This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

Feasibility Assessment of Repeater Jamming Technique for DSSS

Hang Wang, Jingbo Guo, *Member, IEEE* and Zanji Wang, *Senior Member, IEEE*
Department of Electrical Engineering, State Key Lab of Power System, Tsinghua University
Beijing 100084, China
wanghang99@mails.tsinghua.edu.cn

Abstract—**Direct sequence spread spectrum (DSSS) systems spread the baseband data signal over a broad bandwidth to achieve anti-jamming protection, which increase the difficulty of spectrum surveillance. The current jamming types, including broadband noise, partial-band noise and so on, are ineffective at the current jamming power level when the processing gain is large enough. This paper proposes a new jamming scheme named repeater jamming, which is based upon radio frequency memory (RFM). The jamming effect of repeater jamming on victim receiver's code acquisition and the bit error probabilities are obtained. Moreover, the feasibility of the repeater jamming in practical communications is discussed. The results of simulation show the deduction is right. The repeater jamming proposed in this paper is a kind of correlative jamming types which are more effective than current jamming types, and it can be used to enhance distributed networked jamming systems in the field of DSSS communication countermeasures besides the commercial frequency surveillance.**

Keywords-DSSS;RFM;Repeater jamming; Security

I. INTRODUCTION

The benefits of frequency hopping spread spectrum (FHSS) are potentially neutralized by a repeater jammer (also known as a follower jammer), which has been investigated for more than ten years. The repeater jamming technique for FHSS has been used in both military communications and commercial communications [1]-[3]. In contrast to this, any power-effective jamming technique used in direct sequence spread spectrum (DSSS) has not been proposed in public literatures. Meanwhile, the current jamming types are ineffective at the current jamming power level when the processing gain is large enough. So it's necessary to investigate a new power-effective jamming technique for the purpose of both commercial frequency surveillance and military countermeasures.

The principal types of jamming on DSSS signals include broadband noise (BBN) jamming, partial-band noise (PBN) jamming, pulsed jamming and tone jamming. The last of these includes both single tone jamming and multiple tones (MT) jamming. The effectiveness of these jamming types is not good, because they are non-correlative jamming types which can not synchronize PN sequences. In order to achieve desired jamming effectiveness, the jammer has to increase power level of jamming signals. Unfortunately the victim receiver will countermine the strong jamming signals with adaptive notch filters, repeat coding and so on [4], [5].

In order to improve the coverage and capacity in cellular networks, repeaters are broadly used as a cost-effective engineering solution [6], [7]. The principle of transparent repeater used in cooperative communications could also be used in the process of repeater jamming design. Reference [8] proposed a design of repeater jamming against DSSS, which is based on radio frequency memory (RFM). RFM is widely applied in simulating target signals, which has been well established in western countries. It is the hardcore of repeater jamming and key field of electronic counter-measures technology.

The rest of the paper is organized as follows: in Section Ⅱ, we present some current jamming types and describe the design of repeater jamming based on RFM in brief. Section Ⅲ analyzes the receiver operating characteristic (ROC) performance in the presence of such repeater jamming; the bit error rate (BER) performances in both non fading environment and Rayleigh fading environment are also given in Section Ⅲ. Next, in Section Ⅳ simulation results are demonstrated and the feasibility of such repeater jamming in practical communications is discussed. Finally, a conclusion wraps up this paper.

II. CURRENT JAMMING AND REPEATER JAMMING DESIGN

The idealized model of passband DSSS system could almost be found in any textbook on wireless communications. Because the bit error performances for BPSK and QPSK are the same and BPSK is the most prolific modulation type for DSSS systems, only the case of BPSK data encoding and bi-phase spreading is discussed in this paper. The general form of the received signal being considered here is as follows:

$$r(t) = \sqrt{2R}d(t-\delta)p(t-\delta)\cos(\omega_c t+\theta_0) + j(t) + n(t) \quad (1)$$

where $d(t)$ represents the data signal, $p(t)$ represents spreading codes, $j(t)$ represents the intentional jamming signal and $n(t)$ represents the noise. The average power of the spread signal is R and δ denotes the time delay. ω_c is the carrier frequency and θ_0 denotes the initial phase angle which could be assumed to be zero.

BBN jamming of DSSS systems is when the jamming signal is noise with a bandwidth W_{ss} approximately the same as the DSSS signal. For rectangular pulse shapes and BBN jamming, the bit error performance is given by [5]

$$P_e = Q\left(\sqrt{\frac{2N}{\frac{1}{\upsilon}+\xi}}\right) \tag{2}$$

where N is the number of chips per data bit , ξ denotes the jamming-to-signal ratio (JSR) and υ denotes the signal-to-noise ratio (SNR). Because the width of band pass filter at receivers could be assumed equal to the bit rate, υ could denote $\frac{E_b}{N_0}$. This is the familiar result for BPSK modulation in the presence of thermal noise, where the thermal noise level has been increased by the BBN jamming. The BER performances of DSSS under several non-correlative jamming types are given in [5]. For details, I refer readers to [5].

All the non-correlative jamming types have two serious disadvantages:

First, the non-correlative jamming types remain relatively ineffective until the processing gain is overcomed. The jammer will need extreme power to overcome the processing gain when the processing gain is large enough (approximate 20dB for IS95). However, it is hard to achieve in some practical communication environments.

Second, many methods of interference rejection have been investigated, which can enhance the receiver anti-jam properties. For example, adaptive interference mitigation, including notch filters, prediction filters and so on, had an obvious effect on rejection of narrowband noise. Repeat coding is also effective against pulse jamming. Moreover, a high-power hostile jamming could be detected by radars.

Reference [9] introduced several different configurations of repeater used in cooperative communications, which could also be used to design a repeater jammer. Because the processing time is an important factor for a jammer, which will be analyzed in Section Ⅳ . And the processing time of conventional repeaters is not satisfying, a novel design is necessary to achieve a lower processing time.

The structure of the repeater jamming generating system depicted on Fig.1 is based on RFM. As shown in this diagram, the signal is intercepted through the air via a repeater's donor antenna. It is then low noise amplified, filtered, down-converted to IF, quantized by suitable A/D converter, stored in memories, and re-radiated through the repeater's coverage antenna by appropriate signal processing, associated D/A conversion, and up-converter. For bi-phase DSSS, the jamming waveform could simply be a reverse replica of the intercepted signal, which can be called an intentional echo of intercepted signal. The waveform, which contains DSSS signal and noise, is too similar to the desired signal at the victim receiver to cause sufficient jamming because the receiver may sometimes make wrong decisions by responding to the jamming signal as if it was the desired signal. Compared with the simplest form mentioned in [9], this design could achieve processing time as low as $0.1\,\mu s$.

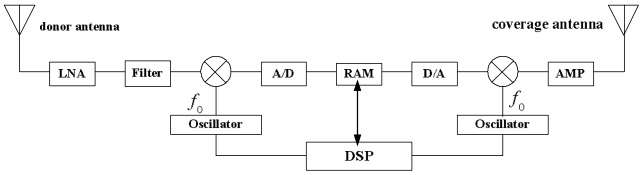

Figure 1. Block diagram of repeater jamming based on RFM.

III. Performance Analysis

When the victim receiver encounters the repeater jamming, the received signal should contain a replica of spread signal.

$$\begin{aligned} r(t) = & \underbrace{\sqrt{2R}d(t-\delta)p(t-\delta)\cos(\omega_c t)+n_1(t)}_{intercepted\ signal} \\ & \underbrace{-\sqrt{2P_J}d(t-\delta^{'})p(t-\delta^{'})\cos(\omega_c t+\theta)+n_2(t)}_{repeater\ jamming\ signal} \end{aligned} \tag{3}$$

where P_J is the average power of the spread signal transmitted by a repeater jammer, $\delta^{'}-\delta$ is the arrival-time delay of the jamming relative to the desired signal at the victim receiver. θ is the phase difference, which normally could be assumed a uniform random variable $[0,2\pi]$. In [8], P_J is assumed equal to R for simplicity. However, this is an idealized assumption which could not be satisfied in practical environments.

First, the power of the original spread signal could be measured in cooperative communications, while this is hard to be done for a jammer. Second, a repeater jammer receives and reradiates signal on the same channel frequency. To avoid instability caused by a feedback loop, the isolation between the donor antenna and the coverage antenna is necessary. However, perfect isolation can never be achieved which should be considered. Third, the fading should be considered in some areas such as insides of buildings, dense urban district and so on. That means the power of a jamming signal received at victim receiver can not be constant even though the output power of the jammer is maintained constantly. Considering these reasons, a new coefficient β is introduced into (3). And (3) can be rewritten as

$$\begin{aligned} r(t) = & \sqrt{2R}d(t-\delta)p(t-\delta)\cos(\omega_c t) \\ & -\beta\sqrt{2R}d(t-\delta^{'})p(t-\delta^{'})\cos(\omega_c t+\theta)+n(t) \end{aligned} \tag{4}$$

where $\beta=\sqrt{\frac{P_J}{R}}$ denotes the square root of power ratio, $n(t)$ is AWGN with double-sided psd $\frac{1+\beta^2}{2}N_0$.

A. Effect on Code Acquisition

Compared with code tracking, initial code acquisition in a spread spectrum system is usually more difficult. In this section, the victim receiver is assumed to achieve perfect carrier synchronization. The decision statistic is then

$$
\begin{aligned}
z &= \frac{1}{2T_b^{\,2}}\left|\int_{T_b} r(t)m(t-\hat{\delta})dt\right|^2 \\
&= \left|\sqrt{\frac{R}{2}}(R_{mm}(\delta-\hat{\delta})-\beta\cos\theta R_{mm}(\delta^{'}-\hat{\delta}))+\frac{1}{\sqrt{2}T_b}\int_{T_b} n(t)m(t-\hat{\delta})dt\right|^2
\end{aligned} \qquad (5)
$$

where $R_{mm}(\tau)$ is the autocorrelation function of $m(t)$. If an m-sequence with period N is used, then $R_{mm}(\tau)$ is

$$
R_{mm}(\tau)=\begin{cases} 1-\dfrac{N+1}{N}\dfrac{|\tau|}{T_c}, & |\tau|\le T_c \\ -\dfrac{1}{N}, & otherwise \end{cases} \qquad (6)
$$

From (5), it is easy to see that under the two hypotheses

$$
\begin{aligned}
H_0 : z &= \left|\frac{1}{\sqrt{2}T_b}\int_{T_b} n(t)m(t-\hat{\delta})dt\right|^2 \ \ phase\,not\,match \\
H_1 : z &= \left|\sqrt{\frac{R}{2}}(1-\beta\cos\theta\frac{T_c-\tau}{T_c})+\frac{1}{\sqrt{2}T_b}\int_{T_b} n(t)m(t-\hat{\delta})dt\right|^2 \ \ match
\end{aligned} \qquad (7)
$$

Assume $T_c \ll T_b$, γ denotes the decision threshold. The false alarm probability P_{fa}, is given by

$$
P_{fa}=P_r(z>\gamma\,|\,H_0)=\exp(-\frac{\gamma T_b}{(1+\beta^2)N_0}). \qquad (8)
$$

Denoting $\tau=\delta^{'}-\delta<T_c$, the miss probability P_m, is given by

$$
\begin{aligned}
P_m &= P_r(z\le\gamma\,|\,H_1)=\int_0^{\sqrt{\frac{\gamma T_b}{N_0}}} u\exp(-\frac{u^2+2\upsilon^{'}}{2})I_0(\sqrt{2\upsilon^{'}}u)du \\
\upsilon^{'} &= (\sqrt{\frac{R}{2}}(1-\beta\cos\theta\frac{T_c-\tau}{T_c}))^2 T_b/((1+\beta^2)N_0)
\end{aligned} \qquad (9)
$$

where $\upsilon^{'}$ is the modified SNR, $I_0(\cdot)$ is the zeroth order modified Bessel function of the first kind.

B. BER Performance

Let us first consider the error probability in non fading environment. The coefficient β could be considered as a constant when the received signal at the victim receiver is dominated by line-of-sight (LOS) component, and the channel degrades to a pure Gaussian channel. In such situation, the coefficient β stands for all the factors including repeater's forward gain, distorting caused by non perfect isolation and so on.

For binary phase-shift keying, the bit error probability could be increased in the presence of repeater jamming, because of both the input SNR's reduction and intentional polarity inversion if possible. The bit error possibility may be larger than 50 percent in case the polarity is inversed by repeater jamming. However, this case will never happen because differential encoding is used to protect against phase ambiguity. Considering differential encoding, the probability of a bit error is

$$
P(e\,|\,\theta)=Q\left(\sqrt{\frac{2N\upsilon(1-\beta\cos\theta\frac{T_c-\tau}{T_c})^2}{1+\beta^2}}\right) \qquad (10)
$$

It should be noticed that the jamming effectiveness depend on the phase of the jamming signal relative to that of the target signal. The average probability of error is calculated by integrating over θ.

Time varying multipath causes fading of the received signal in a wireless mobile environment. A single-ray channel model is assumed here. The envelope of the fading signal is Rayleigh distributed which means β satisfies the following probability density function.

$$
p(\beta)=\frac{\beta}{\sigma^2}\exp(-\frac{\beta^2}{2\sigma^2}) \quad (0\le\beta\le\infty) \qquad (11)
$$

where $\sigma=E[\beta]/1.2533$. Therefore, the BER in Rayleigh fading environment is

$$
P(e\,|\,\theta)=\int_0^{\infty}\frac{\beta}{\sigma^2}\exp(-\frac{\beta^2}{2\sigma^2})Q\left(\sqrt{\frac{2N\upsilon(1-\beta\cos\theta\frac{T_c-\tau}{T_c})^2}{1+\beta^2}}\right)d\beta \qquad (12)
$$

There is no known closed-form solution to this integral so it must be evaluated numerically. The simulated results are given in Section Ⅳ.

IV. Simulation Results and Discussion

Comparison of receiver operating characteristic (ROC) performances in the presence of BBN and repeater jamming is illustrated in Fig.2. The coefficient β is set to be 3dB, the τ is set to be 75 percent of a chip duration and θ is set to be $\pi/4$. It's easy to see that repeater jamming is severer than BBN in the process of code acquisition. The result could be explained

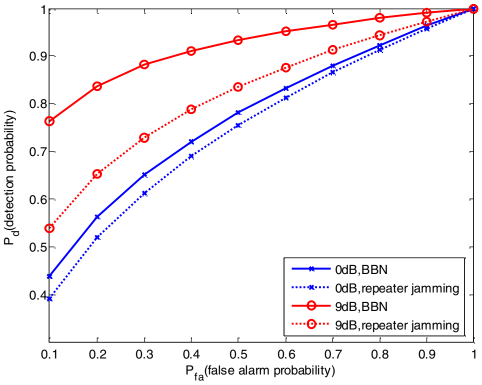

Figure 2. Comparison of ROC performance in the presence of BBN and repeater jamming (β =3dB, $\tau=0.75T_c$, $\theta=\pi/4$).

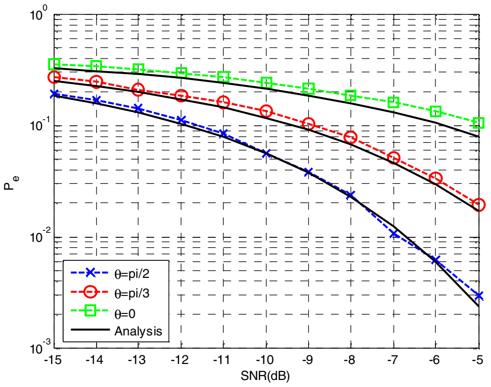

Figure 3. BERs in the presence of repeater jamming at different θ ($\beta =$ 3dB, $\tau = 0.75T_c$).Simulated BERs are plotted as dashed lines and analytical BERs are plotted as solid lines.

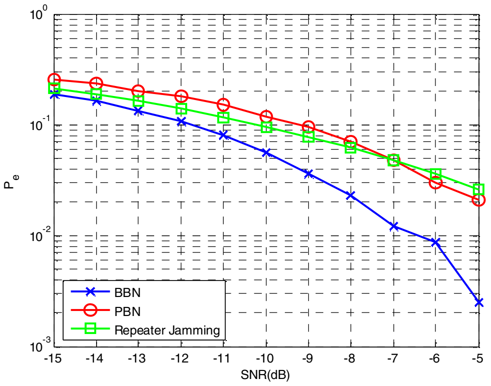

Figure 4. Comparison of simulated average BERs in the presence of BBN, PBN and repeater jamming by averaging over θ ($\beta =$3dB, $\tau = 0.75T_c$).

that repeater jamming signal contains the intentional echo of intercepted signal, which keep the property of high correlation with original spread signal.

BERs at different values of θ are illustrated in Fig.3. It could be seen that $\theta = 0^\circ$ yields the best jamming effect, while the repeater jamming degrades to BBN jamming with $\theta = 90^\circ$. The analytical BERs are also plotted which are obtained from the expression (10). From the figure, the consistency between the analytical results and the simulated results is evidenced.

Being justified, Fig.4 depicts the comparison of average BERs over θ in the presence of BBN, PBN and repeater jamming. If τ can be assumed a uniformly distributed random variable in $[0, T_c]$, the total BERs can be calculated and illustrated in Fig.5. Comparison of average BERs in Rayleigh fading environ-ment is given in Fig.6. The results show that the jamming effect of repeater jamming outperforms that of BBN jamming. The repeater jamming and PBN jamming have comparable jamming performance.

As mentioned in Section Ⅱ, techniques have been investigated for suppression of the effects of PBN jamming [10]; however, the repeater jamming is a correlative broadband jamming type, which can not be suppressed by such techniques. Moreover, for the limitation of time resolution, the repeater jamming can not be seemed as new fingers by Rake receivers to improve the victim receiver's performance inside its jamming range.

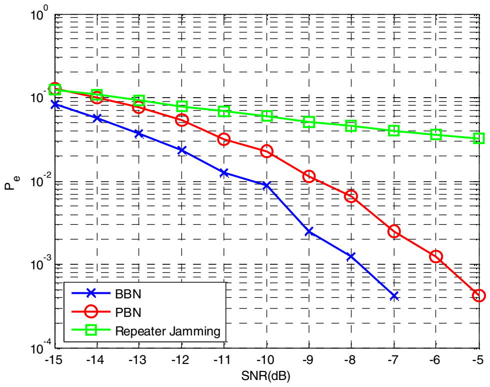

Figure 5. Comparison of simulated total BERs in the presence of BBN, PBN and repeater jamming ($\beta =$0dB).

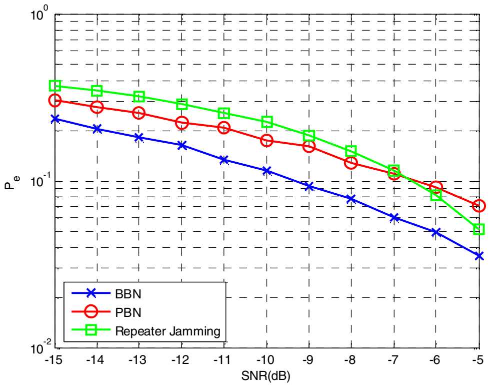

Figure 6. Comparison of average BERs in Rayleigh fading environment ($E[\beta] =$3dB, $\tau = 0.75T_c$).

Several questions should be mentioned to assess the feasibility of repeater jamming, while three of them are discussed in this section.

A. Jamming Range

Fig.7 depicts the geometrical jamming scenario [1]. If relative time delay τ exceeds chip duration, the repeater jamming signal becomes a non-correlative jamming. In other words, for the repeater jamming to be effective, we must have

$$\tau = \frac{D_{TJ} + D_{JR} - D_{TR}}{c} + T_{rep} \le T_c \qquad (13)$$

where c is the speed of propagation, T_{rep} is the processing time required by the jammer which could be less than $0.1\mu s$, T_c is the chip duration. According to the inequality, the maximum jamming ranges for different communication scenarios including commercial communications and military communications can be calculated. Here they are listed in Table. Ⅰ. For instance, if $T_c = 1/1.2288\mu s$ (used in IS95), then

$$\begin{aligned} D_{TJ} + D_{JR} - D_{TR} &\le (T_c - 0.1\mu s)\cdot c \\ &\approx 214m \end{aligned} \tag{14}$$

That means, if the difference in distance between the indirect transmitter-to-jammer-to-receiver path and the direct transmitter-to-receiver path exceeds 214m, then the repeater jamming will be ineffective for IS95. It could be seen that in commercial communications, the repeater jamming can be used to disable mobile phones in designated areas; while in military communications, the repeater jamming can also disables the personal role radio (PRR). Moreover, as a close-approach correlative jamming, the repeater jamming could be used to enhance the WolfPack which is a distributed networked jamming system proposed by Defense Advanced Research Projects Agency (DARPA).

B. Rake Receivers

A Rake receiver is used in almost all the DSSS systems. If the multipath components (MPCs) are delayed in time by more than one chip duration, it attempts to collect these time-shifted versions of the original signal by providing a separate correlation reveiver for each of the multipath signals. However, the SNR of each finger could be decreased by the repeater jamming. The performances of all the Rake receivers, including conventional Rake receivers, selective Rake receivers and partial Rake receivers, are degrades by such repeater jamming.

C. Area outside Jamming Range

Considering Rake receivers, the repeater jamming signals may be seemed as new fingers if the victim receiver goes outside the jamming range. Obviously it's not an anticipant result from a jammer's view. When the repeater jamming is used in the field of commercial frequency surveillance, the target is to disables the normal operation of mobile phones present in a closed area. The closed area could probably be a concert hall or a meeting room. The repeater jamming signals at victim receivers outside the closed area will not be as strong as fingers because of the attenuation due to the walls. The situation is worse in outdoor environment. It is strongly suggested that the repeater jamming should work in non continuous state. Like a pulsed jamming, the repeater jamming transmits signals for a while and is off for the next fraction of the time. From the victim receiver's view, it is difficult to deal with the repeater jamming signals as steady fingers.

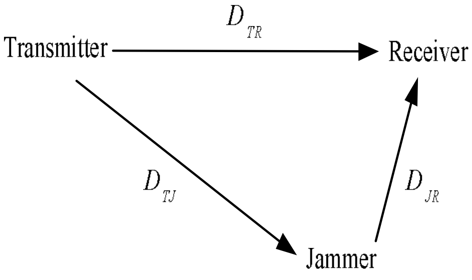

Figure 7. Geometrical jamming scenario.

TABLE I. MAXIMUM JAMMING RANGE FOR DIFFERENT COMMUNICATIONS

	Commercial Communications		**Military Communications**
	CDMA2000/IS95	***WCDMA***	***PRR[1]***
Maximum Jamming Range	214m	48m	570m

[1] PRR: Personal Role Radio, a short-range DSSS communication system, which has been armed in more than twenty countries' armies.

V. CONCLUSION

Just as DSSS systems increase the difficulty of spectrum surveillance, so has the importance of investigating a new power-effective jamming type. The new jamming type, referred to here as the repeater jamming, keeps the property of high correlation with original spread signal to affect both code acquisition process and bit error performance.

In order to assess the feasibility of such repeater jamming, three practical questions are discussed. All these results show that the repeater jamming is a promising alternative to existing jamming types at current jamming power level. And it fulfils the practical systems' demands, which can be used to enhance distributed networked jamming systems besides the commercial frequency surveillance.

ACKNOWLEDGMENT

The authors would like to thank K.Salehian for helpful information on repeaters used in digital television broadcasting service. They would also like to thank B.Agee for many fruitful discussions about wireless security.

REFERENCES

[1] D.J.Torrieri, "Fundamental limitations on repeater jamming of frequency-hopping communications," *IEEE J. Sel. Areas Commun*, vol. 7, pp.569-575, 1989.

[2] L.P.Riddle, "Performance of a hybrid spread spectrum system against follower jamming," *Proc. IEEE MILCOM 1990*, vol.1, pp.420-424, 1990.

[3] J.M.Pousada-Carballo, F.J.Gonzalez-Castano, F.Isasi de Vicente, and M.J.Fernandez-Iglesias, "Jamming system for mobile communications," *IEEE Electronics Letters*, vol.34, pp.2166-2167, 1998.

[4] L.B.Milstein, "Interference rejection techniques in spread spectrum communications," *Proceedings of the IEEE*, vol. 76, pp. 657-671, 1988.

[5] R.A.Poisel, Modern Communications Jamming Principles and Techniques, Norwood: Artech House, 2004.

[6] M.Rahman, and P.Ernstrom, "Repeaters for Hotspot Capacity in DS-CDMA Networks," *IEEE Trans. Veh. Technol.*, vol.53, no.3, pp.626-633, May 2004.

[7] M.N.Patwary, P.B.Rapajic, and I.Oppermann, "Capacity and Coverage Increase With Repeaters in UMTS Urban Cellular Mobile Communication Environment," *IEEE Trans. Commun.*, vol. 53, no. 10, pp. 1620-1624, 2005.

[8] W.Hang, W.Zanji, and G.Jingbo, "Performance of DSSS against Repeater Jamming," *Proc. IEEE Electronics, Circuits and Systems*, 2006., accepted for publication.

[9] K.Salehian, M.Guillet, B.Caron, and A.Kennedy, “On-Channel Repeater for Digital Television Broadcasting Service,” *IEEE Trans. Broadcasting.*, vol.48, no.2, pp.97-102, June 2002.

[10] P.Shamain, and L.B.Milstein, “Minimum mean square error (MMSE) receiver employing 16-QAM in CDMA channel with narrowband Gaussian interference,” *Proc. IEEE MILCOM 1999*, vol.2, pp.826-830, 1999.