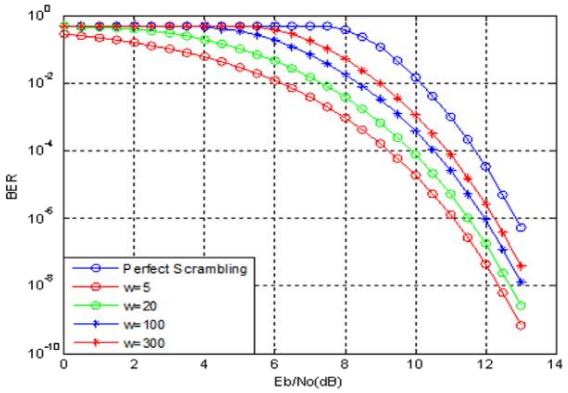

Figure 4. BER of different level of scrambling using BPSK over AWGN channel

3.4. Physical layer security for the error correction codes

The idea behind the coding techniques is to make the mutual information between the message and the encoded message is zero. The information leaked for the data may reach zero if the uncertainty of the randomization is small [15, 17]. In this paper, the S_G is performance metric used. The security for the transmitted data exists by maintaining the BER of the receiver close to aero and the eavesdropper to 0.5 and above. This condition ensures that the eavesdropper not able to decode the received message back. Let the BER average at the legitimate receiver and the eavesdropper be P_{B_e} and P_{E_e} respectively. Then, it is required that P_{E_e} be high to ensure security and that P_{B_e} be adequately low for ensuring the reliability. If the errors are identically independent distributed (IID) and P_{E_e} is close to 0.5, then eavesdropper is incapable of extracting data from the received sequence Z_n . For fixed $P_{B_e,max}, (\approx 0.5)$ and $P_{E_e,min}, (\approx 0.5)$ it must hold that

$a)\ P_{B_e} \leq P_{B_e,max}(reliability).$
$b)\ P_{E_e} \leq P_{E_e,min}(security).$

Let $SNR_{B_{min}}$ be the lowest SNR for which a) holds and let $SNR_{B_{max}}$ be the highest SNR for which b) holds. It is assumed that the receiver operates at $SNR_{B_{min}}$ and that eavesdropper SNR is strictly lower than $SNR_{B_{min}}$. The S_G performance metric is defined as $\frac{SNR_{B_{min}}}{SNR_{E_{max}}}$ in dB. The authors of [22] introduced a scheme in terms of the S_G which is the ratio between the SNR for the legitimate receiver and the SNR for the eavesdropper $\frac{SNR_B}{SNR_E}$.

3.5. Energy efficiency analysis

Based on [4], the largest energy consumption in a communication system is the tasks of reception and transmission. In (10) calculates the consumption of energy for sending data bits m throughout a wireless channel to the legitimate receiver at distance d.

$$E_L(m,d) = E_T(m,d) - E_R(m) \quad (10)$$

Where E_T is the consumed energy in the transmitter and E_R is the consumed energy at the receiver. At the transmitter the energy consumed is calculated as,

$$E_L(m,d) = E_{TC}(m,d) + E_{TA}(m,d) \quad (11)$$

where E_{TA} is the energy spent at the transmitter amplifier and E_{TC} is the spent energy by the transmitter circuit. The relationship between the energy spent per bit at the receiver and the energy spent per bit at the transmitter is assumed to be linear and can be found by the equation:

$$E_T(m,d) = m\left(e_{TC} + me_{TA}^{d^{\alpha}}\right) \quad (12)$$

$$E_R(k) = me_{RC} \quad (13)$$

where e_{TC} and e_{RC} are the components of the hardware. Finally, the relationship between energy consumption and the probability of bit error is illustrated as,

$$E_T(A) = \sigma\left(\frac{S}{N}\right)_r \quad (14)$$

$$\sigma = (NF_{RX})(N_o)(BW)(r\pi\lambda)^{\alpha}/(G_{ant})\left(n_{amp}\right)(R_{bit}) \quad (15)$$

4. SIMULATION RESULTS AND DISCUSSION

This section presents and analyses the comparison between the RS and t-error correction codes in terms of S_G metric. The codeword length for both techniques is considered as $n = 127$. RS and scrambled t-error correction codes are applied on the AWGN channel. Moreover, the data bits length for RS and scrambled t-error correction codes are considered to be $k = 106$. The error correcting ability for both RS and scrambled t-error correction codes are considered to be $T = 10$. The channel bit error probability for AWGN channel for both error correction codes is calculated as,

$$P = {}^{1}/_{2} * erfc\left(\sqrt{\left(ENL_{in} * {}^{k}/_{n}\right)}\right) \quad (16)$$

where $\frac{k}{n}$ is the code rate and ENL_{in} is the SNR. The S_G is illustrates Table 1 for the error correction codes.

Based on Table 1, RS correcting code technique is not added to another technique such as scrambling. Moreover, RS correcting code technique gives the smallist S_G compared with the other t-error correcting code techniques. Based on the S_G result, RS code is most secure error correcting without the addition of other techniques. Figure 5 shows the BER for the RS code and the scrambled t-error.

Table 1. Security gap for different error correction codes

Error correcting code	Securitygap(dB)
Scrambled error correction codes	4.8
Reed Solomon	4.5
Punctured LDPC	8
Unscrambled BCH	11

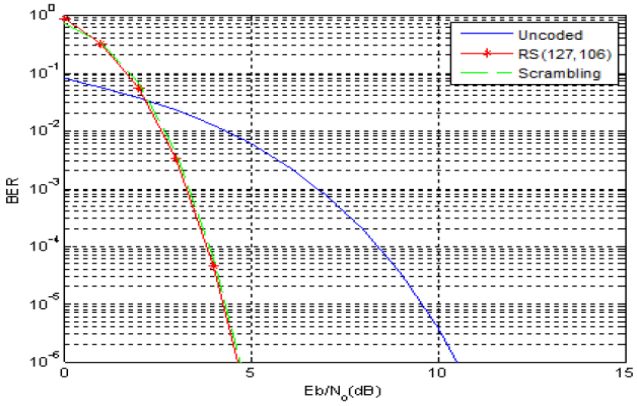

Figure 5. BER for the scrambled t-error RS codes

Table 2 compares the required time to simulate the error correction codes by using MATLAB version 7.14 (R2012a). Based on Table 2, we observe that the *RS* correcting code required less time (5.782384s) to execute the simulation of PLS. However, to execute the LDPC correcting code, more than 100 seconds are required. The computational complexity due to RS correcting code is seen to be less compared to scrambled error correcting, punctured LDPC, LDPC, and BCH codes.

Table 2. The run time for several error correction codes

Error correcting code	Runtime(s)
BCH	$24.512958s$
Reed Solomon	$5.782384s$
Punctured LDPC	$98.993429s$
Scrambled error correction codes	$20s$
LDPC	$102.439194s$

4.1. Comparison of energy efficiency between RS and BCH

Table 3 provides the required simulation parameters for compariong the efficiency of energy between RS and BCH. Based on Figure 6, the estimated consuming energy of the BCH code is less than the estimated consuming energy of the RS code. In the communication system the lower BER is estimated to consume low energy. In other word, the better quality of the channel is the lower energy consumption. At the probability for bit error of 0.04 the estimated consumption of energy is 0.05 for the BCH code. On the other hand, at the same probability of bit error for the RS code the consumption of energy is almost 0.16 joules/bit. It is clear that the BCH consume less energy than the RS within the conditions of wiretap channel.

Table 3. Simulation parameters for the energy efficiency comparison

Parameter	Value
Thermal noise	-173.8 dBm/Hz
Hardware dependent constant eTC	50
Hardware dependent constant eRC	50
Transmitter power efficiency	0.2
Receiver noise figure	10 dBm
Raw bit rate	115.2 k
Bandwidth	115.2 k
Antenna gain	10 dB
Path loss exponent	3
Wavelength	0.3 meter

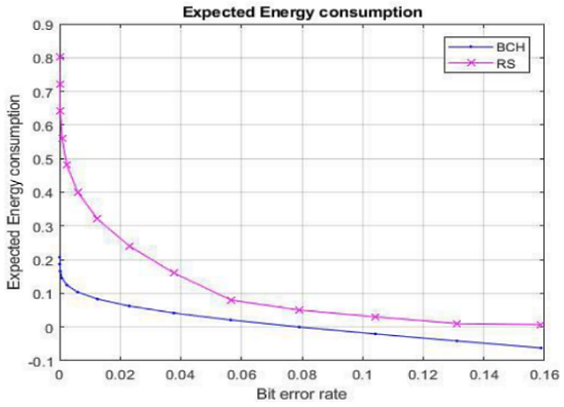

Figure 6. Estimated consumption of energy for RS code

5. CONCLUSION

We have presented the performance of RS and BCH codes in terms of energy consumption security aspects. We found that RS has almost the same S_G as scrambled error correction codes which require more energy consumption than RS. On the other hand, BCH is poised to be a good candidate in WSNs for physical

wireless security benefits as it consumes less energy consumption than RS. The limitation of this study is when both receivers have the same channel quality. For future studies, we will analyze the proposed work under different network physical interfaces.

REFERENCES

[1] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19-26, 2017.

[2] M. A. Salem, A. B. Abd. Aziz, M. Y. Bin Alias and A. A. Abdul Rahman., "Secrecy performance on half-duplex two-way multi-relay transmission technique under wireless physical layer security," *International Symposium on Information Theory and Its Applications*, pp. 668-672, 2018.

[3] H. El-gamal, H. V. Poor, and S. S. Shitz, "Wireless Physical Layer Security," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, 2015.

[4] M. A. Salem, A. B. Abd. Aziz, and M. Y. Bin Alias, "Cooperative Relay Transmission under Physical Layer Security for Non-Orthogonal Networks Layer Security for Non-Orthogonal Networks," *12th International Conference on Computer Science and Information Technology*, 2019.

[5] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned from Information Theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814-1825, 2015.

[6] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 1027-1053, 2017.

[7] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948.

[8] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros and B. Kwak, "LDPC for Physical Layer Security," *IEEE Global Telecommunications Conference GLOBECOM*, pp. 1-6, 2009.

[9] M. Baldi, M. Bianchi and F. Chiaraluce, "Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883-894, 2012.

[10] M. Dener," Security Analysis in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[11] N. A. Alrajeh, U. Marwat, B. Shams, S. Saddam, and H. Shah., "Error Correcting Codes in Wireless Sensor Networks : An Energy Perspective," *Applied Mathematics & Information Sciences Applied Mathematics & Information Sciences*, vol. 818, no. 2, pp. 809-818, 2015.

[12] M. A. M. Albashier, A. A. Aziz, Hadhrami Abd. Ghani, "Performance analysis of physical layer security over different error correcting codes in wireless sensor networks," *20th International Symposium onWireless Personal Multimedia Communications (WPMC)*, 2017.

[13] J. Choi, J. Ha and H. Jeon, "Physical layer security for wireless sensor networks," *IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1-6, 2013.

[14] H. Jeon, J. Choi, and S. W. Mclaughlin, Channel Aware Encryption and Decision Fusion for Wireless Sensor Networks, vol. 8, no. 4, pp. 619625, 2013.

[15] Y. Ren, A. Boukerche and L. Mokdad, "Performance analysis of a selective encryption algorithm for wireless ad hoc networks," *IEEE Wireless Communications and Networking Conference*, pp. 1038-1043, 2011.

[16] A. D. Wyner, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[17] K. D. Rao, "Channel Coding Techniques for Wireless Communications," *Springer*, 2015.

[18] W. K. Harrison and S. W. McLaughlin, "Physical-Layer Security: Combining Error Control Coding and Cryptography," *IEEE International Conference on Communications*, pp. 1-5, 2009.

[19] J. Zhu, Y. Zou and B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks," *IEEE Access*, vol. 5, pp. 5313-5320, 2017.

[20] V. Potdar, A. Sharif and E. Chang, "Wireless Sensor Networks: A Survey," *International Conference on Advanced Information Networking and Applications Workshops*, pp. 636-641, 2009.

[21] M. A. M. Albashier, A. A. Aziz, HA Ghani, "Performance Analysis of Physical Layer Security Over Different T-error Correcting Codes," *TENCON 2017*, 2018.

[22] M.A.M. Albashier, A.A. Aziz, HA. Ghani, AK Samigan., "Performance comparison of energy efficiency and physical layer security for reed solomon and bose-chaudhuri-hocquenghem codes in wireless sensor networks," *Proc. of 7th Int. Conf. on Computer and Communication Engineering*, 2018.

[23] T. Bartee and D. Schneider, "An electronic decoder for Bose-Chaudhuri-Hocquenghem error-correcting codes," *IRE Transactions on Information Theory*, vol. 8, no. 5, pp. 17-24, 1962.

[24] H. Modares, R. Salleh and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," Third International Conference on Computational Intelligence, Modelling & Simulation, pp. 308-311, 2011.

[25] M. Bloch, M. Hayashi and A. Thangaraj, "Error-Control Coding for Physical-Layer Secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725-1746, 2015.

BIOGRAPHIES OF AUTHORS

Mohammed Ahmed Magzoub received the B.S. degree in Telecommunication Engineering from Multimedia Universiti (MMU), Malaysia, in 2016. He is currently pursuing the master's degree in Telecommunication Engineering at Multimedia University (MMU), Malaysia. His research interest includes Wireless physical layer security, coding theory in communication systems, signal processing and wireless sensor networks.

Azlan Bin Abd Aziz received the B.S. degree in electrical and computer engineering from Ohio State University, Columbus, Ohio, USA in 1998 and the M.S. degree in communication engineering from the University of Manchester, UK in 2004. In March 2012, he obtained a Ph.D. degree in engineering and computer science at Nagoya Institute of Technology. His current research includes physical layer security for wireless networks, vehicular communications, and smart antenna applications.

Mohammed Ahmed Salem received the B.S. degree in Mechatronics Engineering from Universiti Teknikal Malaysia Melaka (UTeM), Malaysia, in 2017. He is currently pursuing the master's degree in Telecommunication Engineering at Multimedia University (MMU), Malaysia. His research interest includes Wireless physical layer security, cooperative relay networks and non-orthogonal multi access network.

Hadhrami Abd Ghani received his bachelor's degree in electronics engineering from Multimedia University Malaysia (MMU) in 2002. In 2004, he completed his master's degree in Telecommunication Engineering at The University of Melbourne. He then pursued his Ph.D. at Imperial College London in the same study area and completed his Ph.D. research in 2011. Currently, he serves as one of the academic and research staff members at Multimedia university (MMU).

Nor Azlina Ab Aziz received her Ph.D. degree from University of Malaya, Malaysia. She is currently a senior lecturer with the Faculty of Engineering and Technology, Multimedia University, Melaka, Malaysia. Her research interests include the fundamental aspects and applications of computational intelligence in wireless communication, bioinformatics, operational research and affective computing.

Azwan Mahmud received the B.Sc. degree (with first-class honors) in electrical and electronic engineering from the University College of London, London, U.K., in 1998, MBA degree in strategic management from the University of Technology Malaysia, in 2008, and PhD in wireless communication system from University of Manchester, UK, in 2014. His current research interests include the performance analysis for 5G cellular systems, heterogeneous systems, relay, small cells, wireless power transfer, D2D, DAS and V2X systems.