Combination of Cryptography and Channel Coding for Wireless Communications

Dr. Mahmood Farhan Mosleh*
Assist. Prof. / Electrical and Electronic Technical College

Dalal A. Hammood
Lecturer /Electrical and Electronic Technical College

Dr. Ahmed Gh. Wadday
Lecturer/Al-Furat Al-Awsat Technical University

Abstract

Huge investigations have been made by the research communities in wireless systems, especially in the past decades. There are a lot of applications over wireless communications networks that have appeared in the recent time, including cellular phones, video conferencing, MMS, SMS, web browsingetc. Communications through wireless channels are exposed to errors in transmission. Moreover, efforts are being made to secure wireless communications through the use of modern encryption technologies. In this paper a combination of cryptography and simple channel codes are presented to make security and forward error correction. The system has been tested to transmit and receive a text with and without encoding for Additive White Gaussian Noise (AWGN). The results showed that it can receive the text with no error at 6 dB of Signal to Noise Ratio (SNR) without using channel coding and 1 dB with it. In addition the systems is experimented in urban wireless system, and has shown that it needs 9 dB to receive the text with acceptable error. All tests are done using Matlab version R2014a.

Keywords :Cryptography, channel code, Security .

التشفير المركب لنظام اتصالات لاسلكية

أ.م.د. **محمود فرحان مصلح** / كلية التقنيات الكهربائية والالكترونية
م. **دلال عبد المحسن حمود** / كلية التقنيات الكهربائية والالكترونية
م.د. **احمد غانم وادي** / هيئة التعليم التقني

الستخلص:
في العقد الاخير اهتم الكثير من الباحثين والمحققين بانظمة الاتصالات اللاسلكية. وظهرت العديد من التطبيقات الشهيرة كالتلفون الخلوي والرسائل وشبكات تبادل الفيد يو وغيرها. الاتصالات اللاسلكية تكون عادة عرضة للخطأ، كما ان السرية باستخدام المشفر هو من الخدمات المضافة. في هذا البحث تم تقديم نظام يخلط بين التشفير لاغراض السرية والتشفير لاغراض معالجة الخطأ. تم استخدام النظام المقترح بارسال نص عبر قناة الضوضاء البيضاء AWGN. النتائج بينت انه يمكن استلام النص بدون خطأ عند 6dB من نسبة الاشارة الى الضوضاء SNR بدون مشفر قناة و 1dB باستخدام هذا المشفر. كذلك تحت تجربة النظام لظروف التراسل اللاسلكي داخل المدينة وتبين انه يحتاج الى 9dB لاستلام النص بنسبة خطا مقبولة. و تم اجراء عمليات الفحص المذكورة اعلاه باستخدام برنامج ماتلاب الاصدار R2014a.

1-Introduction:

In the last decade, a lot of applications over the wireless have appeared, and many of them are under development. Among the most prominent end-user applications that are received on the popularity of a simple messaging, cellular phones, multimedia messaging, internet access, web browsing, file transfer, streaming audio, video and visual conferencing is the tip of the iceberg. There are large variations in the wireless systems applications (the previous applications). Therefore, the error tolerance of these applications varies depending on the application, for example, there is more tolerance for errors in voice communications compared to the file transfer applications [1]. In addition to that, data were sent through

wireless communication channels were exposed to issues of data security. Therefore, to overcome these difficulties, cryptography is adopted to secure the data transfer, must be protected against manipulations of transmitted data or eavesdropping, or disclaimer of data origin. It is worth mentioning that the topics of data security and error corrections, are still dealt with separately [2]. Redundant information is applied in channel coding for detectioning or correcting errors when data are transmitted through noisy channel. Cryptography is applied to provide secure transfer of information from manipulation, or eavesdropping or masquerading of data origin [3].

References [4] and [5] show the cooperation between cryptography and channel coding: improvement of decryption outcomes by using channel decoding,or vice versa, the improvement of channel decoding by using cryptography. The "Joint Channel Coding and Cryptograph" for this concept was launched. The channel code and cryptographic techniques are considered as inner and outer codes respectively [3].

Over a noisy channel a cryptographic check value for the message is transmitted through channel coding mechanics (coding/decoding). The process of decryption for the check cryptographic value is very sensitive, because when one or more bits of the decryption input are wrong, about fifty percent of the decrypted bits are false, which leads to verification failure in value of the cryptographic check. Therefore, every bit in the message and the check value of the cryptographic must be correct at the decryption input. A correction method called soft decoding input is applied to solve this problem [4].

Authors in [6] used Low Density Parity Check (LDPC) channel codes for security. They proved that the combination of signaling and coding for secrecy is more effective than either one alone and is key to providing information-theoretic security in more practical systems.

In this paper attempt has been made to design a wireless system including security to hide, the original information data ultimately through the decryption process to the message contents in the original information. In addition a simple channel code is added to the system to ensure the message is received without error.

2- Cryptography:

Cryptography is used to keep secret certain information which has always existed, and tries to preserve secrets [7]. When the data are processed through some substitute techniques, table references, shifting techniques or mathematical operations encryption will occur. These processes produce a various form of that data. The unencrypted data denote to the plaintext and the encrypted data to the ciphertext, that represents the original information in a difference form [8]. This paper will focus on caser cipher, this type of cipher doesn’t depend on key, it depends on shift (+) or (-) for the letters (A.. Z). For instant to encrypt the letter "a", ascii code of "a" is 97, so 97 +3 is the asci of the ciphered letter, and so.

2-1- Encryption:

Information secrecy can be achieved by encryption means. A modern technique of the encryption is a mathematical conversion (algorithms) which deal with messages as algebraic elements or numbers in a space and convert them between a region of "meaningful messages" and a region of "unintelligible messages". Cleartext refers to the messages in the significant region while ciphertext refers to the ambiguous output from the encryption algorithm**.** Secrecy is at the heart of cryptography. Fig.1 shows the encryption process [7, 9, 10].

The encryption can be achieved by using arithmetic modular, first the letters are transformed into numbers, according to, A = 0, B = 1,……. Z = 25. Equation (1) shows mathematical description for encryption letter *x* by a shift *n* [9, 11, 12]

$$E_n(x) = (x + n) \quad mod\ 26 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

In this paper a simple method has been used to encrypt or decrypt text which is Caser Cipher. The method depends on shift letter which is shift (+3) for encryption or shift (-3) for decryption. This type of cipher doesn't depend on a key or symmetric key. It depends on shift of a certain number

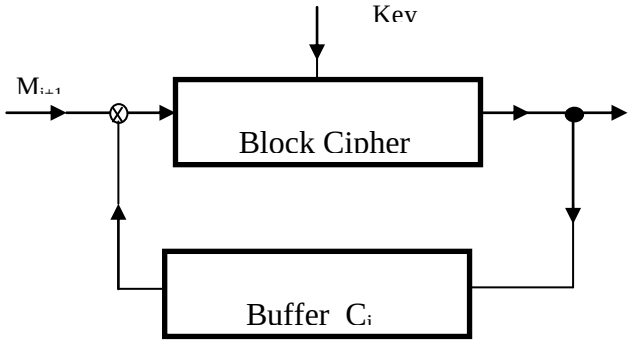

Figure 1: Block diagram of encryption process

2-2- Decryption:

The process of decryption is the opposite of the encryption process. The buffer must be initialized with the same initial value that was used to start encryption. The pracss couldb fixed constant or part of the secret key.

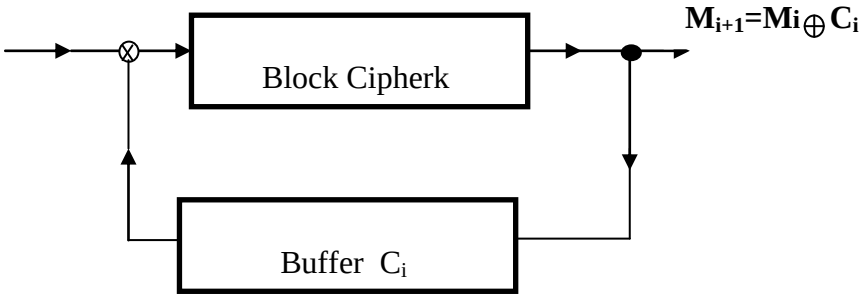

Figure 2: Block diagram of Cipher Chaining Decryption

Similarly, decryption is performed,

$$D_n(x) = (x - n) \quad mod\ 26 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

The modular operation has different definitions. In the above equation, there has been need to subtract or add 26 when the result is in the range 0...25. i.e., if $x+n$ or $x-n$ is not in the range 0...25, [9,11,12].

3- Channel Coding:

Many recent researches in coding have been in the region of joint source and channel coding as well as widely distributed source coding and data compression using methods that are more conventionally associated with channel coding [13]. The most important channel codes and widely used in modern communication systems is Convolutional Codes (CC). Due to the fact that CC has regular trellis structures , it is used for increasing the transmission reliability and hence Viterbi algorithm can be used for the decoding [14].

A binary convolutional encoder of rate k/n $(k < n)$ generates an n-bits word for every k-bits word at the input. A three-tuple (n, k, m) is denoted a binary CC, where n corresponds to encoder output bits which are generated, k are received input bits, and for which the n current outputs are linear combinations of the present k input bits and the previous $m \times k$ input bits Fig. 3 shows the encoder for the binary $(2, 1, 2)$ CC with generators $g_1 = 7$ and $g_2 = 5$ (numbers in octal), where g_i represents the i^{th} output of the generator polynomial characterizing. [15].

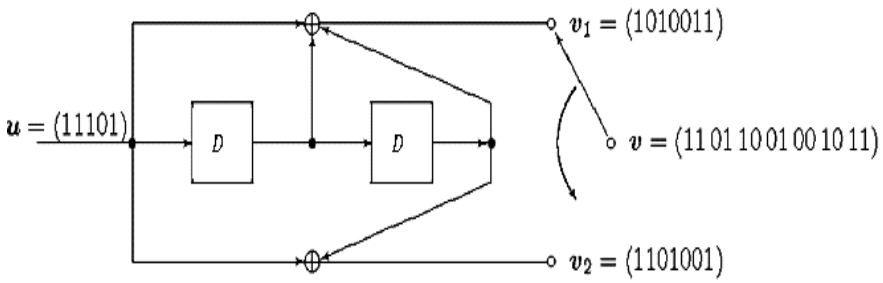

Figure 3 Convolutional encoder

The input of the sequence *u* to the convolutional encoder with a rate of *k/n* of *k* tuples [13]:

$$u_t = \left(u_t^1, \dots\dots\dots\dots, u_t^k\right) \dots\dots\dots\dots \dots\dots\dots\dots (3)$$

The *n*- tuples output from such encoder is a sequence *v*:

$$v_t = (v_t^1, \dots\dots\dots\dots, v_t^n) \dots\dots\dots\dots \dots\dots\dots\dots (4)$$

From the coding theory, it is possible to use the *D* element as an operator to represent the above input and output as:

$$u(D) = (u_0 + Du_1 + D^2u_2 + \cdots) \dots\dots\dots\dots (5)$$

and

$$v(D) = (v_0 + Dv_1 + D^2v_2 + \ \dots.) \dots\dots\dots\dots\dots\dots (6)$$

Another representation of composite form for convolutional encoder the sequences of input and output is as follows:

$$u = \left(u_0^1,\ u_0^2, \dots., u_0^k;\ u_1^1, u_1^2, \dots, u_1^k;\ u_2^1, u_2^2, \dots., u_2^k, \dots.\right) \dots\dots (7)$$

$$v = (v_0^1,\ v_0^2, \dots., v_0^n;\ v_1^1, v_1^2, \dots, v_1^n;\ v_2^1, v_2^2, \dots., v_2^n, \dots.) \dots \dots (8)$$

The code word in a convolutional code is generated by simple multiplication of the

sequence of input message with a vector or matrix called generator matrix as follow:

$$v(D) = u(D)G(D) \ldots\ldots\ldots\ldots\ldots (9)$$

The generator matrix *G(D)* in a form of polynomial with a size of $k \times n$ is represented by

[16]:

$$G(D) = \begin{bmatrix} g_1^{(1)}(D) & g_1^{(2)}(D) & \ldots & g_1^{(n)}(D) \\ g_2^{(1)}(D) & g_2^{(2)}(D) & \ldots & g_2^{(n)}(D) \\ \vdots & \vdots & & \vdots \\ g_k^{(1)}(D) & g_k^{(2)}(D) & \ldots & g_k^{(n)}(D) \end{bmatrix} \ldots\ldots (10)$$

The Viterbi decoding is an optimal algorithm for decoding of CC. It consists of three major Parts:

Branch metric calculation for hard decision and soft decision decoders.

Path metrics calculation using a procedure called ACS (Add-Compare-Select).This procedure is repeated for every encoder state.

Trackback the decisions made by path metric due to maximum-likelihood which restores in Back-trace unit. Since it does it in opposite direction, a Viterbi decoder contains a FILO (first-in-last-out) buffer to rebuild a correct order.

4- System model:

The system used in this paper is shown in Fig. 4.

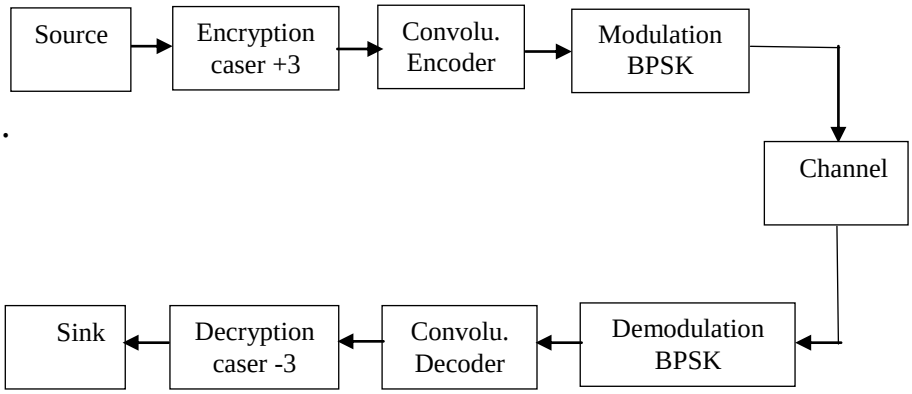

Figure 4: System model

The source is the data to be communicated, such as a text file, voice, or video. In this paper attempt has been made to transmit text file without any error in a media of wired and wireless environments. The encryption hides or scrambles information so that unitended listeners are unable to discern the information content. A redundant data is added to the inputs symbols in the channel codes in a way that allows errors which are conducted into the channel to be corrected. Convolutional codes are used in this paper because they are very simple to encode and decode and powerful to correct errors in various environments. The constraint length of convolutional encoder is 7 and the generator polynomials are [171, 133], which are practical parameters. The code rate used is ½, this means that half data is carrying information and the rest data is used to detect and correct error. Redundant data

can be compensated using high level constellation of the modulator which collect two bits or more in one symbol.

The modulator converts symbol sequences from the channel encoders into signals appropriate for transmission over the channel which requires the signals be sent as a continuous-time voltage or an electromagnetic waveform. In this research the above two forms have been used for compression. Phase Shift Keying (PSK) with Binary PSK (BPSK) and Quadrature PSK (QPSK) with gray code are used as modulation schemes in this paper.

The channel is the media over which the information is conveyed. It may be wired or wireless. As signal pass through a channel they are corrupted. For example, noise may be added to signal, timing jitter, it may experience time delay, suffer from attenuation and interference with other signals. The channels are frequently characterized by mathematical models. In this paper Additive White Gaussian Noise (AWGN) and Rayleigh fading channels are used. At the received end, all processors are mirrored to its counterpart in the transmitter side.

5- Simulation and results:

All simulations are done using MATLAB version R2014a and the results are obtained and cleared out as tables and graphs. The simulations have been done in the form of four steps:

5-1- Encryption and Decryption:

The first step is to evaluate the encrypter to make sure that this block can encrypt successfully which means that any one cannot read the encrypted text. The following text is used for first experiment: "*MY BABY HAS BEEN MISSING FOR OVER A MONTH NOW, AND I WANT HIM BACK SO BADLY*". Each letter will be converted into American Standard Code for Information Interchange (ASCII), so that the above text becomes as the fallowing numbers:

"77 121 32 98 97 98 121 32 104 97 115 32 98
101 101 32 103 110 105 115 115 105 109 32 110
109 32 97 32 114 101 118 111 32 114 111 102
110 97 32 44 119 111 110 32 104 116 110 111
109 105 104 32 116 110 97 119 32 73 32 100
97 98 32 32 111 115 32 107 99 97 98 32
121 108 100"

Then apply caser algorithm or shift each of the above number by +3.

Then converting those numbers to mod (26) to obtain (A - Z) or (0 – 25) as shown:

"8 20 23 22 23 20 3 22 14 23 0 0 9 8
4 14 14 4 9 2 1 10 13 10 17 0 13 22
8 10 9 15 3 9 10 18 22 9 25 4 18 22
9 15 3 4 8 23 22 24 6 14 10 23 22 25
7 20".

Then each number is converted to binary form to be accepted in the channel coding block.

5-2 Transceiver System:

The second step is to use such encryption with transceiver system with AWGN channel to transmit any encrypted text and received it without error and then decrypt it to retrieve such text as in original manner. The system is now without code so expect to get an error during transmission at low Signal to Noise Ratio (SNR). For SNR=1dB and BPSK and for the same text used in the first step, the received text in this step is *"MyB**S**B**i**HASB**K**NMISSI**GJP**ROVERA**N**ONThNOWA**>**DIWaN **SF**I**=**B**=**K**[C**OBADLy"*. As is clear the received text contains 17 letters in error form so we cannot read the text correctly. The bits in error are 26 and Bit Error Rate (BER) is 0.0489. The minimum value of SNR, which can obtain the text with no error is 6dB. Table 1 is summarizes the results for each value of SNR from 1, to 6 dB:

Table 1: Summary Results of 5-2 subsection

SNR (dB)	No. Letters in error	Bits in error	BER
1	17	20	0.0493
2	12	13	0.032
3	7	5	0.0123
4	2	3	0.0074
5	1	2	0.0049
6	0	0	0

From the results in table 1 it has been shown that the error decreases dramatically and the BER must be less than

0.0049 to achieve the text without any error. But it is clear that up to 4 dB of SNR we have only two letters in error which indicate that the system active above such value of SNR, but the channel used here is AWGN which is an ideal state.

5-3 Transceiver System with Channel Codes:

Now repeating the last subsection with the same parameters and text, by adding CC to the system to show the effect of the presenceof channel codes within the system. For 1dB SNR the received text is "**g**ybabyhasbeenmissingforoveramonthnowand**c**wanthimbacks obadly". As it is clear only two letters are in error, while it needs 4dB to get the same amount of error for the system without code as shown in table 1, which indicate that channel code makes the system active in low SNR. To increase the spectral efficiency the constellation has been increased up to 4 or two bits per symbol to reduce the bandwidth by 50%. When SNR is 3dB the results show that the error is the same as the system without code but the SNR is 4dB, which means that 1dB gain is achieved by adding CC with the same bandwidth. Another comparison can be done using the plotting of Bit Error Rate (BER) versus SNR to show the potential of such system. Fig. 3 shows 3 curves, at BER of 10^{-4} and for Binary Shift Keying (BSK) Modulation (M=2), 6 dB code gain can be achieved. But here the spectrum must be doubled because the code rate used is ½, from other hand, when M=4 the system can achieve 2dB gain as illustrated in Fig.5, which shows that the system can provide good performance.

5-4 Wireless Transceiver:

In subsections 5-2 and 5-3 the channel used is AWGN. Here the system will be used Rayleigh channel model used to

simulate wireless communication with no line of sight (urban environments) with parameters: Input Sample Period: 1.0000e-05, Doppler Spectrum: [1x1 doppler. jakes], Max Doppler Shift: 0, Path Delays: 0, Path Gains: 0.0553 + 0.0908i. Here it is impossible to transmit any information without channel codes, but such system with CC can receive the transmitted information at specific SNR.

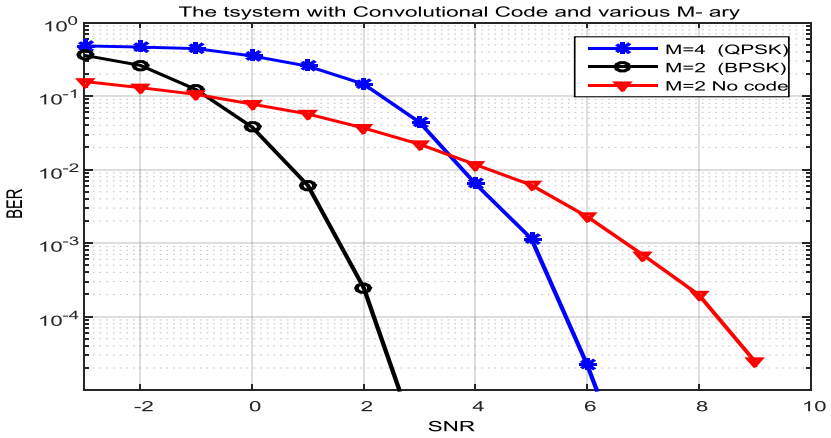

Figure 5: BER comparison of the system

For the previous system but with Rayleigh channel the fallowing text is received without any error at SNR=9 dB: "Mybabyhasbeenmissingforoveramonthnowandiwanthimbacksobadly"
But when reducing the SNR to 8dB, many error show in the text as shown:
"mzerfyhasbeenmissimfpwfmwdxawbphvnowakdhaynthimbacugmeuiur". Because the amount of error now out of code capability. Note that for AWGN channel the error is reduces linearity as indicated in table 1.

6- Conclusions:

In this paper a system has been designed to combine Cryptography and Convolutional Codes. Such system can transmit and receive text messages through various types of channel. The system has been experimented with AWGN channel with and without code. It has also been tested with wireless Rayleigh fading model. The results confirm that the proposed system can transmit and receive any text with acceptable error for AWGN channel. 4 dB of SNR is enough to receive the text with only two error letters without codes, while only 1 dB is achieves the same results when adding channel code. On the other hand the system needs 9 dB of SNR for urban environments to receive the text without error but it is impossible to do this without channel code.

References:

[1] A. Goldsmith, "Wireless Communications," Cambridge University Press, 2005.

[2] N. ZIVIC, C. Ruland and O. U. Rehman, "Error Correction over Wireless Channels Using Symmetric Cryptography", 1st International Conference on Wireless Comm., Vehicular Tech., Information Theory and Aerospace & Electronics Systems Technology, 2009.

[3] N. Ziviü and C. Ruland, "Parallel Joint Channel Coding and Cryptography", Int. Journal of Electrical and Electronics Engineering 2010.

[4] N. Ziviü and C. Ruland, "Soft Input Decryption", 4uı Turbo code Conf., IEEE, in Plastics, Munich, April 2006.

[5] N. Ziviü and C. Ruland, "Feedback in Joint Coding and Cryptography", 7th Int. ITG Conf. on Source and Channel Coding, IEEE, January 2008.

[6] W. K. Harrison, J. Almeida, M. R. bloch, S. W. McLaughlin, and J. barros, "Coding for Security",

IEEE Signal Processing Magazine, September 2013.
[7] W. Mao , "Modern Cryptography: Theory and Practice" , Prentice Hall PTR, New Jersy, July 2004.
[8] J. Freeman, R. Neely, and L. Megalo "Developing Secure Systems: Issues and Solutions". IEEE Journal of Computer and Comm., Vol. 89, 1998, PP. 36-45.
[9] C.A. Henk, van Tilborg, "Fundamentals Of Cryptology A Professional Reference And Interactive Tutorial", Kluwer Academic Publishers, London, 2002.
[10] D.R. Stinson, "Cryptography Theory and Practice", 3rd Edition, Chapman and Hall/CRC, 2006
[11] Goldreich, Oded, "Foundations of Cryptography Basic Applications", Cambridge university press,Vo. 2, 2004.
[12] W. Stallings, "Cryptography and Network Security, Principle and Practices," 3rd Edition, Pearson Education, 2005.
[13] P. Mitran, "The Asymptotic Uniformity of the Output of Convolutional Codes Under Markov Inputs". IEEE Communications Letters, Vol. 13, No. 12, December 2009, Pp 944-946.
[14] H. H. Tang and M. C. Lin, "On (n; n 1) Convolutional Codes With Low Trellis Complexity", IEEE Trans. on Comm., Vol. 50, No. 1, January 2002
[15] S. Lin and D.J. Costello, "Error Control Coding", Pearson Prentice Hall, USA, 2004.
[16] S. Srinivasan, and S. S. Pietrobon, "Decoding of High Rate Convolutional Codes Using the Dual Trellis", IEEE Trans. on Information Theory, Vol. 56, No. 1, Jan. 2010.