Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 8, August 2019

A REVIEW ARTICLE ON DIRECT SEQUENCE SPREAD SPECTRUM (DS-SS)

Dr. Krishnakant Singh
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id- ks.krishna@jainuniversity.ac.in

Abstract

Security has long been a challenging concern in wireless networks, largely because of the communication nature of broadcast. This opens up easy but efficient steps to prevent useful contact between radios that are legal. Spread spectrum technologies have been developed as effective countermeasures against, for instance, jamming attacks, such as direct sequence spread spectrum (DSSS). Using physical layer attributes, keyless DSSS mechanisms and watermarked DSSS (WDSSS) systems, this paper explores previous research on securing a DSSS channel even further. The former was motivated by the fact that the establishment and sharing of the hidden spread sequence between the transmitter and the receiver without being detected by adversaries is still an open issue. The basic concept of the above is to leverage the redundancy inherent in the spreading method of DSSS to embed information about watermarks. For an intelligent attacker who obtains the spread sequence to produce fake messages, it can be considered a counter measure (authentication). An adaptive DSSS scheme that takes into account both jam resistance and communication efficiency is also introduced and evaluated in this paper.

Keywords: *Pseudo Noise (PN), Spread Spectrum, Security, Wireless Network.*

I. INTRODUCTION

The demands for power efficiency for mobile devices and timely security services for complex wireless environments, along with the growth of wireless communication systems, have drawn considerable attention to physical layer security research[1]. Spread spectrum technologies were originally designed for this purpose, such as direct sequence spread spectrum (DSSS).

For eg, with pseudo noise (PN) sequences, DSSS spreads out the spectrum of the content signal to mimic white noise[2].

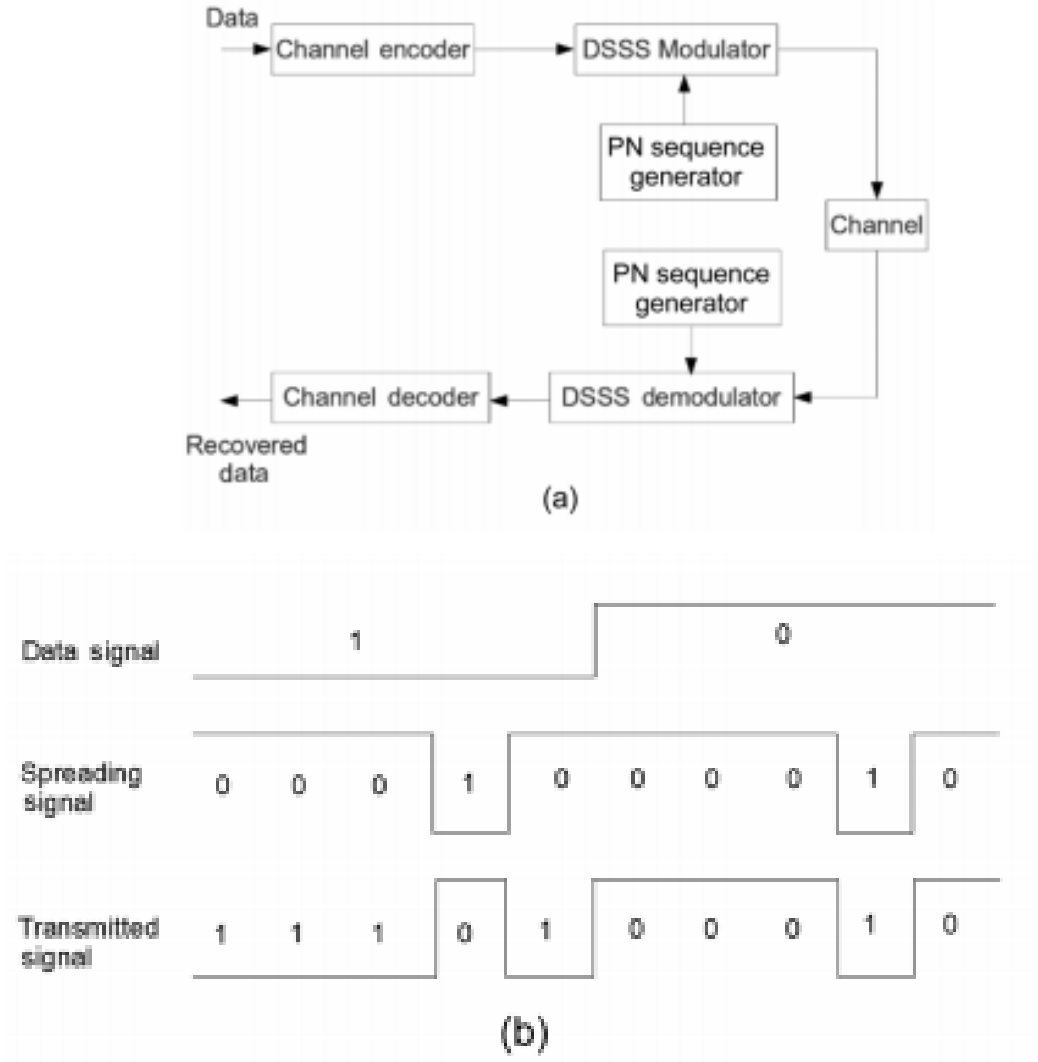

Fig. 1: Illustrates (a) Direct sequence spread spectrum (DSSS) prototypical (b) DSSS spreading operation; the pseudo noise (PN) sequence [3].

Thus, jamming resistance, intrusion denial, message privacy and a variety of other desirable properties are provided by the DSSS technique. For e.g., unless it knows the spread sequence, or the key and algorithm for generating the spread sequence, a jammer signal is not able to jam the wide-band signal. DSSS is commonly adopted in commercial wireless network standards, such as IEEE 802.11 and IEEE 802.15.4, to provide robust communications, specifically with the interference rejection property[4].

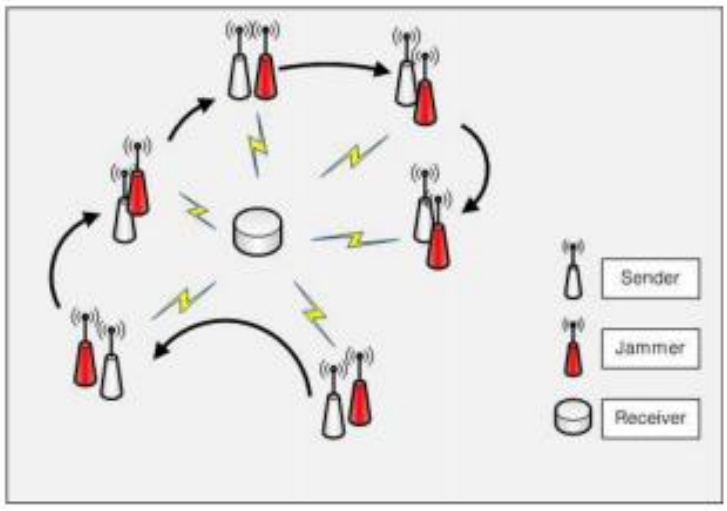

Fig. 2: Illustrates the 3 node scenario: the jammer chases and the sender[3].

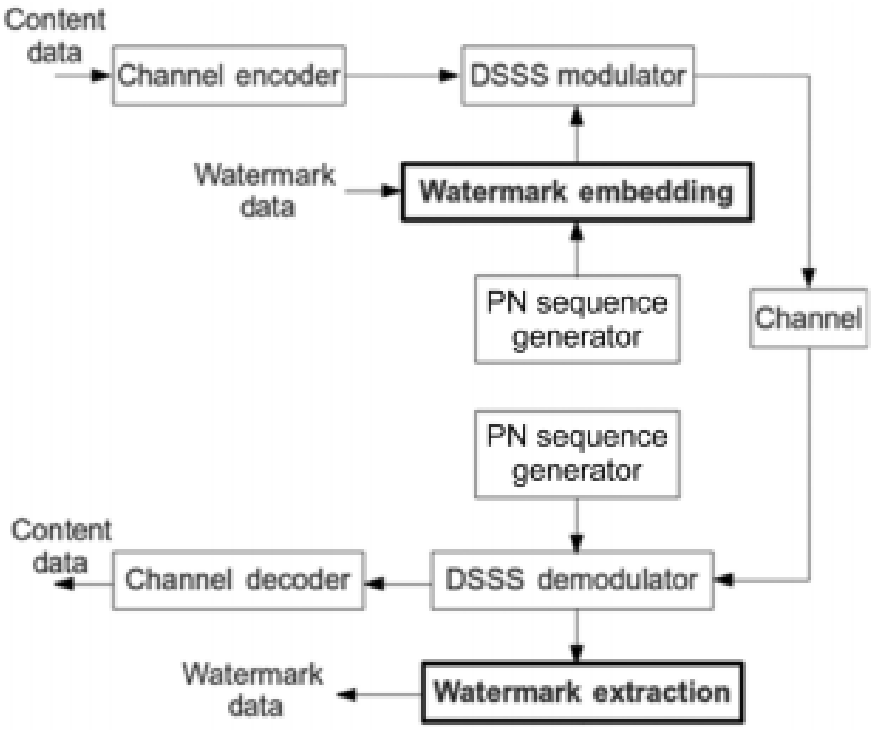

Fig. 3: Illustrates the Watermarked direct sequence spread spectrum (DSSS) system model[3].

In Figure 1 Direct sequence spread spectrum (DSSS) prototypical and DSSS spreading operation; the pseudo noise (PN) sequence is show, in Figure 2 the 3 node scenario: the jammer chases and the senderis shown and in Figure 3 the Watermarked direct sequence spread spectrum (DSSS) system model is shown.

II. LITERATURE REVIEW

Xu et al. conducted a survey on combined equalization and demodulation of chaotic direct sequence spread spectrum signals for multipath channels. Chaotic direct sequence spread spectrum (CD3S) signals have the benefits of a low likelihood of intercept (LPI) and a high degree of protection due to the inherent noise-like characteristics of chaotic signals and their sensitivity to the initial value. Therefore, demodulation of non-cooperated CD3S signals is a difficult problem. It is even more difficult for the receiver to demodulate it blindly if the signal is sent through multipath channels. We concentrate more on signals passing across multipath channels based on the current theories and methods [5].

III. DISCUSSION AND CONCLUSION

With the growing use of wireless communication, the provision of reliable and robust communications in the presence of attackers is becoming more critical. This paper discusses many DSSS-based physical layer techniques. Since a shared spread sequence between the sender and the receiver is still difficult to establish, Section IV addresses previous work in addressing this issue. This paper also introduces an adaptive modulation and anti-jamming method where the sender and the receiver adaptively modify the modulation scheme and spread the duration of the series with the change in the condition of the channel. Because they experience the same channel, this can be used to deduce the same spread series length separately, which is an additional hurdle for the jammer, since a different channel is encountered.

IV. REFERENCES

[1] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[2] E. N. Kumar and E. S. Kumar, “A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach,” 2013.

[3] T. Kang, X. Li, C. Yu, and J. Kim, “A Survey of Security Mechanisms with Direct Sequence Spread Spectrum Signals,” J. Comput. Sci. Eng., 2013, doi: 10.5626/JCSE.2013.7.3.187.

[4] H. Dai and Y. Zhang, “A real orthogonal space-time coded uwb scheme for wireless secure communications,” Eurasip J. Wirel. Commun. Netw., 2009, doi: 10.1155/2009/571903.

[5] X. Xu and J. Guo, “Combined equalization and demodulation of chaotic direct sequence spread spectrum signals for multipath channels,” Circuits, Syst. Signal Process., 2013, doi: 10.1007/s00034-013-9599-y.

ISSN: 0374-8588
Volume 21 Issue 8, August 2019