International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 11, Issue 02 (February 2015), PP.74-78

Contemporary Spread Spectrum Techniques: A Comparative Study

Ashish G. Nandre [1], Yogesh R. Risodkar [2]
[1]*MET's IOE, BKC, Nashik..*
[2]*Sandip Institute of Engineering & Management, Nashik*

Abstract:- Anti-jamming is an important problem in broadcast communication. In this paper , we provide an overview of recent contributions pertaining to the anti-jamming techniques. Specifically, the paper focuses on comparative study of anti-jamming techniques' performance against jammers. Due to secret key sharing between sender and receiver in classical Spread spectrum techniques, Anti-jamming Broadcast problem arises. To have jamming resistant communication, Uncoordinated SS, Randomized differential-DSSS, Quorum Rendezvous Channel Hopping are proposed and implemented in the respective domain of communication. From the discussion provided in this paper, it is concluded that the brief review of anti-jamming techniques can help the researchers to understand the functionality and practical applications of the techniques based on DSSS and FHSS.

Keywords:- DSSS, FHSS, QRCH, UDSSS, UFH-DSSS, Jammers.

I. INTRODUCTION

Traditional communication systems require less power for transmission and bandwidth usage is efficient. But, these systems are not immune to jamming. Hence at the cost of more bandwidth and higher power usage for transmission, the Spread Spectrum Techniques provides excellent immunity to all sorts of jamming. Besides this, SS Techniques possess following advantages:

- Ability to selectively address
- Bandwidth sharing
- Security from eavesdropping
- Difficulty in detection
- Resistance to fading

But these techniques undergoes anti-jamming broadcast problem due to pre sharing of secret keys between sender and receivers. To have remedy on this problem the Anti-jamming techniques are proposed in this paper which gives the best performance against the specific jammers.

MOTIVATION:

Spread spectrum techniques use data independent, random sequences to spread a narrow band information signal over wideband of frequencies. It is hard or infeasible for an attacker to jam the entire frequency band; the receiver can correlate the received signal with replicate of the random sequence to retrieve the original information signal. Important instances of spread spectrum techniques are Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS).In traditional Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS) based communication, the sender and the receiver share a secret prior to their communication which enables the receiver to generate the random sequence and to detect and decode the sender's spread signal. This reliance on a pre-shared secret generally precludes unanticipated transmission between unpaired devices as well as communication from a sender (or a base station) to an unknown set of receivers. This problem is known as the anti jamming broadcast problem. This leads to an anti-jamming/key establishment dependency cycle.[1]

II. LITERATURE REVIEW

In adversarial conditions, following types of jammers can jam the communication: Random, Sweep and Static jammers can jam the channel permanently without sensing the ongoing transmission messages. These jammers can be distinguished by regularity of their jamming signals. Reactive jammers sense the ongoing transmission and with acknowledgement of message transfer they start jamming. Repeater jammers are a subclass of reactive jammers that intercept the signal (especially DSSS) , low noise amplify, filter and retransmit it on the channel(knowledge of used spreading codes is not necessary). Combination of the above types is the Hybrid jammers which jam the channel during the search of message transmissions.[1]

To address the Anti-jamming broadcast problem and immunity against interferences; some researchers have provided the solutions like Uncoordinated Spread Spectrum (USS) [1], Randomized Differential DSSS

(RD-DSSS) [2]. The solutions like Quorum Rendezvous Channel Hopping (QRCH) and Dual Code-DSSS (DC-DSSS) help to find pattern for hopping sequence and better encryption of spreading codes in FHSS and DSSS respectively.

USS Techniques:

UDSSS, UFHSS, UFH-DSSS are instances of USS techniques and based on SS techniques in that they spread the information signal over a frequency band that is much larger than the band required for transmission of information signal. In USS, the sender uses the public set C:={c_1,c_2,….,c_n} of communication channels within the available frequency band instead of a pre-agreed spreading sequence. This set C is known to all receivers. In UFH and UDSSS, the communication channels are frequency channels and spreading code sequences respectively. The sender secretly chooses the transmission channel among C and receivers try to predict the sender's selected channel to receive the message during the acceptance of delay in the reception of repeatedly transmitted messages (Figure 1). The repeated transmission of messages enables receivers to get synchronized and receive the messages successfully even in jamming conditions.

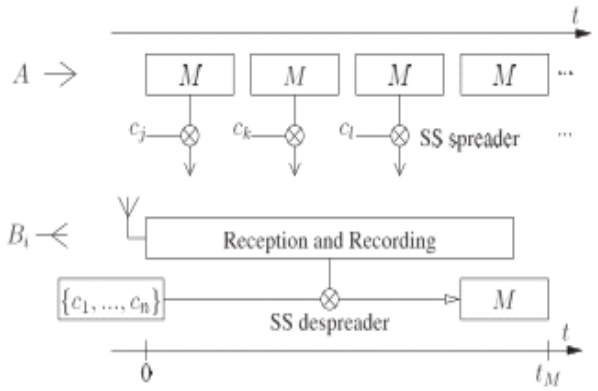

Fig.1: The basic principle of USS Techniques [1].

Uncoordinated DSSS (UDSSS):

In UDSSS techniques user utilizes fresh spreading code randomly. Therefore it is hard to predict the code for jammers. The code sequences are used to spread the entire message, hence, no need of fragmentation and reassembly at sender and receivers is not required. On the contrary more time is required to receive the data because the channel gets recorded and UDSSS efficiency depends on balanced spreading codes with good auto cross correlation properties.

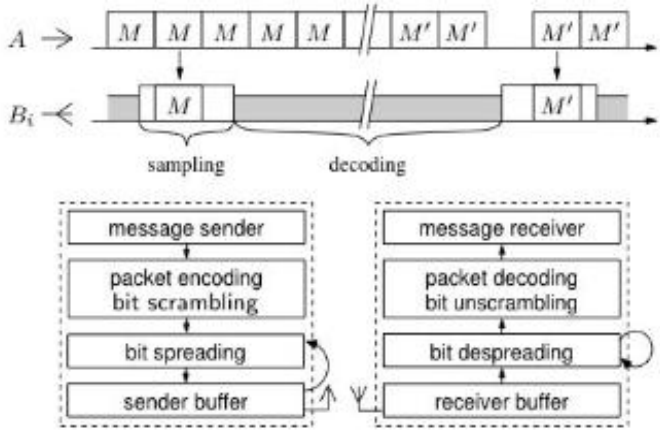

Fig.2: UDSSS: The sender A spreads and transmit the message using randomly selected spreading codes ; the receiver records the channel and subsequently try to identify the used spreading sequence to decode the message [1].

Uncoordinated FHSS (UFHSS):

In UFHSS the jammer's chances to jam the right channel decreases if more numbers of channels are used. But due to fragmentation of messages the reassembly is not that much easy at receiver. The fragmentation allows jammers to insert his own messages to jam the channel.

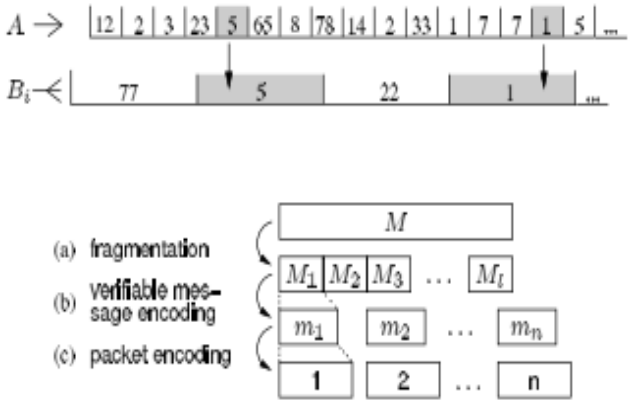

Fig.3: UFHSS: The sender A and each receiver B_i choose the channels on which they send and listen randomly from the set C of available frequency channels respectively. Messages are too long to fit on the one frequency hop and are thus fragmented, message encoded and packet encoded by sender; after reception, the messages are reassembled and verified at the receiver [1].

In uncoordinated FH-DSSS the spreading code and the carrier frequency is selected randomly from the predefined set for message transmission. First the spreading process takes place on signal and then it is fed to frequency hopper which chooses random frequency channel. At the receiver exactly reverse procedure takes place. The advantage of UFH-DSSS is that it provides low probability of intercept and frequency diversity over a large spectrum. Requirement of advanced technique to receive the originally transmitted signal makes UFH-DSSS stronger against reactive jamming attacks.

Randomized Differential DSSS:

In RD- DSSS the sender and the receiver share spreading code set in which there should be low correlation between two codes selected randomly. A sender encodes each bit of data using the correlation of two unpredictable spreading codes. Bit '0' is transmitted with two different spreading codes having low correlation with each other and bit '1' is spread using two identical spreading codes with high correlation. The correlation between two codes for each bit (High correlation => Bit '1'; Low correlation => Bit '0' at the time of de-spreading at the receiver. For reducing the communication overhead each code sequence is associated with a special coding code called a Index code. It is advisable that the correlation between two index codes is low. The index code set and spreading code set should have no overlap for distinguishing index code and a regular spreading code.

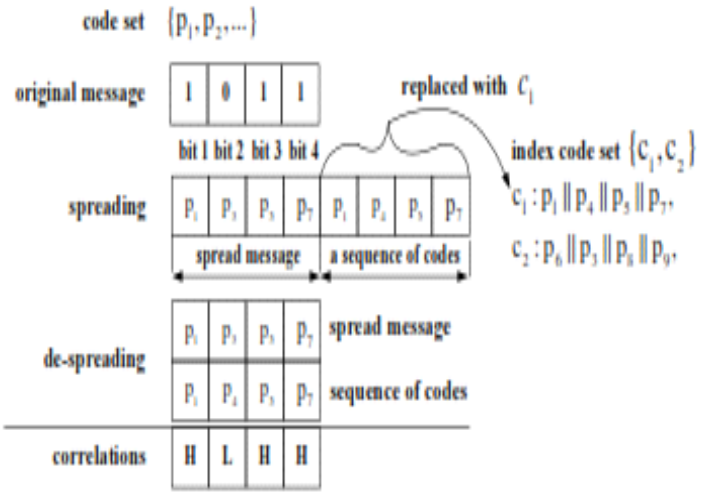

Fig. 4: RD-DSSS Basic Scheme [2].

In RD-DSSS since the correlation properties of spreading code are utilized, the intellectual jamming attacks can be removed. But, due to storage of spreading as well as index code the communication overheads of RD-DSSS are high [2].QRCH is the technique which is utilized to select the hopping sequence in PCH (Pseudo

random channel/ frequency hopping) system. The hopping sequences are constructed using Quorum system which guaranties the nodes to meet within bounded amount of time in WSN [5]. In Dual code DSSS the spreading code is encrypted and decrypted at sender and receiver end respectively which gives security against hijacking of the spreading codes [6].

III. PERFORMANCE ANALYSIS OF ANTI-JAMMING TECHNIQUE

Table I Comparison of Anti-jamming Techniques

Anti-jamming Techniques	USS Techniques	RD-DSSS
Message Integrity	USS Techniques require measures that check the integrity of the messages. Specifically, UDSSS (UFH) requires the messages (packets) are identifiable and the bit modification can be detected. UFH further requires that fragments which belong to the same message can be efficiently identified.	RD-DSSS requires the check for message integrity against the presence of reactive jammers.
Authenticity\ Confidentiality	Message authentication or confidentiality are not general part of USS techniques but can be achieved on the application layer which runs on the top of the USS schemes e.g. by making use of public key cryptography, timestamps and message buffering.	Message authenticity depends upon to what extent the public information is captured by the jammers.
Efficiency	Although the message latency under jamming is longer for USS techniques than the coordinated counterparts, the same message latency as SS communication can be achieved in absence of jamming.	RD-DSSS efficiency affected by the computations of correlations to identify the index codes, storage overheads due to spreading code storage and communication overhead due to appending the index code along with message body.
Applications	Anti-jamming Navigation Broadcast, Anti-jamming Emergency alerts, Bootstrapping SS Communication.	It's a theoretical simulation based technique inspired by UDSSS and can be used efficiently against reactive jamming attack.

IV. CONCLUSION

In this paper, the comparative study of three main Anti-jamming Techniques, viz, UDSSS, UFHSS and RD-DSSS are compared. These techniques are basically dependent on coordinated SS in case of spreading the message but differ in the method of choosing the communication channels. The techniques exhibit different properties against different jammers, i.e., RD-DSSS deals effectively against reactive jamming attacks. . DC-DSSS[6] is the extension to traditional SS with additional encoding of the barker code. The other techniques like ZPK-DSSS [7] tells the concept like intractable forward decoding and efficient backward decoding along with key scheduling method. Baird et al. in [8] represented BBC algorithm for achieving the same level of jamming resistance as traditional spread spectrum, at under half the bit rate with no shared keys. These are the contemporary Anti-jamming Techniques.

REFERENCES

[1]. Popper C., Mario strasser, Srdjan Capkun. "Anti-jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques" in IEEE Journal on selected areas in Communication, Vol. 28 No.5, pages 703-715, June 2010. Doi: 10.1109/JSAC.2010.100608.

[2]. Yao Liu, Peng Ning, Huaiyu Dai, An Liu. "Randomized Differential DSSS: Jamming Resistant Wireless Broadcast Communication" in Proceedings of IEEE international Conference on Computer Communication (INFOCOM), 2010.

[3]. Popper C., Mario strasser, Srdjan Capkun."Jamming-resistant Broadcast Communication without Shared Keys" in ETH-Zurich INFK-Tech.Report 609, March 2009.

[4]. Mario Strasser. "Novel Techniques for Thwarting Communication Jamming in Wireless Networks", A dissertation submitted toETH ZURICH for the degree of Doctor of Sciences,2009.

[5]. Eun Kyu Lee, Soon Y. Oh and Mario Gerla. "Randomized Channel Hopping Scheme For Anti-jamming Communication", in the poster session of ACM MobiCom, 2010.

[6]. Rahat Ullah and Shahid Latif.” Improving the security level in Direct Sequence Spread Spectrum using Dual Code DSSS (DC-DSSS) “ in International Journal of Security and its Applications, Vol 6 No 2,pages 133-136,April 2012.

[7]. Tao Jin,Guevera Noubir.” Pre-shared Secret Key Establishment in Presence of jammers” in MobiHoc09, Orleans, Louisiana, USA, May 2009.

[8]. Baird III L., Bahn W., Collins M., Carlisle M. " Keyless Jam Resistance" in the proceedings of the Workshop on Information Assurance, United states Military Academy, West point, New York, USA, 20-22 June 2007.