IMPROVING BER PERFORMANCE AND SECURITY IN PLC CHANNEL USING OSTBC, CONVOLUTIONAL CODING AND INTERLEAVING WITH HYBRID SDES-AES ENCRYPTION

B. RAJKUMARSINGH and S. SEECHURN

Abstract — This paper aims to improve data security and BER performance in the Power Line Communication channel by using encryption and channel coding techniques. In particular, improvement in BER performance has been obtained while using OSTBC rather than STBC as compared to the results obtained in a previous work. The improved system has been extended to include data security in the PLC channel. In this respect, a Hybrid SDES-AES encryption scheme has been developed. The BER performance of the Hybrid SDES-AES encryption in the PLC channel has been improved by using Convolutional coding, Interleaving and OSTBC. A performance improvement of 11.8 dB has been obtained at a BER of $3 \times 10^{-5}$ when compared with the Uncoded Hybrid Encryption case.

Keywords — Power Line Communication, OSTBC, Hybrid SDES-AES encryption, Interleaving, Convolutional coding.

I. INTRODUCTION

Power Line Communication (PLC) refers to the idea of transmitting data over the Power Line distribution system. This emerging technology has been around since the early 1920’s and consequently more and more attention and consideration is being given to the latter. PLC has evolved as one of the potential candidate for technology for the distribution of information data and for multimedia purposes in home or small office premises. Moreover, PLC has been evolving as a home network technology as it permits potential users to utilize their existing wiring system for inter-connecting their home appliances together and to the internet (Mannan et al., 2014).

The first practical challenge encountered in PLC is noise. According to Zimmermann and Dostert (2002), the noise in power grid is a combination of colored background noise, strong narrowband interference and random impulse noise. Iterative impulse suppression algorithms and interleaved coding are proposed to combat the impact of impulsive noise in PLC (Pighi et al., 2009). For the challenges mentioned above, we focus on the channel modeling of PLC for the following reasons as any research for PLC, especially, the research on deployment and communications theory approaches deeply depend on the channel model. But, there is still not a widely accepted convenient channel model for PLC. Second, it is necessary to find new technologies in order to improve the security performance of the PLC channels, thus making it a competitive candidate among the other communications solutions.

The interest and demand for Broadband and multimedia services have expanded significantly in the last decades. As such, this has opened the door for the development of a range of technologies designed for Broadband access. The data needs to be protected and secured especially in a communication network prone to attacks.

PLC can be considered as a multipath environment, but there are also the fading effects involved. The Rayleigh fading model can also be used to model the multipath and fading effects in PLC channel (Mathur et al., 2014). The experiments conducted have shown that the measured parameters of the transfer function follow the Rayleigh distribution. The Doppler shift is an important factor for the Rayleigh fading channel which is due to movement of objects. However, for the PLC channel, there is no Rayleigh fading due to Doppler effect as there is no Doppler shift because the latter is a wired communication channel but the multipath propagation causes the fading effect to be valid.

In fact, many researchers have been designing and modeling PLC systems but few have been investigating the effect of encryption in the PLC channel. Recent investigators (Kuo and Hsu, 2012) have developed a low cost design of PLC with Tiny Encryption Algorithm (TEA). PLC is sought to be one of the potential candidates for Broadband internet in the near future and as such, data transmission over the PLC channel needs to be secured.

In this research work, the BER performance of Orthogonal Space Time Block Coding (OSTBC) together with Convolutional coding, Interleaving techniques has been compared to a similar work done while using STBC (Papaioannou et al., 2004). This work has also been extended to improve data security on the PLC channel by using Hybrid SDES-AES encryption algorithm.

The outline of this paper is as follows: in section II, the system structure and simulation parameters are presented. The simulation results and discussions are given in section III while section IV provides the conclusion to the presented work.

II. SYSTEM STRUCTURE AND SIMULATION PARAMETERS

The block diagram of the Hybrid-OSTBC Convolutional system is shown in Fig. 1.
The following sections provide the implementation techniques and details of the proposed system and also some programming details. Table 1 gives the information on the operating system (OS) and processor used for the simulations. The simulations were performed in Matlab R2014a for a range of Eb/N0 values and after obtaining their corresponding BER values, the graphs for the BER plots were plotted. The simulations were carried out for about 1056000 data bits in order to compute the BER and to evaluate the performance of the systems implemented. Multiple simulations were carried out in order to minimize the errors so that the results could be validated.

A. Hybrid SDES-AES scheme

In the proposed algorithm, Hybrid SDES-AES, a combination of SDES and AES algorithms has been done. Professor Edward Schaefer of Santa Clara University was the founder of the Simplified DES algorithm. The properties of the latter are identical to the DES algorithm but it operates on a smaller block size and key size. The block size consists of 8 bits while the key size consists of 10 bits. It was developed for educational purpose as it is easier to understand than the DES algorithm, hence it can be considered as an unsecure encryption algorithm (Kumar, 2008). Moreover, AES algorithm also known as Rijndael algorithm was developed by Joan Daemer and Vincent Rijmen in October 2000 as United States Advanced encryption algorithm. AES is a symmetric encryption algorithm in which only one key is utilized by both the sender and receiver for encryption and decryption (Reddy and Kumar, 2016). Figure 2 shows the Hybrid SDES-AES algorithm flow diagram.

For encryption of data:

i. The input plaintext is converted to blocks of 8-bit.

ii. Then, the 8-bit blocks of the plaintext are passed through the SDES encryption algorithm first.

iii. Next, the encrypted data output from the SDES encryption is combined into 128-bit blocks and the latter are fed as input to the AES encryption algorithm.

For decryption of data:

i. The 128-bit block of encrypted data is applied to AES decryption algorithm first, which provides a decrypted set of 128-bit blocks of data.

ii. These 128-bit blocks data sets are broken into 8-bit blocks of data and then applied to the SDES decryption algorithm to decrypt the ciphertext and convert the latter back to the original size of the input plaintext.

B. Implementation of Interleaver and Deinterleaver

It is proposed to use the Interleaving and Deinterleaving process so as to reduce the burst effect and hence improving the BER performance of the communication system. The state for random number generator is set to 5200. The randintrlv function is a Matlab function that uses the parameter state to perform the random permutation. This form of Interleaver i.e. Random Interleaver is a form of Block Interleaver which is chosen for ease of implementation. The randdeintrlv function is used for the Deinterleaving process. The latter restores the data elements in their original state by performing an inversion of the random permutation. The state for the random number generator is kept the same in order to leave the data bits unchanged.

C. Implementation of Convolutional Encoder

A (3,1,4) Convolutional Encoder of rate 1/3 is implemented in this research work. Table 2 shows Convolutional codes of rate 1/3 with different constraint lengths and minimum distance. The constraint length K=4 is chosen and implemented. For K=4, the impulse responses are 54s, 64s and 74s which are represented in octal form.

The Viterbi decoding scheme is used for the decoding process.
D. Implementation of OSTBC Encoder and Decoder
Since the Powerline network is a 3-phase network, the application of STBC can take advantage of the Spatial Diversity (SD) (Paparizou et al., 2005). The scheme used in this research work is referred to as OSTBC 3X3, where 3 emitting points and 3 receiving points are used. The number of transmitting antennas is set to 3. Then, an Orthogonal Space Time Block Code (OSTBC) encoder System object is created by using the function comm.OSTBCEncoder which provides a block-wise mapping of the input bits and also the output codeword matrices are concatenated in the time domain. Another important property of the OSTBC Encoder object is the Symbol Rate which by default is set to ¾ by Matlab when the number of transmitting antennas is greater than 2. Before constructing the OSTBC Combiner object, the number of transmitting and receiving antennas is set to 3. The latter filter is applied to it. The number of transmitting antennas and the number of receiving antennas denoted by numTx and numRx, respectively, are defined. They are set to a value based upon the OSTBC 3X3 that will be used alongside it. Secondly, the sampling rate which is de-noted by Rs is set to 100MHz. Then the path delay values and average path gains are inserted. The path gains values are evaluated so that it can be used by the OSTBC combiner for channel estimation. The fading distribution property is set to Rayleigh. Also, the Doppler shift property is not defined because for a wired communication channel such as the PLC channel is not affected by the Doppler effect.

E. Implementation of the BPSK Modulation and Demodulation schemes
In the proposed system, BPSK modulation has been chosen because of its low complexity and ease of implementation. An NRZ-L signal is multiplied by the carrier signal so as to form BPSK modulated signal. Parameters for the matched transmitter and receiver filters are given in Table 3. A correlation receiver is used to demodulate the received noisy signal.

F. Evaluation of Multipath parameters and implementation of the MIMO PLC Channel
To combat multipath effects that exist in Power Line Communication channels, the PLC channel can be modelled by the Rayleigh fading model. The Eqs. (10) to (14) (Rajkumarsingh and Poonye, 2014) were used for the evaluation of the Multipath parameters. Table 4 shows the results obtained for the electrical parameters of the cables NAYY35 and NAYY150 (Duche and Gogate, 2014).

Table 5 shows the results obtained when the multipath parameters were evaluated. The path delays are in the order of μs.

In order to implement the MIMO PLC channel, the comm.MIMOChannel system, object that is available in Matlab, is used. The latter filters the input signal that is applied to it. The number of transmitting antennas and the number of receiving antennas denoted by numTx and numRx, respectively, are defined. They are set to a value based upon the OSTBC 3X3 that will be used alongside it. Secondly, the sampling rate which is de-noted by Rs is set to 100MHz. Then the path delay values and average path gains are inserted. The path gains values are evaluated so that it can be used by the OSTBC combiner for channel estimation. The fading distribution property is set to Rayleigh. Also, the Doppler shift property is not defined because for a wired communication channel such as the PLC channel is not affected by the Doppler effect.

G. Implementation of Narrowband noise
A sum of modulated sinusoidal signals can be used to model the Narrowband noise and which is given by

\[ N_{\text{narrowband}}(t) = \sum_{i=1}^{N} A_i(t) \sin(2\pi f_i t + \varphi_i) \]  

where \( N \) is the total number of carriers, \( A_i \) is the amplitude of the \( i^{th} \) disturber, \( f_i \) is the central frequency of the \( i^{th} \) disturber, \( \varphi_i \) is the phase of the narrowband noise received at the receiver side. In fact, the phase can be randomly selected in the interval \([0, 2\pi]\) (Çelebi, 2010). The parameters illustrated in Table 6 are used to model the Narrowband disturbance.

The amplitude \( A_i \) is assumed to be changing with varying values of SNR and is given by

\[ A_i = \frac{0.5}{\sqrt{\frac{SNR}{R}}} \]  

Since, \( P = \frac{A_i^2}{R} \) where \( R \) is assumed to be 1Ω and taking the signal power to be 0.5W, the equation for the amplitude \( A_i \) is obtained as shown in Eq. 2.

H. Implementation of Impulsive noise
Middleton’s Class-A Impulsive noise model is used to implement the Impulsive noise (Bert et al., 2011; Andrei et al., 2015). The inputs for the Class A Middleton model are: \( A, \ Gamma, M \) and \( N. A \) is the impulsive index, \( Gamma \) is the average power ratio of the Gaussian to Impulsive noise components, \( M \) is the number of terms that
should be defined for the noise samples and \( N \) is the number of samples that needs to be evaluated. A value of 0.1 for \( A \) is considered to be very impulsive. High frequencies do not affect the background noise, hence the value for \( \Gamma \) is chosen to be 0.01 and \( M \) is chosen to be 3. In the sample code, approximately 20 noise elements are generated so as to obtain a better estimation of the Impulsive noise components.

### III. SIMULATION RESULTS

In this section, the effect of channel coding techniques without encryption is first investigated and compared with a previous research work. Secondly, the BER performance of Convolutional coding on the Hybrid SDES-AES encryption is investigated and finally the effect of OSTBC, Convolutional coding and Interleaving on the Hybrid SDES-AES encryption is investigated.

#### A. BER performance comparison of Implemented OSTBC, Convolutional coding and Interleaving without encryption with previous research work

Figure 3 shows the BER performance comparison of the implemented system with the previous research work (Papaioannou et al., 2004). The research work conducted in the latter evaluated the performance of STBC, Interleaving together with Convolutional coding and BPSK modulation in the PLC channel and wireless channel.

The results taken from the previous research work are only for the PLC channel so that a comparison can be easily made with the implemented system without encryption. The previous work uses a STBC consisting of 3 emitting and receiving points, referred to as STBC 3X3. Table 7 shows the performance comparison of the implemented system and the previous work.

It can be observed that there is a marginal improvement of 11.7 dB for the case of OSTBC. This discrepancy is due to the OSTBC used in the implemented system compared to STBC which is used in the previous work. The OSTBC coding technique is an enhanced version of STBC which uses orthogonality to encode and decode the bits alongside channel estimation. In fact, this comparison was made so as to validate the results obtained.

#### B. Effect of Convolutional coding on BER performance of Hybrid Encryption in PLC channel

Figure 4 shows the BER performance of the Uncoded and Convolutional coded Encryption which includes SDES, AES and Hybrid SDES-AES encryption techniques.

From Fig. 4, it can be observed that the BER plot of the Uncoded SDES provides better performance when compared to AES and Hybrid SDES-AES. The main reason for this discrepancy is that the SDES has a low complexity and it is easily implemented. Despite having a good BER performance, the SDES encryption is easily prone to attacks and therefore it does not provide a good security. On the other hand, the AES and Hybrid SDES-AES provide better performance in terms of security levels. AES being a powerful encryption technique is difficult to crack and also it is more complex than SDES and the time taken to perform encryption is much more than that of the SDES. Hence, when the AES is merged with the SDES to form the Hybrid SDES-AES encryption, the security level is increased which is good for transmission of data. Also, it can be observed that the error performance of the Convolutional coded version of encryption is much better than the Uncoded version.

It is interesting to observe that the BER plot of the Convolutional coded Hybrid encryption in PLC channel has a marginal improvement of 7.1 dB in comparison to the Uncoded version at a BER of \( 1 \times 10^{-4} \). The application of the Convolutional coding significantly improves the performance of the Hybrid SDES-AES Encryption technique. This improvement is to be expected because the Convolutional coding is a forward error correction code. Hence, it is clear that the Convolutional coded Hybrid encryption system performs better that the Uncoded one.
Table 7: BER performance comparison of Implemented system and previous system.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Previous system</th>
<th>Implemeated system</th>
</tr>
</thead>
<tbody>
<tr>
<td>STBC</td>
<td>20</td>
<td>8.3</td>
</tr>
<tr>
<td>STBC + CONVOLUTIONAL</td>
<td>3.3</td>
<td>3.1</td>
</tr>
<tr>
<td>STBC + CONVOLUTIONAL + INTER</td>
<td>3.1</td>
<td>2.8</td>
</tr>
</tbody>
</table>

Table 8: Critical Analysis of obtained results

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Eb/N0(dB) values required to obtain a BER of $2 \times 10^{-5}$</th>
<th>Coding gain (dB) in comparison to Uncoded Hybrid Encryption</th>
<th>Total Number of bits transmitted</th>
<th>Time taken [s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncoded Hybrid Encryption</td>
<td>20.4</td>
<td>0</td>
<td>1056000</td>
<td>1359.53</td>
</tr>
<tr>
<td>OSTBC + Hybrid Encryption + INTER without Convolutional Coding</td>
<td>12.6</td>
<td>7.8</td>
<td>1057280</td>
<td>1607.27</td>
</tr>
<tr>
<td>Convolutional Coded Hybrid Encryption</td>
<td>12.6</td>
<td>7.8</td>
<td>1056000</td>
<td>3145.38</td>
</tr>
<tr>
<td>OSTBC + Hybrid Encryption + Convolutional Coding + INTER</td>
<td>8.6</td>
<td>11.8</td>
<td>1057280</td>
<td>3810.33</td>
</tr>
</tbody>
</table>

Figure 5. BER performance comparison of OSTBC, Convolutional coding and interleaving with Hybrid Encryption.

C. Effect of OSTBC, Convolutional coding and Interleaving on BER performance of Hybrid Encryption

Figure 5 shows the BER performance comparison plots of the implemented systems. From Fig. 5, it can be seen that the OSTBC + HYBRID + CONVOLUTIONAL + INTER system has a much better BER performance compared to the other implemented systems. It is clear that the application of OSTBC, Convolutional coding and Interleaving to the Hybrid Encryption outperforms the other implemented systems.

A gain of 4 dB at a BER of $3 \times 10^{-5}$ is obtained when the HYBRID + CONVOLUTIONAL and OSTBC + HYBRID + INTER systems are compared with the OSTBC + HYBRID + INTER + CONVOLUTIONAL system. It is worth noting the performance improvement that the OSTBC, Convolutional coding and Interleaving with Hybrid Encryption system has over the other implemented systems. There is a marginal improvement of 11.8 dB in the latter which is much greater than the other implemented systems.

D. Critical Analysis of results obtained

Table 8 shows the time taken for the different scenarios implemented. The time taken for the Uncoded Hybrid Encryption is less but it takes 20.4 dB to achieve a BER of $3 \times 10^{-5}$. The use of OSTBC, Convolutional coding and Interleaving has been observed to give a lower BER and has been found to be more robust. However, the implementation is relatively more complex and as such the simulation time required is long enough as shown in Table 8. We can see that despite the relative complexity of the OSTBC, Convolutional coding and Interleaving with Hybrid Encryption, the latter has a major performance improvement compared to the other implemented systems. It takes only 8.6 dB to achieve a BER of $3 \times 10^{-5}$ and an improvement of 11.8 dB is obtained as compared to the Uncoded Hybrid Encryption case. This is due to the Interleaving technique because the latter can combat the burst error effects that exist in the PLC channel. Hence, the application of OSTBC, Convolutional coding and Interleaving to the Hybrid Encryption has proved to be very efficient as they provide a significant improvement in performance and also they provide a great security level for communication in PLC channel. Overall, we can deduce that this system performs better and can combat the burst error effect in the PLC channel as well as improving the data security in this type of channel.

IV. CONCLUSION

It is found that the use of OSTBC, Convolutional coding and Interleaving provide a major improvement in the BER performance of the implemented system as compared to previous work. It was also observed that when the Hybrid SDES-AES encryption technique was used, there was an improvement of 11.8 dB at a BER of $3 \times 10^{-5}$ for the OSTBC, Convolutional coding and Interleaving with Hybrid Encryption system when compared with the Uncoded Hybrid Encryption case. This improvement in BER performance was in fact greater than the other scenarios considered. As such this demonstrates the capability that the OSTBC technique brings to the system due to the diversity gain and orthogonality. On a conclusive note, from the simulation results obtained, it is clear that the application of OSTBC, Convolutional coding and Interleaving with Hybrid Encryption in PLC has proved to offer the best performance results but there is a trade-off between data security and BER performance.
REFERENCES


Received: August 1, 2017.
Sent to Subject Editor: February 1, 2018.
Accepted: March 19, 2019.
Recommended by Subject Editor: José Guivant.