Coding and Spectrum Technique for Satellite Communication to Improve Protection of High Data Links under Security Threats

[1]Tarun Varma, [2]Dr.Akhilesh R. Upadhyay,
[1]Research Scholar PhD, [2]Supevisor
ECE, Mewar University, Chittorgrah, India
Email – [1]tarunindia@rediffmail.com, [2]akhileshupadhyay@gmail.com

Abstract: *DSSS is an anti-jamming modulation technique which is a type of spread spectrum in terms of spreading the data using pseudo spreading codes, but not depends on secret pre-shared spreading sequences but the spreading codes are set in random order so it is called uncoordinated DSSS. In disparity to counter-jamming uncoordinated DSSS communication, where the spreading sequence is secret and it shared only by the authorized communication receivers.*

Key Words: *DSSS, Turbo Codes, Coding Scheme, Spreading Codes, MIJI*

1. INTRODUCTION:

In DSSS, an open set let it is "S" of spreading pseudo sequences employed by the source and the destination. The random order code "S" may be unknown to the attacker . To broadcast information, the transmitter frequently chooses random new spreading sequence from "S" and spreads the information over this sequence. The recipient's received the signal by monitoring and decodes it on the channel and de-spread the information by pre-defined sequences from S. The code sequences employed to spread the entire information. Hence, DSSS neither requires information fragmentation at the source nor information reassembly at the receivers.

$$\text{N (Pm)} \approx \sum_{j=0}^{n}.\sum_{j=0}^{n} D(L,j)((1-Pm)^{i})^{L-j}.(1-(1-Pm)^{i})^{j}L, \qquad (1)$$

where D(L, j) is the numeral of sets with cardinality j that do not allow the reconstruction of the information. The duration t_M of a frequency hop (i.e. the moment to toggle the frequency and transmit a packet)

$$t_M^1 \approx \sum_{i=0}^{n}.\sum_{j=0}^{n} D(L,j)((1Pm)^{i})^{L-j}.(1-(1-Pm)^{i})^{j}Ltm, \qquad (2)$$

$$t_M^g \approx \sum_{i=0}^{n}(1-(1-\sum_{j=0}^{n} D(L,j)((1-Pm)^{i})^{L-j}.(1-(1-Pm)^{i})^{j}Ltm \qquad (3)$$

With DSSS, the expected time to decode a information of length $|M|$ is

$$t_M^1 \approx \frac{Nkq|M|/r_c}{\Lambda_{B(N)}}\left(\frac{n}{1-p_j}-\frac{n}{2}\right) \qquad (4)$$

$$t_M^1 \approx \frac{Nkq|M|/r_c}{\Lambda_{B(N)}}\left(\sum_{i=1}^{\infty}(1-(1-p_j^i)^g)n+\sum_{i=1}^{n}(1-(\frac{i}{n})^g)\right) \qquad (5)$$

Fig.1(a),(b) Massage size and group size

DSSS uses balanced pseudo spreading codes to achieve proper synchronization at receiver end and for proper mutual minimum interference of the spreading codes. There is no time-synchronization between the receivers which is using only spread spectrum and the transmitter regarding the signals in spreading form, i.e., there is no information to

recipient about the information bit or massage synchronization. In case where information losses due to MIJI , the source broadcasts the information over and over in repeated manner and the receivers applies sliding window protocol to synchronize with the transmission.The constraint of DSSS is the receivers to store all bits received, analyze them reproduce to find the used of spreading code. More numbers of transmitters which in contrast with DSSS, enhance the performance and jamming-resistance of DSSS. More precisely, if consider m = 1, it enable parallel broadcast transmissions of the similar information with different random spreading codes. This combination could be attained if one transmitter transmitting M signals in parallel with each spread code with a different spreading codes or another combination is by using M separate sending devices. In DSSS process, the receivers has to search through multiple set of codes and has to use synchronization windows so as to dispread the received information.

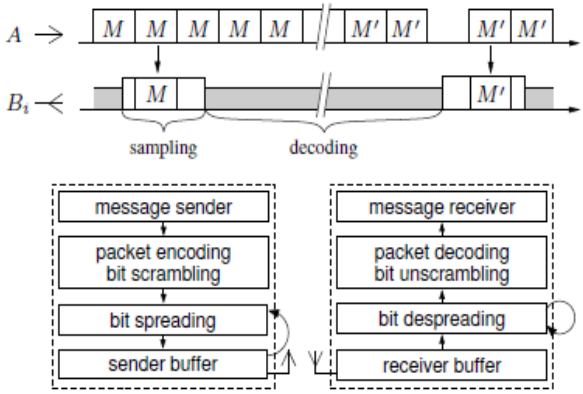

Figure 2: Uncoordinated DSSS (DSSS). The transmitter repeatedly spreads and transmits the information ,the receivers monitor the channel and apply window.

2. CODING FOR SATELLITE COMMUNICATION:

Satellite and Wireless communication systems mostly used topology in which multiple small terminals communicated with a hub or base station using a predefined shared channel. Transmission is in frames or in form of packets and a fundamental problem is the secure and efficient sharing of the particular channel. Typically such systems are known as very small aperture terminal (VSAT) satellite systems. For the mitigation of the effect of co-channel signals interference cancellation and decoding is suitable method. In other type of wireless communication systems the collisions between two or more systems causes packet and the exclusion or diminution of frame loss leads the significant improvement in achievable output and efficient usage of system resources. Turbo codes are employed to independently and separately encode each user's data, which is transmitted on an AWGN channel. By using this each user is allocate a dissimilar power, which allows the decoding of high power users to point toward dedicated path and this leads reduction in interference so that the decoding of lower power users can then also point towards dedicated path. Iterative decoding assigned within every Turbo codes multiple subscribers. Each subscriber has arbitrary assigned codes and after the employment of turbo code encoder there is generation of code bit interleaver. There is another alternative and current method is that when Reed Solomon (RS) coding is combined with a Turbo code and used for broadcast over a digital video broadcasting (DVB) satellite system. The Turbo codes of multiple users are jointly decoded by means of a combined trellis for every component used in convolutional codes in such a way that iterative decoding is assigned to performed among trellis decoders. This leads to the fact that in Turbo codes and convolutional codes having small difficulty and as a result the difficulty is managed in trellis. For the use of optimal maximum a posteriori (MAP) decoding the transmitted symbols are structured such that both users have combined component codes. This method provides significantly improved decoding the two users' which uses codes independently and maintaining feasible decoding complexities. Symbol-based decoding is employed to facilitate improvement in combined decoder convergence. The transmitted symbol from both users responsible to create composite constellation and the decoder which uses metrics is based on composite constellation and higher order modulation is also possible, because Turbo codes do not perform fine with higher order modulation so the use of symbol interleaving improves convergence. When the receiver gets entire data in decoded form, it is necessary to provide different signature to different user so data is decoded by the correct user .The easy solution is to employ different component codes. The encoding and decoding are using the tail biting method.

3. TURBO CODES:

The joint probability of symbol A and B where A is broadcasted symbol and B is received symbol can be given as,

$$P(A, B) = P(B|A)\, P(A)$$

where P(B|A) is known as a- posteriori probability or probability of received symbol after transition.
The encoder works on the fact that every time it tries to estimate the broadcasted symbol A and received symbol B .So by calculating a posteriori probability of received symbols the Turbo code calculate a priori probability for the broadcasted symbols. Recursive Systematic Convolutional Codes (RSCC) are connected in parallel. The input binary data u_k was fed directly to the RSCC1 and parity bits p_k 1 was obtained, while a interleaver was used change the order of u_k in order to obtain a different set of parity bits p_k . The encode worked at rate 1/3 (for every one bit of data parity bits are produced) but, to obtain higher data rate parity bits were punctured using a Puncturer.

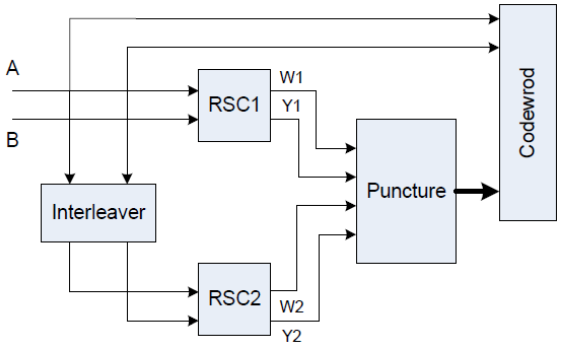

Fig 3 Recursive Systematic Convolutional Codes (RSCC)

RSCC are such type of convolutional encoders which are having forward and backward feedback loops. For the purpose of reliable decoding the RSCC having recursive systematic property which allow encoder to use independent parity bits from the different input. The generator matrix for RSCC is given by

$G_R(D)=[1 \quad g_2(D)/g_1(D)]$ (6)

In recursive systematic convolution encoder the polynomials $g_1(D)$ and $g_2(D)$ defines feedback and feedforward connection which comes under the generator matrix for the RSCC and given by,

$g_1(D) = [1\ 0\ 0\ 1\ 1]$

and the feedforward connection is given by,

$g_2(D) = [1\ 1\ 0\ 0\ 1]$

Interlevear

The Turbo encoder produces random code words. The interleaver scrambles the sequence in pre determined order at encoder and re arrange the sequence in original form at decoder. There are various types of interleaver which divided on the basis of bit position like ,Even & Odd interleaver, Rectangular interleaver and Random interleaver. In Even & Odd interleaver the scrambling is done on the basis of even and odd position of bits, in Rectangular interleaver scrambles bits coloum wise for reading and row wise for writing and Random interleaver improves the distance d between the code words with reducing association between the bits. For code rate of 1/3 ,two parity bits are produced by RCSS1 and RCSS2 for information bit u_k. It is also important to achieve higher code rate so the data become better for any system[24,25] this can be achieved by using puncturing in Turbo code. The puncture reduces some parity bits so to reduce overload. The even bits from RCSS 1 and Odd bits from RCSS 2 are discarded to achieve higher code rates of ½. A particular pattern of puncturing P(p,q) is used for achieving code rate higher than 1/2 , where p corresponds remaining bits from RCSS 1 and q corresponds remaining bits after reduction of some bits in RCSS2.

4. MAXIMUM A- POSTERIORI (MAP) TURBO DECODER:

Maximum A- Posteriori (MAP) Turbo Decoder MAP algorithm generates certain samples on the basis of estimated error and identifies the original symbol which generated as the received set of signal L(e|w) in other words MAP algorithm identifies the population and it is maximum likelihood function of error. The ‘e’ denotes estimation at the receiver from a particular symbol ‘w’ on signal. MAP algorithm is always concentrated towards the value which maximize the L(r|w) and this value is provided only by ‘w’. This method is used for decoding. There are two MAP decoders used by decoders in Turbo decoding process. The MAP calculate the value of reliability ‘L’ over which each trellis based decoder decodes the bits. By using input sequence u_k and parity bits p_{k1}, the decoder 1 calculates the value of ‘L’ and passed these value to decoder 2 ,now decoder 2 also uses input sequence u_k and parity bits p_{k2} and generates new value of ‘L’ and thus iteration process starts between decoders which passes the value of L. The decoders generates same pattern as generated by encoder for the value of L. The decoder use the previous value of bit reliability for correction of decoding error and this value of L passed to another decoder iteration process. Depend on the trellis used the data is split into blocks of data and ‘k’ represents time association in each bit for a particular frame of data.as mentioned decoder 1 and decoder 2 are depend on used trellis, now for correcting the bits correctly we need any two information by three elements: current state's', input bit 'u_k' and next sate ' s' '. The joint probability that for a input bit u_k and the switch from state s to s', assuming the entire sequence 'y' is received " is P(s', s, y)

$$L_K=\frac{\sum_{u_{k=1}} P(s's,y)}{\sum_{u_{k=0}} P(s',s,y)} \quad (7)$$

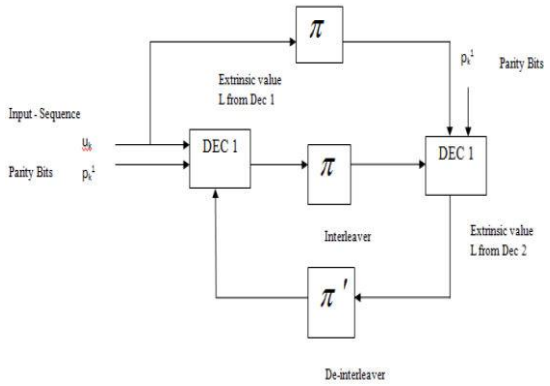

Fig 4 :- *De-interleaver*

The summation ratio of probability of transition which corresponds to value '1' or '0' respectively,provide the reliability value 'L' for k^{th} bit i.e. L_k.The sign of the reliability value denotes the decoded value either it is binary zero for negative value or it is binary one for the positive value. The dependability of the decoded bit indicates magnitude.
Using the Bayer's theorem P(s',s,y)

$$P(s',s,y)=P(y_f|s',s,y_p,y_k)P(s',s,y_p,y_k) \quad (8)$$

where, y_p , y_k and y_f are the past data sequence, current input data bit, and future data sequence respectively. As the future data is independent of current and past inputs, Equation 4.8 becomes

$$P(s',s,y)=P(y_f|s)P(s',s,y_p,y_k) \quad (9)$$

Again, applying Bayer's theorem
Using Equations 4.8 and 4.9, we get

$$P(s',s,y_p,y_k)=P(s,y_k|s',y_p)P(s',y) \quad (10)$$

where, the terms can be defined as,
$P(s',y_k)=\alpha_{k-1}(s)$= Forward Transition Metric.
$P(y_f|s)=\beta_k(s)$= Backward Transition Metric.
$P(s,y_k|s',y_p)=\Upsilon_k(s',s)$= Gamma Transition Metric.

If the k^{th} bit received at the encoder then the trellis structure is constructed on this basis and to make a decision on the transmitted bit, the a ,ß and ϒ values are calculated for each branch which result transition from '1'and '0' input respectively.

5. CALCULATING METRICS:

y_k is probability of transition on a particular branch at k^{th} bit, which is also initial value for the calculation. the transition does not depend on the past values so neglect the term y_p and there for equation become

$$\Upsilon_k(s',s)=P(s'y_k|s') \quad (11)$$

Using Bayer's theorem

$$\Upsilon_k(s',s)=P(y_k|s',s)P(s|s') \quad (12)$$

But,

$$P(s|s')=P(u_k) \quad (13)$$

Because the probability of transition on an edge is similar to that of the probability of receiving of particular bit u_k at k^{th} instant. The transmitted bit become zero therefore $P(u_k)$ is neglected for the not calculation. The final form of ϒ is $\Upsilon_k(s',s)=P(y_k|u_k)$ (14)
The final step for bit decision making is depend on calculation of bit reliability value, which is referred to as $L(u_k)$ and mathematically represented as

$$L(u_k)=\log\left(\frac{\sum_{u_k}\alpha_{k-1}(s')\gamma_k(s',s)\beta(s)}{\sum_{u_k}\alpha_{k-1}(s')\gamma_k(s',s)\beta_{(s)}}\right) \quad (15)$$

Where

$$\alpha_k(s)=\sum_{All-s'}\Upsilon(s',s)\alpha_{k-1}(s')$$

$\alpha_k(s)=\begin{cases} 1 \ if \ s=1 \\ 0 \ otherwise \end{cases}$

$B_{k-1}(s')=\sum_{All-s'} \beta_k(s')\gamma(s',s)$

$B_N(s)=\begin{cases} 1 \ if \ s=0 \\ 0 \ otherwise \end{cases}$

6. TURBO DECODER:

For calculation of bit decision making the value '0' is calculated. But '0' value does not used directly in decision making because it is attended by single decoder in single iteration. For the completion of one iteration the value'0' calculated at decoder 1 is passed to decoder 2. For making the decision process the '0' value calculated at decoder 2 is passed to decoder 1. The value '0' used for decision making improves or reliability value improves as iteration increases. Turbo code resembles the working of turbo engine as in iterative action passing of bits from one decoder to another improves the decoder performance hence the name Turbo code comes. The Turbo code use channel estimation value which is value '0'.Thus the combination of channel estimation, trellis property and iterative decoding represents turbo coding which is near shanon limit coding gain

$L_f(u_k)=L(u_k)+L_{extrinsic}(u_k)$ (16)

7. CONCLUSION:

The mitigation of the effect of co- channel signals interference cancellation and decoding is a suitable method. In Even & Odd interleaver the scrambling is done on the basis of even and odd position of bits, in Rectangular interleaver scrambles bits coloum wise for reading and row wise for writing and Random interleaver improves the distance d between the code words with reducing association between the bits. There are two MAP decoders used by decoders in Turbo decoding process.so this may improve security.

REFERENCES:

1. Thomas A. Groshong (June 2011), Satellite Communications System Security Risk Analysis by Sr 20.
2. Don Wilcoxson (2011), Advanced Commercial Satellite Systems Technology for Protected Communications by in military conference.
3. Christina P¨opper , Mario Strasser , Srdjan ˇ Capkun (JUNE 2010) , Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 28, NO. 5,
4. Michael *Spuhler* , *Domenico* Giustiniano, Vincent Lenders, Matthias Wilhelm, Jens B. Schmitt (MARCH 2014) , Detection of Reactive Jamming in DSSS-based Wireless Communications and IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 3,
5. Hamdan.O.Alanazi, Rafidah Md Noor, B.B Zaidan, A.A Zaidan (*FEBRUARY 2010)*, 'Intrusion detection system Detection System: Overview' *JOURNAL OF COMPUTING, VOLUME 2, ISSUE 2, , ISSN 2151-*9617https://sites.google.com/site/journal of computing
6. Ali Jafarnia-Jahromi , Saeed Daneshmand and Gerard Lachapelle (Dec 2013) , Spoofing Countermeasure for GNSS Receivers - A Review Of Current And Future Research Trends 4th Intern Colloquium on Scientific and Fundamental Aspects of the Galileo Programme, Prague, 4-6
7. Wenzhun Huang, Multi-sub-channels Spread Spectrum Anti- interference System and its Performance, China International Conference on Logistics Engineering, Management and Computer Science (LEMCS 2014)
8. Nguyen Xuan Quyen, Chuyen T. Nguyen, Pere Barlet-Ros, and Reiner Dojen, 'A Novel Approach to Security Enhancement of Chaotic DSSS Systems', 978-1-5090-1801-7/16$31.00 ©2016 IEEE
9. Aleksandar Jovanovic , Multi-test Detection and Protection Algorithm Against Spoofing Attacks on GNSS Receivers, Electronics and Signal Processing Laboratory (ESPLAB) Ecole Polytecnique Federale de Lausanne Lausanne, Switzerland© 2014 IEEE.
10. V. Le NirH and B. Scheers , 'Robust blind carrier frequency synchronisation for direct sequence spread spectrum systems ELECTRONICS LETTERS 5TH MARCH 2015 VOL. 51NO. 5 PP. 425-427
11. Sungdon Moon, Chiho Lee, *Yungkyun* Choiand Kiseon Kim , 'Performance of Satellite Communication System with Fh-Mfsk Under Various Jamming Environments - Department of Information and Communications Kwang-Ju Institute of Science and Technology (K-JIST), 1 Oryong-dong, Puk-ku, Kwangju 500-712, S. Korea, 5-MILSATCOM.
12. Bo Chen, Shan Tang, Xiuli Du, Xu Wu, Study on An Anti-Jamming Method of Spread-Spectrum Communication Based on Lt Codes School of Information Engineering, Dalian University, Dalian, China
13. Philippa A. Martin , Marcel A. Ambroze, Desmond P. Taylor, and Martin Tomlinson (AUGUST 2009), Coding for Shared Satellite Channel Communications, TRANSACTIONS ON COMMUNICATIONS, VOL. 57, NO. 8,

14. Riccardo De Gaudenzi, , Albert Guillen i Fabregas, and Alfonso Martinez,(September 2006), Performance Analysis of Turbo-Coded APSK Modulations over Nonlinear Satellite Channels,. IEEE Transactions On Wireless Communications, Vol. 5, No. 9,
15. Weihua DaiH, Chunjie Qiao, Yueke Wang and Chao Zhou ,(Weihua DaiH, Chunjie Qiao, Yueke Wang and Chao Zhou) 'Improved anti-jamming scheme for direct- sequence spread-spectrum receivers ELECTRONICS LETTERS 21ST JANUARY 2016 VOL.52 NO. 2 PP. 161-163
16. Efficient Uncoordinated FHSS Anti-jamming Communication Mario Strasser Communication Systems Group ETH Zurich, Switzerland Christina Popper System Security Group ETH Zurich, Switzerland.
17. Satellite Raoul Prevost1'2, Martial Coulon1, David Bonacci2, Julia LeMaitre3, Jean-Pierre Millerioux3 and Jean-Yves Tourneret ,(2012) ' Interference Mitigation and Error Correction Method for AIS Signals Received 120th European Signal Processing Conference (EUSIPCO 2012) Bucharest, Romania, August 27 - 31,
18. Michael G. Luby, Michael Mitzenmacher, M. Amin Shokrollahi, and Daniel A. Spielman ,(February 2001) Efficient Erasure Correcting Codes IEEE Transactions on Information Theory, Vol. 47, No. 2,
19. Detection Strategy for Cryptographic GNSS Anti-Spoofing Todd E. Humphreys Preprint of article in IEEE Transactions on Aerospace and Electronics Systems
20. C. E. Shannon, \A mathematical theory of communication," *Bell System Technical Journal*, pp. 379{427, 1948.
21. R. Hamming, \Error detecting and error correcting codes," *Bell System Technical Journal*, pp. 147{160, 1950.
22. M. Golay, \Notes on digital coding," *Proc. IEEE*, vol. 37, p. 657, 1949.
23. P. Sweeney, *Error Control Coding: An Introduction*. New York: Prentice Hall, 1991.
24. P. Ellias, \Coding for noisy channels," *IRE Nat. Conv. Record*, vol. 3, no. 4, pp. 37.
25. A.J. Viterbi, \Error bound for convolutional codes and asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260{269, Apr. 1967.
26. BT nodes - A Distributed Environment for Prototyping Ad Hoc Networks. http://www.btnode.ethz.ch/.