Performance Evaluation of Satellite Communication in Intentionally or Unintentionally Interference Environments and its possible Detection Techniques

Tarun Varma[1], Dr. Akhilesh R. Upadhyay[2]
[1] ECE,Mewar University,Raj
[2] SIRTS Bhopal(MP)

Abstract- *Interference and jamming severely disrupt our ability to communicate by decreasing the effective signal-to-noise ratio and by making parameter estimation difficult at the receiver. The objective of this research paper is to design robust wireless satellite communication systems and algorithms to suppress the adverse effects of non-intentional co-channel interference (CCI) or intentional interference. In particular, we develop chip-combining schemes with timing, channel, and noise-power estimation techniques, all of which mitigate CCI. We also exploit the spatial diversity and iterative receiver techniques for this purpose. Most of the existing timing estimation algorithms are robust against either large fre¬quency offsets or CCI, but not against both at the same time. Hence, we develop a new frame boundary estimation method that is robust in the presence of severe co-channel in¬terference and large carrier-frequency offsets. We analyze the diversity order, coding gain, and bit-error rate (BER) upper bound for a quasi-static Rayleigh-flat-fading channel. We also propose a blind, accurate, and computationally efficient signal-to-noise ratio (SNR) estimator for the constant-envelope system.*

Keywords- CCI, BER, Rayleigh-flat-fading channel, SNR.

I. INTRODUCTION

Due to the shared use of the communication medium, wireless radio communications are highly vulnerable to a wide range of attacks, including eavesdropping, message synthesis, Denial-of-Service (DoS), and spoofing attacks. Given the focus of this paper, we discuss DoS and spoofing attacks in the following paragraphs. DoS attacks. The term DoS attack refers to attempts that aim at disrupting the devices or the network operation. It also encompasses any active attempt to diminish or eliminate the device capabilities of performing their expected functions, in particular of carrying out their communication. The most destructive DoS attack on wireless communication is jamming. Jamming takes effect on the signal transmission. In jamming attacks, the attacker emits jamming signals that interfere with an ongoing transmission such that they prevent the intended receiver(s) from successfully recognizing and decoding the transmitted message. This can happen either because the power of the jamming signal overwhelms the information content in the legitimate signal or because the combined (legitimate and jamming) signals have characteristics that prevent the receiver from extracting the proper information. Jamming makes communication attempts temporarily ineffective, but does not destroy devices. In this context, reactive (or responsive) jamming denotes that attackers sense for ongoing transmissions in order to compose their jamming signals (they apply power management to identify the appropriate direction of transmission, power, and timing for their jamming signals). This enables them to jam in a targeted manner without wasting energy (no ineffective jamming) and lowers their risk of detection due to high power jamming and long transmission phases.[1][2][3]

II. DETECTION TECHNIQUES AND COUNTERMEASURES

Traditional ways to detect jamming are based on the use of energy detectors and on sudden drops in the packet reception ratios. Countermeasures against jamming address the problem of enabling communication despite the presence of intentional interference. Traditional countermeasures are spread-spectrum techniques, in particular frequency hopping and direct-sequence spread-spectrum. Further techniques are packet coding schemes that enable error correction e. g., using erasure codes, Countermeasures against spoofing attacks. Most countermeasures against spoofing and jamming attacks rely on secrets that must be pre-shared between the communicating devices prior to the start of their communication. This impede jamming-resistant. Spread-spectrum techniques are effective against jammers that cannot cover the entire bandwidth of the available frequency spectrum simultaneously with their jamming signals i.e. wideband jammers, would require significant amounts of power and thus risk fast detection and localization. Spread-spectrum techniques make a sender spread a signal over the

available band of radio frequencies in a way that is unpredictable for the attacker. The attacker's ability to alter or erase a message is limited by the achieved processing gain of the spread-spectrum communication. The processing gain indicates the ratio by which interference can be suppressed relative to the original signal. Essential for both FHSS- and DSSS-based communication is that the sender and the receiver share a secret prior to their communication which enables the receiver to generate the random sequence used by the sender.[5][6][7][12]

III. FHSS

In FHSS, the frequency of the carrier signal is switched within a wide frequency band according to a spreading (hopping) sequence defined by a pseudo-random number. When the receiver follows the hopping sequence of the sender, it can receive the sender's signal and demodulate the message. The transmitted signal uses only a narrow band of the available frequency spectrum at each instant in time. The time during which the sender dwells on the same frequency. One can, however, distinguish between fast frequency hopping (FFHSS) and low frequency hopping (LFHSS). The latter method allows several consecutive data bits to be modulated on the same frequency slot. FFHSS is characterized by several hops within each data bit. The bandwidth of a frequency-hopping signal is the bandwidth of each hop channel times the number of available frequency slots. The processing gain of an FHSS communication system corresponds to the number of available orthogonal (non-overlapping) frequency channels. [8][9][[13][15]

IV. DSSS

In DSSS, the spreading process effectively multiplies (mixes) the carrier signal with apseudo-noise digital signal. More specifically, the data signal is modulated with a predefined spreading signal of a higher rate; this mixing basically corresponds to applying the XOR-operation to the binary values. This results in an RF signal that requires a wide bandwidth and approximates the spectral equivalence of noise. The demodulation process mixes the same (e. g., BPSK- or QPSK-) modulated spread carrier with the incoming RF signal. When the correlation of the two signals exceeds a certain threshold, it is filtered and sent to a demodulator. Except for the secret code, all other communication parameters (modulation, frequency band, etc.) can be public. The processing gain of DSSS directly relates to the length N of the spreading code used to spread one data bit. The sender modulates and transmits the result. Upon signal reception, each receiver samples and demodulates the signal. FHSS and DSSS techniques share a property regarding broadcast communication as a side effect of the symmetry of the jamming prevention (the sender and receivers use the same secret), they enable dishonest or compromised receivers, which are in possession of the secret, to disrupt the transmission for other receivers within their transmission radius by jamming. This limits the use of these techniques to settings where the receivers can be trusted, compromise can be excluded, and receivers are known in advance so that the secret can be shared in advance. To investigate the suitability of different attacker models for wireless satellite communication The interference occure ongoing wireless transmissions in the propagation Channels.

In wireless mobile communications, the transmitted signal is subject to various impairments caused by the transmission medium combined with the mobility of transmitters and/or receivers. Path-loss is an attenuation of the signal strength with the distance between the transmitter and the receiver antenna, and the frequency reuse technique in cellular systems is based on the physical phenomena of path-loss.[15][2][6]

V. INTER SYMBOL INTERFERENCE (ISI)

In radio channels for digital communication, ISI is due to multipath propagation when the delay spread of the channel is large compared to the duration of modulated symbol.[1][4][8]

Co-Channel and Adjacent-Channel Interference (CCI and ACI)

CCI is introduced when a frequency band is shared by multiple users at the same time. In cellular systems, CCI arises by the frequency reuse in neighboring cells. As frequency reuse factor decreases to increase the system capacity, CCI increases as the distance between the co-channel cells decreases. Therefore, the performance of a frequency reuse system is limited by CCI rather than by additive noise.[13]

Interference Mitigation Techniques

The characteristics of CCI and ISI of a wireless communication system is determined by the radio interface and the network topology of the system. Accordingly, a broad range of interference mitigation techniques have been employed at transmitter. In system-design approaches, transmission of co-channel signals is properly managed so that the power of received CCI is maintained below an acceptable level. In con¬trast, receiver-design approaches actively mitigate the CCI/ISI which cannot be separated by the

preemptive system-design approaches. In practical systems, both approaches are employed in joint fashions to reduce the interference.

Frequency Reuse and Multiple Access

Information streams from multiple users can be transmitted in parallel through a shared radio spectrum by isolating signals from different users from each other in multiple do¬mains. In time, frequency, and code division multiple access (TD/FDMA) techniques, signals from multiple users are transmitted by using non overlapping time slots, non overlapping frequency bands, and codes having very small cross correlations, respectively, so that signals from different users are easily separated. Two forms of CDMA, frequency hopping (FH) and direct sequence (DS), are widely used in military and commercial appli¬cations. [17]

Diversity Combining for CCI Suppression

ISI equalization, this drawback can be compensated for by using a concatenated symbol-by-symbol equalizer or sequence estimator.[19]

Two-Stage Interference Cancellation

In frequency selective fading channels, all co-channel signals experience ISI. Liang et al.'s work on two-stage CCI/ISI reduction method was motivated by this observation. In the two-stage interference mitigation, the CCI is suppressed by a space-time filter in the first stage and the ISI is cancelled by a Viterbi type equalizer in the second stage systems.[12]

Multiuser Detection

Distinguished from single-user detection techniques, which treats signals from co-channel users as interference, multi-user detection (MUD) detects all co-channel signals simultaneously. Since MUD techniques not only increase the system capacity but also improve the quality of an individual communication link by eliminating CCI from multi-users[8]

VI. PROPOSED MODEL

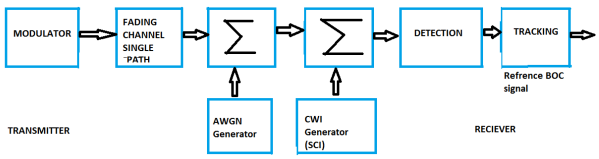

Figure 1. proposed model for interference mitigation using AWGN

Simulation Result

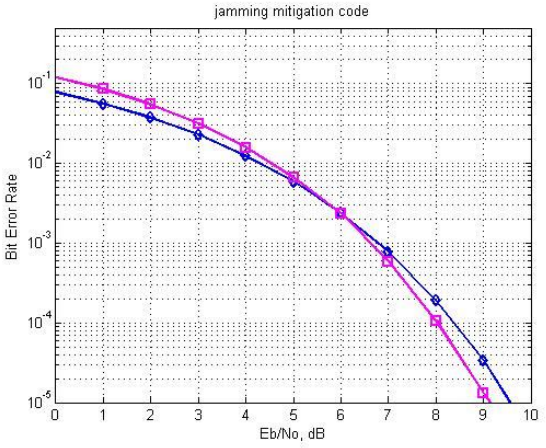

Figure 2. simulation result of signal in terms of BER and E0/N

VII. CONCLUSION

This paper addressed the problem of mitigating the adverse effects of CCI and jamming by developing systems and algorithms. Many of the techniques presented in this paper and can be applied to other systems. The proposed system does not require additional error-correction coding or interleaving to guarantee full spatial diversity. The proposed system is capable of iteratively estimating JSI, that enhances the SINR at the output under both type of interfernce.

REFERENCES

[1] R. W. CHANG, "Synthesis of band-limited orthogonal signals for multi-channel data transmission," Bell System Technical journal, vol. 46, pp. 1775-1796, 1966.

[2] R. CHANG, and R. GIBBEY, "A Theoretical Study of Performance of an Orthogonal Mult iplexing Data Transmission Scheme," IEEE Trans, on Commun., vol. 16(4), pp. 529-540, Aug. 1968.

[3] E. BIGLIERI, R. CALDERBANK, A. CONSTANTINIDES, A. GOLDSMITH, A. PAULRAJ, and H. V. POOR, MIMO Wireless Communications, Cambridge University Press, 2007.

[4] U. MENGALI and ALDO N. D'ANDREA, Synchronization Techniques for Digital Re¬ceivers, New York: Kluwer Academic/Plenum Publishers, 1997.

[5] H. MEYR, M. MOENECLAEY, and STEFAN A. FECHTEL, Digital Communication Receivers, New York: John Wiley & Sons, Inc., 1998.

[6] Y. ERIC WANG and T. OTTOSSON, "Cell Search in W-CDMA," IEEE J. Select. Areas Commun., vol.18, No.8, August 2000.

[7] K. Fazel and S. Kaiser, Multi-Carrier and Spread Spectrum Systems, John Wiley & Sons Ltd., 2003.

[8] S. HARA and R. PRASAD, "Overview of multicarrier CDMA," IEEE Commun. Soc. Mag, vol. 35, pp. 126-133, Dec. 1997.

[9] S. Kondo and L. B. Milstein,"Performance of multicarrier DS CDMA systems," IEEE Trans. Commun., vol. 44, no. 2, pp. 238-246, Feb. 1996.

[10] J. TAN and G. L. STUBER, "Anti-jamming performance of multi-carrier spread spectrum with constant envelope," in Proc. IEEE ICC, 2003, pp. 743-747.

[11] D. C. CHU, "Polyphase codes with good periodic correlation properties," IEEE Trans. Inform. Theory, vol. 18, pp. 531-532, July 1972.

[12] J. G. PROAKIS, Digital Communications, McGraw-Hill, 4th Ed., 2000.

[13] A. WITTNEBEN, "A new bandwidth efficient transmit antenna modulation diversity scheme for linear digital modulation," in Proc. IEEE ICC, 1993, pp. 1630-1634.

[14] J. H. WINTERS, "The diversity gain of transmit diversity in wireless systems with Rayleigh fading," IEEE Trans. yeh. Technol, vol.47, pp. 119-123, Feb. 1998.

[15] S. M. ALAMOUTI, "A simple transmit diversity technique for wireless communica¬tions," IEEE J. Select. Areas Commun., vol. 16, pp. 1451-1458, Oct. 1998.