# Signal-level Honeypot: A Covert Communication and Interference Collection System

Cheng Chang[1], Xingsheng Zhu[2], Yue Gu[3], Zhijun Deng[4], and Sheng Liu[5]
{loeibx@163.com[1], zhuxsh@hotmail.com[2], guyue01@163.com[3]}

China Academy of Launch Vehicle Technology, 1 South Dahongmen Road, Beijing, China[1,2,3]

**Abstract.** Honeypot is originally a network trap that can attract hostile attackers and collect their attack behaviors to protect the real cyber systems and resources. Signal-level honeypot is a covert communication system with signal-level trap, which utilizes the basic idea of traditional honeypot and transform domain communication technology to attract and confront hostile interferences for reliable communication and interferences recording. In the transmitter, actual modulated signal is hidden underneath a well-camouflaged "target" signal. The actual modulated signal is designed to be noise-like, low power spectrum density, and orthogonal with the "target" signal to engage covert communication. In the receiver, a band-pass transform domain filter is used to separate signals to demodulate the actual modulated signal and collect the interferences. The proposed system can supply a high reliable communication approach with an "active" passive defense mode.

**Keywords:** Signal-level honeypot, Transform domain communication system, Covert communication, Reliable communication, Interferences collection

## 1 Introduction

With the fast development of information technology, wireless communications bring infinite convenience to the world. However, corresponding countermeasures are also continuously evolving, wireless communication systems have been plagued by various interferences and invasions [1]. Signal-level reliability that involves physical layer and data link layer is the foundation of communication systems. Most of the existing signal-level reliability measures are sorted into resisting, hiding, offsetting, and eluding 4 categories [2]. Resisting measures utilize power benefit to extract data signals from received signals, such as direct sequence spread spectrum technology [3]; hiding measures conceal data signals or their characteristics, such as embedding and noise-like technologies [4]; offsetting measures can restrain interferences or reinforce data signals, such as interference cancellation technology [5]; eluding measures utilize orthogonal or other characteristics to ensure the data signal and interferences being separated [6]. Nowadays, wireless communications can be regarded as a gaming between users and attackers. Therefore, some more active measures should be considered to achieve reliable communications.

Honeypot technology is an active cyber resources protection technology, which can build a fraudulent cyber environment to attract hostile cyber attackers to detect, attack, and capture it, so as to record their hostile behaviors [7]. Honeypot itself can be regarded as a strictly monitored computing resources. Every accessing behavior is suspectable, and the value of the

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2294228

honeypot is measured by the recorded information. Honeypot technology is widely used in computer network and its related field to collect cyber-attacks [8]. However, it has not received intensive consideration in the literature for signal-level reliability.

In this paper, transform domain communication technology [9] is combined with the basic idea of traditional honeypot to propose a signal-level honeypot to attract hostile interferences for reliable communication and interferences collection. In the transmitter, the actual modulated signal is hidden underneath a well-camouflaged "target" signal. The actual modulated signal is designed to be noise-like, low power spectrum density (PSD), and orthogonal with the "target" signal to engage covert communication. In the receiver, a band-pass transform domain filter is used to separate two signals to demodulate the actual signal and collect the interferences. The differences between traditional honeypot and the proposed system is showed in Table 1. The proposed system can supply a high reliable communication approach with an "active" passive defense mode. The next section of this paper will briefly review transform domain communication technology and the basic idea of honeypot. The signal-level honeypot is proposed detailedly in Section 3. Simulations and analysis are presented in Section 4. The paper is then concluded in Section 5.

**Table 1.** Differences between traditional honeypot and proposed signal-level honeypot

| Characteristics | Traditional honeypot | Signal-level honeypot |
|---|---|---|
| Purpose | Recording cyber-attacks, protecting cyber systems and resources | Covert communication, recording signal-level interferences and invasions |
| Action range | From network layer to application layer | Physical layer and data link layer |
| Entity | Trap | Communication system with trap |

## 2 Preliminary

### 2.1 Transform domain communication technology

Transform domain communication system (TDCS) provides reliable communications with spectrum spreading in the unoccupied frequency bins of the real-time environment [10]. The transmitter senses spectrum to get spectrum mask $A(k)$, which is a 1-D matrix composed by 0 and 1 if the $k$ th frequency bin is occupied or unoccupied. The spectrum mask and a pseudo-random $\theta_k$ are applied element by element to get frequency domain basis waveform $B(k)$. After inverse fast Fourier transform and normalization, $B(k)$ turns to time domain basis waveform $b(n)$, which is used to generate modulating symbols with cyclic code shift keying (CCSK). Then data is modulated in Gray code. The $i$ th transmitting symbol is deduced as

$$s_{TDCS,i}(n) = \frac{1}{\sqrt{NN_1}} \sum_{k=0}^{N-1} A(k) e^{j\theta_k} e^{-j2\pi m_i k/M} e^{j2\pi kn/N} \tag{1}$$

In Equation (1), $N$ and $N_1$ are the numbers of the total and the unoccupied frequency bins, respectively. $m_i \in [1, M]$ is the $i$ th transmitting data. In the receiver, local modulating symbols are generated as the transmitter, data is demodulated with maximum peak detection of the correlations between the received signal and local modulating symbols.

### 2.2 Honeypot technology

The protection process of the traditional honeypot is generally divided into 3 stages. The first stage is trap construction. Fraudulent data and files are built to improve the "sweetness" of the trap to attract cyber-attackers and facilitate interactions. The degree of the interactions depends on the fidelity between the trap and the actual system. The second stage is intrusion behavior detection and recording. Specific objects such as flows, ports, permissions, bugs, and documents are monitored and recorded to prevent damages. The last stage is post processing. The records of the attack behaviors are processed with data visualization, flow analysis, attack identification, alert generation, and traceability to supply further improvement for the actual systems.

## 3 Signal-level honeypot model

### 3.1 System structure

The diagram of the signal-level honeypot is showed in Fig. 1. The transmitter generates a false "target" signal and conceals the modulated signal beneath it. "Target" mask $A_1(k)$ is the same as spectrum mask in TDCS, with $k = 1$ representing the spectrum bins that the "target" signal occupied. To improve the "sweetness" of the trap, "target" signals $b_1(n)$ are composed by common QPSK modulated signals. Transmitting mask $A_2(k)$ is complementary with the "target" mask to generate the $i$ th modulated signal $b_{2,i}(n)$. As shown in Equation (2) and (3), $I(k)$ is an all 1 matrix, $N_2$ is the number of 1 in $A_2(k)$. Then the "target" and the modulated signals are superimposed with power adjustment to control the covert communication ability. The transmitting signal is showed as Equation (4), $\gamma$ is the factor of the power adjustment.

$$A_1(k) + A_2(k) = I(k) \tag{2}$$

$$b_{2,i}(n) = \frac{1}{\sqrt{NN_2}} \sum_{k=0}^{N-1} A_2(k) e^{j\theta_k} e^{-j2\pi m_i k/M} e^{j2\pi kn/N} \tag{3}$$

$$x_i(n) = \gamma b_{2,i}(n) + b_1(n) \tag{4}$$

In the receiver, received signal is firstly passed through a transform domain filter, whose frequency range coincides exactly with predetermined "target" mask $A_1(k)$, to separate the received "target" part $c_1(n)$ and received data part $c_{2,i}(n)$. Then the "target" part is recorded

and analyzed, while the data part is demodulated with maximum peak detection of the correlations between the received signal and local modulating symbols. In Equation (5) and (6), $C_i(k)$ and $B_2(k)$ are the frequency forms of the received data part and local generated modulating signal $b_2(n)$, $conj(\cdot)$ and $real(\cdot)$ are the conjugate and the real part of the complex signal.

$$R_i(\tau) = IFFT[C_i(k) \cdot conj\left(B_2(k)\right)] = \frac{1}{\sqrt{N_2 N}} \sum_{k=0}^{N-1} e^{-j2\pi k(\tau-\tau_i)/N} \tag{5}$$

$$data\,i = \underset{\tau\in[0,1\ldots N-1]}{\arg\max}[real\left(R_i(\tau)\right)] \tag{6}$$

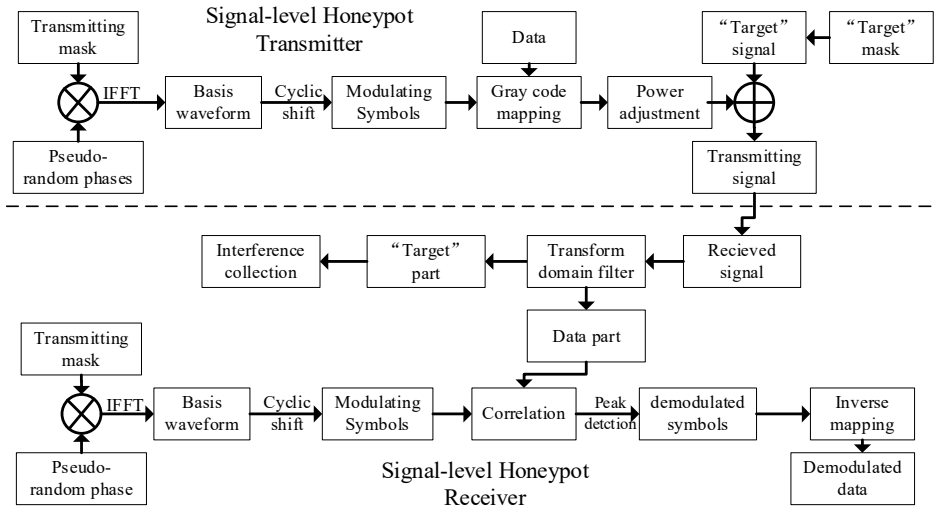


**Fig. 1.** The diagram of signal-level honeypot

### 3.2 Performance analysis

According to the Shannon theory [11], transmission rate is in direct proportion to available bandwidth and signal noise ratio (SNR). For the power of $b_2(n)$ is equally distributed in unoccupied frequency bins, the wider bandwidth of the modulated signal, the lower PSD of the system can achieve.

$$PSD(b_2(n)) \propto \frac{1}{W} \propto \frac{1}{N_2}, R_b \propto W \propto N_2 \tag{7}$$

Frequency domain low detection performance is evaluated by the signal power of modulated signal. The less power adjustment factor, the lower signal power of modulated signal, the less likely to be detected, and the lower transmission rate of the system.

Time domain low detection performance depends on the performance of the pseudo-random sequences. The longer sequence, the better performance system achieved [12].

Bit error rate (BER) with certain transmission rate and additive white Gaussian noise (AWGN) is the key indicator of the proposed system. The lower BER, the better transmitting performance achieved.

Bandwidth of the "target" signal is used to evaluate the collection range. The wider bandwidth of the "target" signal, the lager of the collection range, but the narrower bandwidth of the modulated signal, the lower transmission rate of the covert communication. Interference identification is not considered in this paper.

## 4 Simulations

To verify the proposed method, a semi-physical system is built. The "target" signal is generated by a signal source with QPSK modulation of 8MHz bandwidth. The modulated signal is generated by a modified TDCS transmitter with CCSK modulation of 62MHz bandwidth to fully use total 70MHz bandwidth. The original output powers of the two signals above are the same, and the power adjustment factor $\gamma$ is set as -35dB. In other words, the power of the "target" signal is 35dB larger than that of the modulated signal. A modified TDCS receiver samples with 8 times oversampling, 560MHz, to obtain the received signal in Fig. 2. In consideration of the path loss and the sensitivity of the receiver, actual received signal power is greatly lowered beneath the noise.

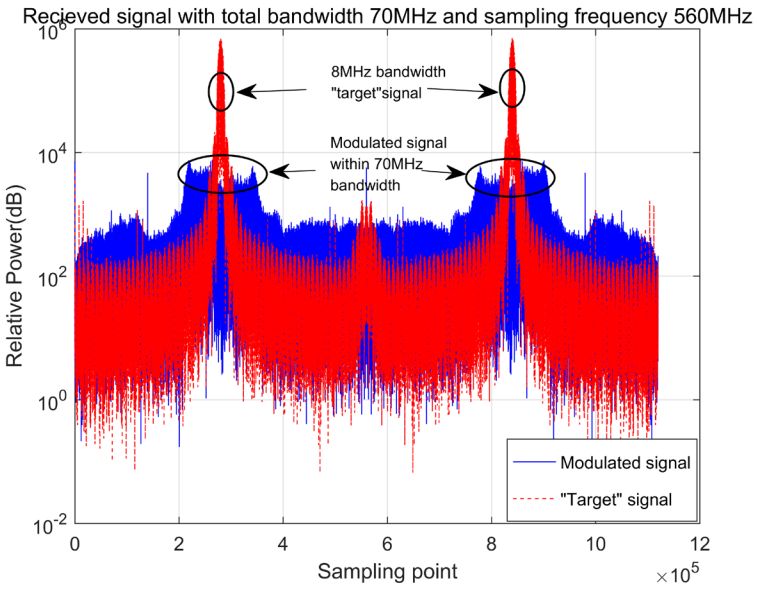


**Fig. 2.** The frequency domain form of the transmitting signal

The BER of the proposed method with different power adjustment factors is showed in Fig. 3. The modulation is set as 64-ary CCSK. A BER without "target" signal is run as the

reference. Power adjustment factor $\gamma$ is set as -20dB, -30dB, and -40dB to get 3 typical BERs with AWGN. When $\gamma$ is -20dB, "target" signal and AWGN collectively influence BER, system needs extra 2.5dB SNR to compensate the BER deterioration caused by the "target" signal at BER=$10^{-4}$. When $\gamma$ is -30dB and -40dB with $E_b/N_0$ less than 5dB, "target" signal and AWGN collectively influence BER. If $E_b/N_0$ is more than 6dB, system cannot fully compensate the BER deterioration, platforms appear at BER=$10^{-3}$. Therefore, when $\gamma$ is more than -20dB, the proposed system can well achieve covert communication and interferences collection.

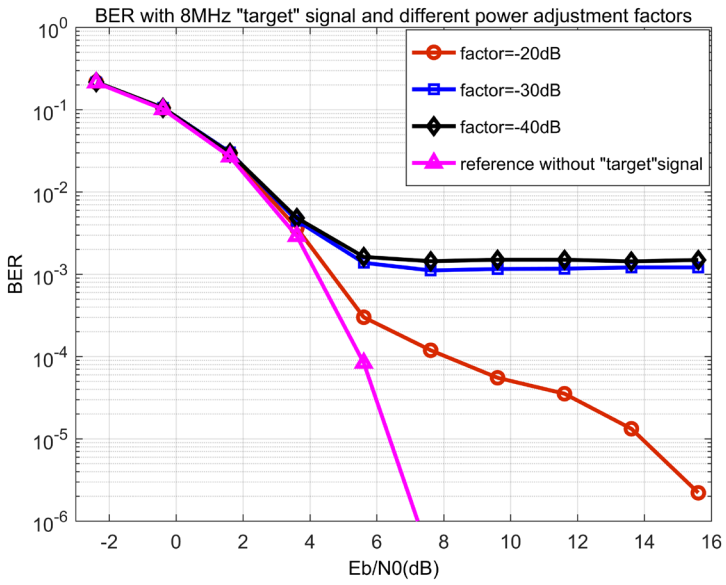


**Fig. 3.** The BER of the proposed method with different power adjustment factors

## 5 Conclusions

This paper introduces a signal-level honeypot, which utilizes the basic idea of traditional honeypot and transform domain communication technology to attract and confront hostile interferences for reliable communication and interferences collection. The proposed system can achieve low detection probability with time domain noise-like and frequency domain low PSD. Besides, by sacrificing affordable $E_b/N_0$, the system can process wideband signal trap to collect hostile interferences. The proposed system supplies a high reliable communication approach with an "active" passive defense mode.

## References

[1] Haykin, S.: Cognitive radio: brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications. 23(2). pp. 201-220 (2005)

[2] Chang, C., Huan, H., Xu, J., et al: Multidimensional parallel combinatory transform domain communication system. International Journal of Communication Systems. pp. e3249 (2017)
[3] Slobodan, D., Marko, S., Igor, D.: Highly non-stationary interference suppression in direct sequence spread-spectrum systems. IEEE 38th International Conference on Telecommunications and Signal Processing (TSP). (2015)
[4] Kiseon, K., Jalel, B., Prem, M.: Covert Communication Networks in Hostile Environments. Security and Communication Networks. pp. 1-2 (2018)
[5] Andrews, J. G.: Interference cancellation for cellular systems: a contemporary overview. IEEE Wireless Communications. 12(2). pp. 19-29 (2005)
[6] Liang, Z., Tian, F., Simon, X., et al: Study on Interference Suppression Algorithms for Electronic Noses: A Review. Sensors. 18(4). pp. 1179 (2018)
[7] Spitzner, L.: Honeypots: tracking hackers. Hackers. pp. 1-405 (2003)
[8] Teo, L., Sun, Y., Ahn, G.: Defeating Internet Attacks Using Risk Awareness and Active Honeypots. IEEE International Information Assurance Workshop. IEEE. (2015)
[9] Chakravarthy, V., Nunez, A., Stephens, J., et al: TDCS, OFDM, and MC-CDMA: a brief tutorial. IEEE Communications Magazine. 43(9). pp. S11-S16 (2005)
[10] Xie, T., Xinyu, A., Chu, Z., Gao, W.: Satellite Covert Communication System Based on the Transform Domain Communication System. Information & Control. 43(5).pp. 524-528 (2014)
[11] Proakis, G.: Digital communications. 5th edition. McGraw-Hill Higher Education (2011)
[12] Sun, H., Cao, F., Qin, H.: Multiple Access Applications of Transform Domain Communication System Based on Phase Coding. In: Proceedings of Fifth International Conference on Big Data and Cloud Computing. pp. 217-222 (2015)