An Integrated System using Joint Channel Coding and Cryptography Scheme for Error Correction over Wireless Channel

Rakesh Sonkar
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

Prof. Preeti Tuli
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

Prof. Somesh Dewangan
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

***Abstract*— Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path. Quite a few popular applications over the wireless communication networks get emerged just lately including, cellular telephony, SMS, MMS, world-wide-web browsing as well as video conferencing, to name a few. Data might be damaged during transmission. For reliable communication, error must be detected and corrected. Joint Channel Coding and Cryptography has been analyzed and simulated in this paper. The method is an extension of Soft Input Decryption with feedback, which is used for improvement of channel decoding of secured messages. we utilize the methods for data security as a tool for the detection and correction of transmission errors. Streaming applications are gaining popularity over not only the fixed Internet but also mobile hand-held devices. Growth in wireless access technologies along with the advanced coding schemes show the promise of better streaming service for the mobile users. However, wireless channels are characterized by fluctuating bandwidth, thereby making it challenging for streaming applications to ensure good quality of user experience (QoE). In this paper, we adopt an objective approach and propose a cross-layer adaptive streaming technique, where we make use of the channel loss information to update the application layer encoding at a slower rate and the link layer modulation and coding scheme at a faster rate. In our adaptive scheme, we focus on a pause-free playback by preventing buffer underflow at the receiver. Our simulation experiments show that, the proposed adaptive technique improves the QoE of the streaming significantly by gracefully degrading quality in the face of pathological cases such as wireless channel error, while ensuring an uninterrupted services.**

Keywords— Soft Input Decryption, L-Values, Joint Channel Coding and Cryptography, RSA, coding gain, block length.

I. INTRODUCTION

wireless networks includes Many applications are cellular telephony, simple messaging service, multimedia messaging service, Web browsing, Internet access, file transfer, streaming-audio-video and video conferencing, to name a few. Wireless transmission, however, due to its broadcast nature is inherently prone to errors. Most of the transmission errors result because of data collision, channel fading and the hideout phenomena.

For the two commonly used error control approaches, automatic retransmission request (ARQ) and forward error correction (FEC), FEC is thought to be more suitable for real time video transmission due to its small transmission delay and can improve the reliability of transmission through adding extra redundancy information to the compressed bit-stream. But the varying channel condition will affect its effectiveness. So, FEC should be designed in an adaptive way to combat the transmission errors occurred in the wireless channel.

Communication involving a wireless channel, cryptography is used to secure the information transfer: it protects against eavesdropping or manipulation of transmitted information, or masquerading of data origin.We propose a novel technique which combines the data security techniques i.e. the cryptographic algorithms, with the techniques for error correction. We use the "additional" data produced by Hash message authentication code(HMAC) as the redundant data for the detection and correction of errors at the receiver side. Thus in this work we make use of cryptographic check values as the redundancy data for error recovery at the receiver end. **Information Security** is simply the process of keeping information secure: protecting its availability, integrity, and privacy. "Information Systems Security" as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

The cooperation between channel coding and cryptography has been researched using channel decoding for the improvement of decryption results, using cryptography for the improvement of channel decoding. This concept is called Joint Channel Coding and Cryptography.

Soft Input Decryption (SID) rectifies bits at the input of descriptor: if the decoder is not able to reconstruct the pristine message and cryptographic check value because of a strepitous channel or inefficiency of the channel decoding algorithm, it is possible to rectify the message with the cryptographic check value utilizing side information of the channel decoder in form of called L-values. Channel decoding can be ameliorated utilizing a message with its cryptographic check value which has been redressed by Soft Input Decryption.

II. SOFT INPUT DECRYPTION

.
The rudimental conception for the amendment of the decrypting mechanisms uses soft output of the channel decoder. The main component is a decryptor which uses soft output of the channel decoder as soft input. The cryptographic mechanism which is utilized by encryptor and decryptor engenders and verifies cryptographic check values providing data integrity, data inception authentication and non repudiation. A decryptor which verifies digital signatures. Here, the decryptor uses redundant information to check if the signature is veridical. So, the decryptor is supplied by an amalgamation of the message and thesignature of the message.

The algorithm of Soft Input Decryption is presented in Fig.1 and functions as follows: The decryption is prosperous, if the verification of the cryptographic check value is positive, i.e. the output of the decryptor is "true". In case that the verification is negative, the soft output of the channel decoder is analyzed and the bits with the lowest |L|-values are flipped (XOR "1"). After, the decryptor performs the verification process and proves the result of the verification again. If the verification is again negative, bits with another cumulation of the lowest |L|- values are transmuted. This iterative process is culminated when the verification is prosperous or the needed resources are consumed. If endeavors for rectification fail, the number of errors is too large as a result of a very strepitous channel or an assailment, so that the resources are not sufficient to endeavor enough amalgamations of flipping bits of low |L|-values. It case that the endeavors for rectification of SID block prosper,but the redressed cryptographic value is not equipollent to the pristine one, it signifies that a collision transpires. This case has a profoundly low probability when cryptographic check values are culled under security aspects. Soft Input Decryption is block oriented. The block which is taken from sequential input bits to the channel encoder and should be redressed by Soft Input Decryption after channel decoding is called SID block (Soft Input Decryption block).

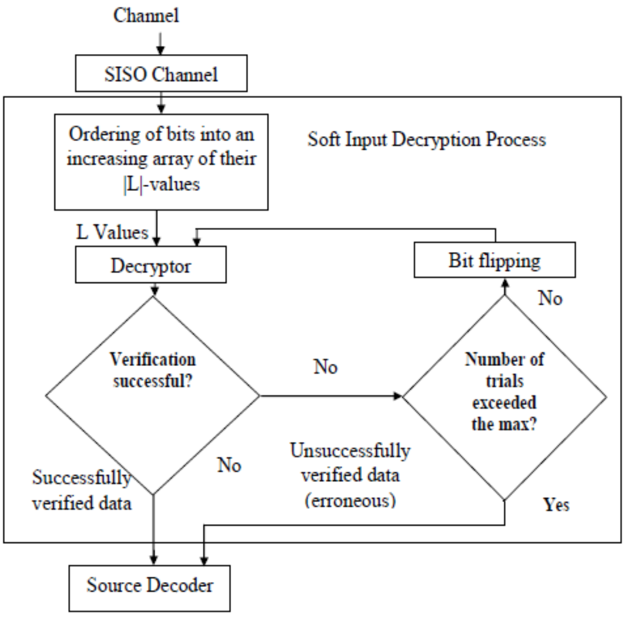
Channel
SISO Channel
Ordering of bits into an increasing array of their |L|-values
Soft Input Decryption Process
L Values
Decryptor
Bit flipping
No
Verification successful?
No
Number of trials exceeded the max?
Successfully verified data
No
Unsuccessfully verified data (erroneous)
Yes
Source Decoder

Figure 1. Algorithm of the Soft Input Decryption

III. JOINT CHANNEL CODING AND CRYPTOGRAPHY

A technique which combines cryptography and error correction together i.e. we use the methods for data security being a tool for the detection and correction connected with transmission errors. Simulation effects obtained that way which most of us call seeing that Joint Channel Coding and Cryptography. Joint Channel Coding and Cryptography is surely an extension connected with Soft Input Decryption having feedback, which can be used for improvement channel decoding connected with secured messages. A great end-to-end transmission system is composed of a encoder, which maps the source symbols in channel inputs, and a system decoder, which maps the channel outputs in noisy reproductions of the original source symbols. The machine encoder can be further divided into the source encoder, which maps the source symbols in an advanced alphabet, typically a set of binary strings, and the channel encoder, which maps the binary strings into coded bits or waveforms for transmission in the channel. Also, the process decoder can be broken into a channel decoder along with a source decoder corresponding towards the respective channel and source encoders. Any process encoder-decoder pair can be represented in this way, although your breakdown isn't unique.

Joint Channel coding and Cryptography makes use of Soft Input Decryption using feedback. The intention of channel coding theory is always to find exclusive codes which often transfer easily, contain several valid code words which often enables it to correct or a minimum of detect several errors. Although not mutually exceptional, performance inside these areas can be a trade away from. So, diverse codes usually are optimal with regards to different apps. The necessary properties of this code mainly count on the chance of problems happening through transmission.

The input with the encryptor is often a data block, which may be part of a data stream. The data block can be split inside two elements of the exact same length, message ma and message mb, both of length of m. All of both mail messages is extended by the cryptographic check value na and nb, both of length n, employing a cryptographic check function(ccf). In general, the program plans of message parts ma and mb and the lengths involving cryptographic check values na and nb need not be same. That unique lengths involving ma, mb, na and nb include only minimal influence with BER understanding that equal lengths plans for ma and mb, along with for na and nb, show the most beneficial results. For that reason, equal lengths of message parts along with cryptographic check values are utilized in this particular paper.

Block a involves the message part ma and the redundancy examine value na:

$a = a_1a_2\dots a_{m+n} = ma_1ma_2\dots ma_m\ na_1na_2\dots na_n$ …(1)

Block *b* consists of the message part *mb* and the redundancy check value *nb*:

$b = b_1b_2\dots b_{m+n} = mb_1mb_2\dots mb_m\ nb_1nb_2\dots nb_n$ ……..(2)

Interleaving of block *a* and block *b* forms the assembled message *u*:

$u = a_1b_1\ a_2b_2\dots a_{m+n}\ b_{m+n}$ ……(3)

u is encoded by a convolutional code, modulated and transferred over the noisy channel.

Following demodulation from the received message, Joint Channel Coding in addition to Cryptography is applied with 3 steps.

The first step consists of:

- channel decoding
- segmentation and de-interleaving of the output *u'* of the decoder into block *a* and block *b*, and
- parallel Soft Input Decryption with feedback of block *a* and block *b*.

The other step comprises is feedback from block a fixed by Soft Input Decryption to be able to block n, or vice versa, by block n corrected by simply Soft Input Decryption to be able to block some sort of. Lvalues of components of a corrected block (for instance, block a) are set to be able to ±∞, due to the fact bits are known and also correspondingly the Lvalues are known. L-values of components of another – definitely not corrected prevent (for instance, block b) are set to be able to 0, which usually represent mysterious bits. These L-values are fed to channel decoder, enabling improved bit miscalculation correction regarding block which should be corrected.

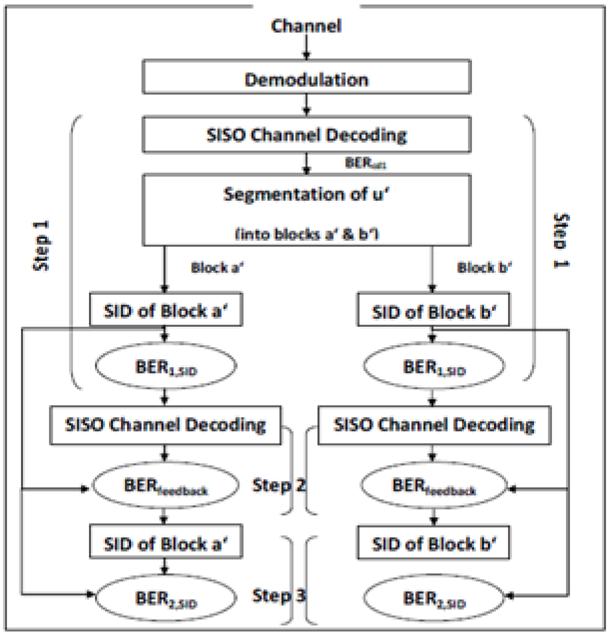

Fig 2:- Algorithm of Joint Channel Coding Cryptography

The third step is additional Soft Input Decryption of block, which has been improved corrected by feedback in the second step.

The second and the third step depend on one of the following cases:

- the results of Soft Input Decryption of block *a'* and Soft Input Decryption of block *b'* are correct, i.e. 0 1. = *SID BER* : *u* is corrected and there is no second and third step
- the result of Soft Input Decryption of block *a'* is correct, but block *b'* could not be corrected: in the following step the corrected block *a'* is used for the correction of block *b'* by feedback to the second channel decoding, resulting in *BERfeedback*. Block *b´* is tried to be corrected by Soft Input Decryption (*BER2.SID*).
- the result of Soft Input Decryption of block *b'* is correct, but block *a'* could not corrected: in the second step the corrected block *b'* is used for the correction of block *a'* by feedback to the second channel decoding,resulting in *BER feedback*. In the third step, block a´ is tried to be corrected by Soft Input Decryption (*BER2.SID*). • neither the result of Soft Input Decryption of block *a'* nor the result of Soft Input Decryption of block *b'* is correct: BER is equal to BER of the convolutional decoder (BER of the inner code).

IV. KEY GENERATION TECHNIQUES

Generating keys for cryptography. An important is used to encrypt and decrypt no matter what data has been encrypted/decrypted. Modern day cryptographic programs include symmetric-key algorithms (such since DES along with AES) along with public-key algorithms (such since RSA). Symmetric-key algorithms work with a single discussed key; preserving data key requires preserving this critical secret. Public-key algorithms work with a public key as well as a private critical. The general public key is distributed around anyone (often by way of a digital camera certificate). A sender encrypts data using the public critical; only the actual holder on the private critical can decrypt this specific data.

A. ElGamal key generation

Inside cryptography, the ElGamal encryption system is surely an asymmetric important encryption formula for public-key cryptography which will be based upon the Diffie–Hellman important exchange. It had been described byTaher Elgamal in 1985. [1] ElGamal encryption can be used in this free GNU Privateness Guard software package, recent variations of PGP, and other cryptosystems. The A digital Signature Algorithm is a variant regarding theElGamal signature scheme, which should not be confused with ElGamal encryption.

Key generation- The key generator works as follows:

- Alice generates an efficient description of a cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.
- Alice chooses a random x from $\{1, \ldots, q-1\}$.
- Alice computes $h = g^x$.
- Alice publishes h, along with the description of G, q, g, as her public key. Alice retains x as her private key which must be kept secret.

B. Cramer–Shoup system-

Inside cryptography, the ElGamal encryption system is an asymmetric critical encryption algorithm for public-key cryptography which is based on the Diffie–Hellman critical exchange. It was described byTaher Elgamal in 1985. ElGamal encryption is used in your free GNU Level of privacy Guard computer software, recent versions of PGP, as well as the Cramer–Shoup system is an asymmetric critical encryption algorithm, and was the primary efficient scheme confirmed to be secure next to adaptive picked ciphertext strike using standard cryptographic assumptions. Its security is based on the computational intractability (widely believed, but definitely not proved) on the decisional Diffie–Hellman premiss. Developed by Ronald Cramerand Victor Shoup in 1998, it is an extension on the Elgamal cryptosystem. Unlike Elgamal, that is extremely malleable, Cramer–Shoup provides other elements to make sure non-malleability actually against the resourceful assailant. This non-malleability is achieved by making use of a wide-spread one-way hash function and additional computations, causing a ciphertext that is twice while large like Elgamal. other cryptosystems. The Electronic digital Signature Algorithm can be a variant involving theElGamal trademark scheme, which mustn't be confused having ElGamal encryption.

Key generation-

- Alice generates an efficient description of a cyclic group G of order q with two distinct, random generators g_1, g_2.
- Alice chooses five random values (x_1, x_2, y_1, y_2, z) from $\{0, \ldots, q-1\}$.
- Alice computes $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^z$.
- Alice publishes (c, d, h), along with the description of G, q, g_1, g_2, as her public key. Alice retains (x_1, x_2, y_1, y_2, z) as her secret key. The group can be shared between users of the system.

C. Elliptic curve cryptography (ECC)-

Elliptic contour cryptography (ECC) is a technique for public-key cryptography using the algebraic construction of elliptic shape over limited fields. Elliptic curves are used in numerous integer factorization algorithms who have applications in cryptography, like Lenstra elliptic contour factorization.

Key generation-
Several discrete logarithm-based protocols have been adapted to elliptic curves, replacing the group $(\mathbb{Z}_p)^\times$ with an elliptic curve:

- the elliptic curve Diffie–Hellman (ECDH) key agreement scheme is based on the Diffie–Hellman scheme,
- the Elliptic Curve Integrated Encryption Scheme (ECIES), also known as Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme,
- the Elliptic Curve Digital Signature Algorithm (ECDSA) is based on the Digital Signature Algorithm,
- the ECMQV key agreement scheme is based on the MQV key agreement scheme.
- the ECQV implicit certificate scheme.

At the RSA Conference 2005, the National Security Agency (NSA) announced Suite B which exclusively uses ECC for digital signature generation and key exchange. The suite is intended to protect both classified and unclassified national security systems and information.

D. RSA technique –

RSA can be a cryptosystem, which is well know among the first practicable public-key cryptosystems and it is widely employed for secure files transmission. In that cryptosystem, the encryption key is public and differs through the decryption key that's kept key. In RSA, this asymmetry is founded on the useful difficulty associated with factoring the merchandise of a couple large excellent numbers, the actual factoring issue. RSA symbolizes Ron Rivest, Adi Shamir along with Leonard Adleman, who first openly described the actual algorithm throughout 1977. Clifford Cocks, the English mathematician, acquired developed the equivalent system in 1973, but it wasn't declassified until eventually 1997.

A individual of RSA creates then publishes the merchandise of a couple large excellent numbers, together with an auxiliary value, since their public key. The excellent factors must be kept key. Anyone may use the public key to help encrypt a message, but having currently published methods, in the event the public key is substantial enough, only a person with knowledge of the excellent factors may feasibly decode the actual message. Smashing RSA encryption is recognized as the RSA issue. It is surely an open question whether it is as hard because the factoring issue**.**

Key generation-

RSA involves a *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[5]
5. Determine d as $d \equiv e^{-1}$ (mod $\varphi(n)$); i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
   - This is more clearly stated as: solve for d given $d{\cdot}e \equiv 1$ (mod $\varphi(n)$)
   - This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond to e and φ(n), respectively.
   - d is kept as the private key exponent.

The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1$ (mod λ) with $\lambda = \mathrm{lcm}(p - 1, q - 1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.
- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

V. SCRAMBLING TECHNIQUES

Error control techniques are designed to ensure reliable data transfer over unreliable communication channels that are frequently subjected to channel errors. In this paper, the effect of applying a convolution code to the **Scattered Random Network Coding (SRNC) scheme** over a multi-hop wireless channel was studied. An interleaver was implemented for bit scattering in the SRNC with the purpose of dividing the encoded data into protected blocks and vulnerable blocks to achieve error diversity in one modulation symbol while randomising errored bits in both blocks. By combining the interleaver with the convolution encoder, the network decoder in the receiver would have enough number of correctly received network coded blocks to perform the decoding process efficiently. Extensive simulations were carried out to study the performance of three systems: 1) SRNC with convolutional encoding, 2) SRNC; and 3) A system without convolutional encoding nor interleaving. Simulation results in terms of block error rate for a 2-hop wireless transmission scenario over an Additive White Gaussian Noise (AWGN) channel were presented. Results showed that the system with interleaving and convolutional code achieved better performance with coding gain of at least 1.29 dB and 2.08 dB on average when the block error rate is 0.01 when compared with different systems respectively.
Recently, cooperative communications have been widely acknowledged as a virtual multi-antenna system that resolves the size or hardware limitations at transmitter. We develop randomized cooperation and analyze its diversity protocols that combat fading induced by multi-path propagation in wireless networks. Decentralized cooperation with

randomized space-time coding exploits both spatial and temporal diversity available through cooperating users' relaying signals and sharing single antenna mutually. With several randomization techniques introduced, we study performance characterizations in terms of symbol error probability, which measures robustness of the transmissions to fading, focusing on the high signal-to-noise (SNR) regime. We also show that the cooperative diversity analysis is theoretically and numerically suitable even for frequency selective channels

VI. PROBLEM DEFFINETION

Communication over a wireless channel, due to its broadcast nature, is inherently prone to data security issues too. In order to overcome this limitation, cryptography is used to secure the information transfer: it protects against eavesdropping or manipulation of transmitted information, or masquerading of data origin. It is however noteworthy that the error correction and data security are dealt separately so far by the researchers. We hereby propose a novel technique which combines the data security techniques i.e. the cryptographic algorithms, with the techniques for error correction. Thus in this work we make use of cryptographic check values as the redundancy data for error recovery at the receiver end. As we discuss further, this scheme gives a coding gain of 0.72 dB over convolutional coding with the same coding rate. By using the HMAC as the redundant data for error correction, we also get all the benefits associated with these schemes such as data origin authentication, non repudiation by source and data integrity.

VII. PRAPOSED WORK

We have to propose a more efficient and effective techniques for the error detection and correction using joint channel coding and cryptography. We work on this with the different combination of the algorithms for channel coding and cryptography which is more efficient. We compare the efficiency with the existing technique. And we also change the scrabbling technique for the massage confidentiality and also change the key generation methods for give the higher security to the our data or massage.

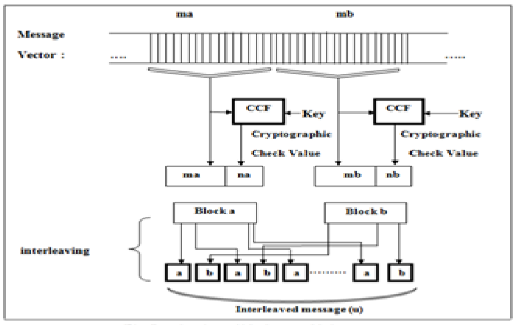

Fig 3:- Interleaving of blocks *a* and *b* into message *u*

ACKNOWLEDGEMENT

I am very much grateful to Department of CSE, DIMAT to give me opportunity to work on Error prevention and detectiotion in wireless communication . I sincerely express my gratitude to Mrs. Preeti Tuli of Dept. of M.Tech CSE, DIMAT for giving constant inspiration for this work. I am also thankful to Prof. Somesh Dewangan, Dept. of CSE, DIMAT for helping me directly and indirectly during this work. I am really thankful to my all friends for their blessing and support.

REFFERENCE

1. A Goldsmith, Wireless communications, Cambridge University Press, 2005
2. L. Zhuo, K. Lam and L. Shen, “Adaptive forward error correction for streaming stored MPEG-4 FGS video over wireless channel”, in Proc. IEEE 5th Workshop on Signal Processing Advances in Wireless communications, Lisboa, Portugal, Jul 2004, pp. 26-30.
3. C. Ruland and N. Živić, Soft Input Decrzption, 4th Turbocode Conference, 6th Source and Channel Code Conference, VDE/IEEE, Munich, Germany, April 3 – 7, 2006.
4. C. Ruland and N. Živić, Feedbaack in Joint Channel Coding and Cryptography, 7th Source and Channel Code Conference, VDE/IEEE, Ulm, Germany, January 14 – 16, 2008.
5. D. Chase, A Class of Algorithms for Decoding Block Codes with Channel Measurement Information, IEEE Trans. Inform. Theory, IT-18, pp. 170-182, January 1972.
6. G. D. Jr. Forney, Generalized Minimum Distance Decoding, IEEE Trans. Inform. Theory, IT-12, pp. 125-131, April 1966.
7. S. Lin and D. J. Costello, Error Control Coding, Pearson Prentice Hall, USA, 2004.
8. Ruland, C: Informationssicherheit in Datennetzen, datacom Verlag, Bergheim 1993, ISBN-3-89238-081-3
9. ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 1999.
10. ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a hash-function, 2000.
11. ISO/IEC 9798-1 Information technology – Security techniques – Entity authentication mechanisms – Part 1: General, 1997.
12. L. Bahl. J., Jelinek, J., Raviv and F., Raviv, Optimal decoding of linear codes for minimizing symbol error rate, IEEE Transactions on Information Theory, IT-20, pp. 284-287, 1974.
13. Hagenauer, J., Höher, P.: A Viterbi algorithm with soft-decision outputs and its applications, Proc. IEEE GLOBECOM `89, Dallas, Texas, USA, vol. 3, pp. 1680-1686, November 1989.
14. M. Jeruchim, P. Balaban and K. S. Shanmugan, Simulation of Communication Systems, Kluwer Academic/Plenum Publ, New York, 2000 756.