International Journal of Innovative
Computing, Information and Control
Volume **10**, Number **4**, August **2014**

 ISSN 1349-4198
pp. 1533–1541

CHAOTIC ULTRA-WIDEBAND COVERT COMMUNICATION SYSTEM BASED ON QUANTUM KEY DISTRIBUTION

Xinliang Wang and Hanyu Liu

School of Electrical Engineering and Automation
Henan Polytechnic University
No. 2001, Shiji Road, Jiaozuo 454003, P. R. China
junci158@163.com; hanyuliu@live.cn

Received September 2013; revised January 2014

Abstract. *Chaotic pulse position modulation (CPPM) Ultra-wideband system can be used in covert communication due to its high security and low interception rate. However, the CPPM scheme introduces delay into the feedback loop, so the wrong decision of data will cause error propagation. Furthermore, the parameters mismatch and not ideal synchronization between receiver and transmitter will arouse high bit error rate. And the security for system parameters is difficult to be guaranteed in the communication process. The CPPM Ultra-wideband covert communication based on quantum key distribution was proposed. The received signal was tracked by online separation using particle filtering in demodulation. And the system parameters of chaotic map and delay time were distributed by the quantum protocol. Simulation and experiment results show that the proposed system has good synchronization robustness in comparison with the traditional CPPM scheme. It can reduce error propagation caused by wrong decision and lower the BER. Moreover, the proposed system has high security by quantum key distribution protocol.*

Keywords: Chaotic communications, Covert communications, Chaotic pulse position modulation, Quantum key distribution, Particle filtering

1. **Introduction.** In recent years, chaotic signals [1-3] and Ultra-wideband communications [4,5] are widely used in covert communication for their wide spectrum, good security and low interception rate. The chaotic Ultra-wideband communication system has great commercial and military application and has been the research focus in wireless communication area. [6,7] use chaos for the Ultra-wideband communications in low rate WPAN, and meet the requirements of low complexity, weak power consumption and low cost of LR-WPAN applications. A chaotic-pulse based Ultra-wideband body area network was proposed in [8]. Moreover, the chaotic Ultra-wideband communications have other different applications, such as WSN, Multimedia and Positioning [9-11].

According to the actual communication circumstances, general chaotic communications require strict conditions of the channel, filtering and noise. Chaotic pulse position modulation (CPPM) Ultra-wideband communication system was proposed in [12,13]. It sends narrow pulses which have ultra-broadband spectrum. The system information is carried by the interval of adjacent pulses in modulation scheme; thus it can reduce the negative impact of the filtering and channel distortion, take full advantage of security performance of chaos and enhance system's reliability. So the CPPM Ultra-wideband scheme is an effective way for covert communications. Given that the delay of CPPM is in the feedback, each chaotic map contains the sent sequence information. These sequences may produce a new divergent generation, thus leading to serious error in demodulation. The synchronous robustness has a great influence on demodulation between the receiver and

transmitter. Because parameters mismatch exists between receiver and transmitter in real system or once a larger disturbance happens, the synchronization error will generate a lot of bit error rate, the strict synchronization of the receiver and transmitter is demanded in system.

Particle filtering algorithm is based on Bayesian importance sampling, and uses optimal estimation to approximate the true value in non-linear conditions. It tracks signal by the random walk of the particle, and uses the mean of sample as to estimate of the system [14,15]. CPPM covert communication demodulation based on particle filtering is proposed in this paper, because chaotic signal is the non-linear signal. The proposed scheme can lower the synchronous requirements between the receiver and transmitter, thus reducing the bit error rate.

Communicating parties must obtain the communication key before carrying out covert communications. So the secure communication for the initial key is required. However, this security cannot be proven in classical secure communication. The existence of the eavesdropper is unknown for the communicating parties, which leads to "catch 22" problem in secure communication. In recent years, people are interested in the topic of getting the secure key using the physical system characteristics, especially using the quantum physics characteristics to get and manage the key. BB84 [16], EPR [17], B92 [18], other classical quantum key distribution protocol and their improved protocols have appeared subsequently. These key distribution protocols have absolute security based on quantum uncertainty theorem and the no-cloning theorem [19]. They can greatly improve the safety performance of the communication system. The applications of quantum technology in covert communications were discussed [20-22]. For the CPPM covert communications systems, the parameters of chaotic map and system delay time are the communication key. We can solve the security of CPPM covert communication key using quantum key distribution.

2. **Principle of CPPM.** The CPPM scheme [12] is built around a chaotic pulse regenerator (CPRG) as shown in Figure 1. In CPPM scheme the binary information is applied to the pulse train at the output of the CPRG by adding a block in the feedback loop that leaves the signal unchanged, if "0" is being transmitted, or delays the pulse by a fixed time if "1" is being transmitted. At the receiver side, the signal is applied to the input of

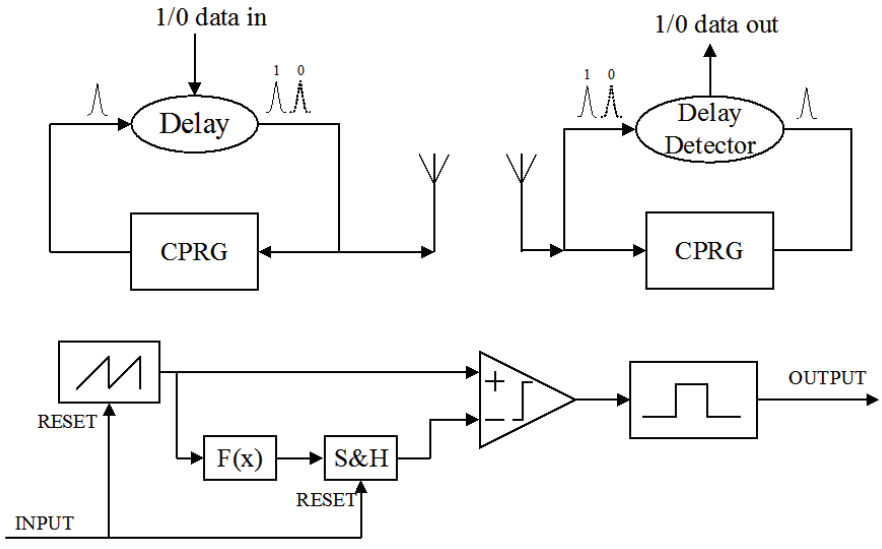

FIGURE 1. Illustration of the basics of CPPM schemes and CPRG operation

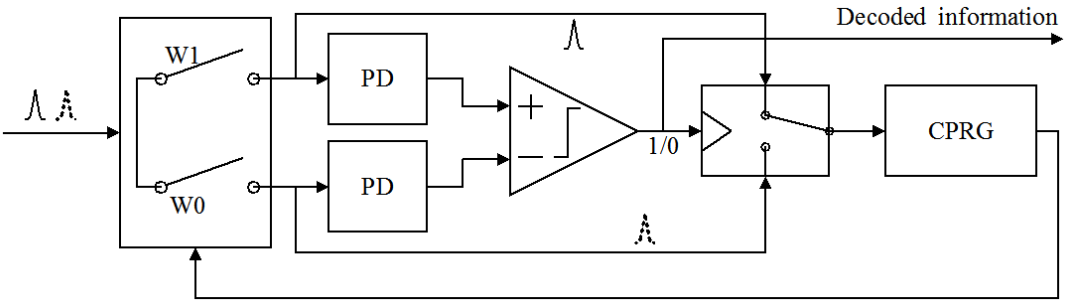

FIGURE 2. Diagram of the receiver

an identical CPRG, so the outputs from the CPRG's in the transmitter and the receiver are identical. By evaluating the relative pulse timings in the received signal and in the signal at the output of the CPRG, the receiver can recover the digital message. When the CPRG's are not matched with sufficient precision, a large decoding error happens [12,13].

The CPPM receiver block diagram [12] is shown in Figure 2. Based on the state of the synchronized CPRG, the input is blocked at all times except the time windows around the expected locations of the pulses corresponding to "1" and "0." The signals within these windows are applied to two Peak Detectors (PD). Based on which window contained the peak of the maximum height, we decide whether "1" or "0" was transmitted and the signal within the corresponding time window is passed to the receiver CPRG.

3. CPPM Covert Communication System Based on Quantum Key Distribution.

3.1. **System structure.** The structure of CPPM covert communication system based on quantum key distribution is shown in Figure 3. The CPPM system takes the binary digital information into the feedback, combined with the original chaotic map. It turns the information into a new map to achieve the modulation. The transmitted signal has narrow pulses with ultra-broadband spectrum. The mathematical model is:

$$T_{n+1} = F(T_n) + S_{n+1} \times d \tag{1}$$

where T_n is adjacent pulse interval, $F(T_n)$ is chaotic map function, and S_n is binary information sent by the system, whose value is "1" or "0", d is the delay length caused

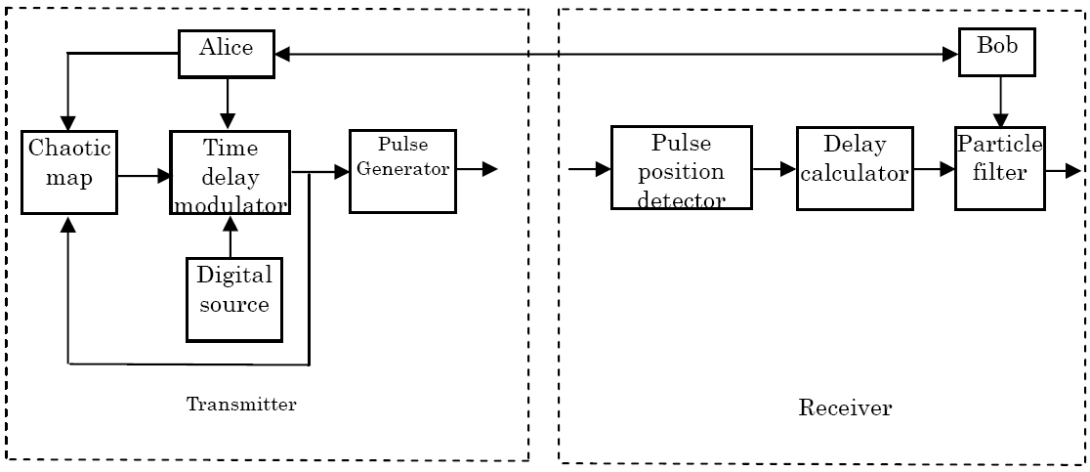

FIGURE 3. Structure of CPPM covert communication system based on quantum key distribution

by the sent data. If the sent signal is "1" then the system adds a delay; if it is "0", do not delay.

The receiver detects the received signal using the pulse position detector, and calculates the time delay between two adjacent pulses. Then the value is sent to the particle filter. The final output is the judgment for the binary information. Specific demodulation algorithm is introduced in Section 3.2.

From the analysis above, we can see that parameters of the chaotic map and the delay time are the communication key between the transmitter and receiver. It is distributed by the quantum key distribution protocol. Specific key distribution process is discussed in Section 3.3.

3.2. **Principle of system demodulation.** The system observation equation is

$$y_n = T_n + \omega_n \tag{2}$$

where ω_n is additive white Gaussian noise with zero mean and power spectral density σ^2, the noise is error of the synchronization, y_n is the observations. It uses online separation of the chaotic signal when tracking and demodulating by particle filter. We define $y_{1:n} \in \{y_1, \cdots, y_n\}$, $T_{1:n} \in \{T_1, \cdots, T_n\}$ and $S_{1:n} \in \{S_1, \cdots, S_n\}$, where $y_{1:n}$ is observed signal with noise, $T_{1:n}$ is source signal, $S_{1:n}$ is binary information sent by the system. If we give the state variable T_n, S_n, observed signal y_n independent from the marginal distribution in specific condition $p(y_n|T_n, S_n)$, recurrence formula can be obtained:

$$p(T_{1:n}, S_{1:n}|y_{1:n}) = p(T_{1:n-1}, S_{1:n-1}|y_{1:n-1}) \times \frac{p(y_n|T_n, S_n) \cdot p(T_n|T_{n-1}) \cdot p(S_n|S_{n-1})}{p(y_n|y_{1:n-1})} \tag{3}$$

In the above formula, the sent binary signal is independent with each other, then $p(S_n|S_{n-1}) = p(S_n)$. From the perspective of Bayesian, filtering problem of the model is that we use the observed signal with noise to estimate joint posterior probability density function $p(T_{1:n}, S_n|y_{1:n})$ recursively, and its marginal distribution $p(T_{1:n}|y_{1:n})$ and $p(S_{1:n}|y_{1:n})$. We can obtain the state of signal from $p(T_{1:n}|y_{1:n})$ and $p(S_{1:n}|y_{1:n})$.

3.2.1. *Description of particle filtering.* Particle filter is a statistical simulation method based on Bayesian sequential importance sampling and resampling. Its main ideal is that experience estimation of expectation's posterior distribution $q(T_{1:n}|y_{1:n})$ can be obtained by sampling enough samples from importance function $p(T_{1:n}|y_{1:n})$ [14,15]. It proves that posterior distribution of expectation can be simulated by a set of particles and its weight $\left\{T_{1:n}^{(i)}, \varpi_n^{(i)}\right\}$, $i = 1 : N$ approximately in [14]. N is the number of particles.

$$\varpi_n^{(i)} = \frac{\tilde{\varpi}_n^{(i)}}{\sum_{i=1}^{N} \tilde{\varpi}_n^{(i)}}, \quad \tilde{\varpi}_n^{(i)} = \frac{p\left(T_{1:n}^{(i)}|y_{1:n}\right)}{q\left(T_{1:n}^{(i)}|y_{1:n}\right)} \tag{4}$$

In order to obtain particle sampling and recursive form of estimation of weight, we need to select importance function as follows:

$$q(T_{1:n}|y_{1:n}) = q(T_0) \prod_{j=1}^{n} q(T_j|T_{1:j-1}, y_{1:j}) \tag{5}$$

Then we can get weight's recursive.

$$\tilde{\varpi}_n^{(i)} = \tilde{\varpi}_{n-1}^{(i)} \times \frac{p\left(y_n|T_n^{(i)}\right) \times p\left(T_n^{(i)}|T_{n-1}^{(i)}\right)}{q\left(T_n^{(i)}|T_{n-1}^{(i)}, y_n\right)} \tag{6}$$

The choice of importance function has great influence on algorithm, so we select prior distribution to form importance function generally.

$$q\left(T_n^{(i)}|T_{n-1}^{(i)}, y_n\right) = p\left(T_n^{(i)}|T_{n-1}^{(i)}\right) \tag{7}$$

Then we get the real-time estimation of state y_n.

$$\hat{y}_n = \sum_{j=1}^{N} y_n^{(j)} \times \varpi_n^{(j)} \tag{8}$$

3.2.2. *System demodulation based on particle filter.* The main idea of CPPM demodulation based on particle filter is that we extract particles from the prior distribution function $U(t)$ randomly, that $U(t)$ is the uniform distribution function, and that the binary information has discrete distributions in the same probability. The adjacent pulse signal delay is detected by pulse position detector, and then it is demodulated by the particle filter. The optimal value is estimated to approximate the true value by particle filter. The particles, which are randomly selected through the chaotic map, are combined with random binary signals. The obtained results and observed results were compared to calculate weight of current particle. After all particles are calculated, resampling is needed to slow degradation if the particle's degradation is severe. Finally, the current value of the particle and the statistical weight are counted averagely to obtain the best results. In summary, the system demodulation process is as follows.

1) Initialization: extract the initial state from the prior distribution $y_0^{(j)}$ and initialize weight $\varpi_0^{(j)} = 1$, $j = 1 \cdots N$. When time is n, the following steps are performed.
2) Prediction by one step:
$$y_n^{(j)} = T_n^{(j)} + \omega_n^{(j)} \tag{9}$$
3) Weight calculation:
$$\varpi_n^{(j)} = p\left(y_n|T_n^{(j)}\right) \tag{10}$$
4) Resampling.
5) Calculating the optimal value of the state $\hat{y}_n$.
$$\hat{y}_n = \sum_{j=1}^{N} y_n^{(j)} \times \varpi_n^{(j)} \tag{11}$$
6) We take demodulation through system equation and observations after getting the optimal value.
$$p_n = \hat{y}_n - y_n \tag{12}$$
where p_n is the decision value. We define $d/2$ as the threshold; greater is "1", otherwise "0".
7) $n \to n+1$ Go to step 2).

3.3. **Principle of system quantum key distribution.** It is assumed that the channel consists of a source which emits pairs of spin-1/2 particles. A and B are the physical quantities required to be measured, the corresponding values are α_i and β_j, and the units are vector a_i and b_j. When there is no noise or eavesdroppers in the channel, EPR entangled bits have the following relation.

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{-+}(a_i, b_j) - P_{+-}(a_i, b_j) \tag{13}$$

Here $P_{\pm\pm}(a_i, b_j)$ denotes the ± 1 probability obtained along a_i and b_j. The correlation coefficient S of entangled bits can be described as follows.

$$S = \sum_{i,j} E(a_i, b_j) \tag{14}$$

According to the principle of quantum mechanics, the EPR entanglement is

$$E(a_i, b_j) = -a_i b_j \tag{15}$$

It is easy to obtain the correlation coefficient without disturbance.

$$S = -2\sqrt{2} \tag{16}$$

Under the disturbance

$$S = \int p(n_a, n_b) dn_a dn_b \left[\sqrt{2} n_a n_b\right] \tag{17}$$

where n_a and n_b are two unit vectors (for particles a and b respectively), $p(n_a, n_b)$ denotes the probability of intercepting a spin component along a given direction for a particular measurement. It can be proved that S is satisfied [17].

$$-\sqrt{2} \le S \le \sqrt{2} \tag{18}$$

So the legitimate users can detect whether there was the adversary or not according to the correlation coefficient of EPR particles. The quantum key distribution protocol of CPPM covert communication system is as followed according to [17].

1) Quantum information source or Alice produces EPR particles by physical method. Each one EPR particle contains two particles. One particle is sent to Alice, and the other is sent to Bob.
2) Alice measures the particle string and records the results randomly. Alice selects 0 or $\pi/2$ phase of interferometer to measure his particles randomly. According to the nature of the EPR particles entanglement, Alice measures the particles, EPR particles are resolved entanglement, and at the same time the quantum state of Bob particle is identified.
3) Bob measures the received quantum string. He selects 0 or $\pi/2$ phase randomly to measure the particle which he has received.
4) Bob selects some from the measured results randomly and informs Alice. Eavesdropping is detected based on the Bell theory. When the sum of the two phases is integer multiple for 0 or $\pi/2$, then Alice's and Bob's particles are associated; otherwise they are invalid qubit done by noise or adversaries. This communication will be given up if the error rate exceeds the standard value.
5) Alice and Bob reserve the measurements of same measurement-based. So they get the original key.
6) Steps 1) to 5) are repeated at intervals of a fixed time. The key is replaced.

Supposed that the system key is $K = (k_1, k_2, \cdots, k_{n_1}, k_{n_1+1}, \cdots, k_n)$ with n bits, it corresponds to parameters of the chaotic map and delay time. The parameter of the chaotic map is $K_c = (k_1, k_2, \cdots, k_{n_1})$ with n_1 bits. The parameter of the delay time is $K_d = (k_{n_1+1}, k_{n_1+2}, \cdots, k_n)$ with $n - n_1$ bits. So the parameter of the chaotic map is

$$c = \frac{2^{n_1}}{c_e - c_s} \times 2^{K_c} + c_s \quad c \in [c_s, c_e] \tag{19}$$

where c_s and c_e are the start and end points of the chaotic parameter range. And the parameter of the delay time is

$$d = \frac{2^{n-n_1}}{d_e - d_s} \times 2^{K_d} + d_s \quad d \in [d_s, d_e] \tag{20}$$

where d_s and d_e are the start and end points of the delay parameter range.

3.4. **System security analysis.** According to the principle of ultra-wideband CPPM system, it has less interference to other communication systems, low interception rate and good concealment because the system sends the signal with narrow pulses of ultra-wideband. The binary information hides in the adjacent pulse interval. The change of adjacent pulse interval is chaotic, and the role of feedback introduces random binary information. So the system has strong security. The eavesdroppers cannot demodulate the signal correctly when they do not know the parameters of chaotic map and delay time caused by data. These parameters of the proposed system are distributed by the quantum protocol. The protocol has excellent security. The unconditional security of symmetric quantum key distribution is proved in [23]. Because the qubit state is uncertain in the transmission process, only when the legal correspondent measures the entangled particles, the state of the particles is confirmed. This property suggests that even the eavesdropper has detected the sent entanglement between Alice and Bob, he cannot get any information. This virtue makes the Trojan horse attack is also invalid. So the system parameters of chaotic map and delay time have very good security. Moreover, changing the key at regular intervals can help to resist the intercepted attack. So the system security is guaranteed.

4. **Simulation and Experiment.** In order to show the good performance of CPPM modulation system based on particle filter, the modulated signals are tracked using particle filter. In simulation, the variance of noise is 10^{-3}, the number of particles is 100 and the bit of signal is 1000, the delay time of sending the signal "1" is $d = 0.5$, and the chaotic map is $x_{n+1} = c\sin^2(2\pi(x_n - 0.6) - \pi/2) + 0.6 + S_{n+1} \times d$, $c = 0.7$. The initial value of chaotic signal generator is 0.9. The 100 bits between 300 and 400 are intercepted. The results are shown in Figure 4. From Figure 4, the tracking results are good and it is very close to the real signal because of particle filter's ability in nonlinear condition and random walks.

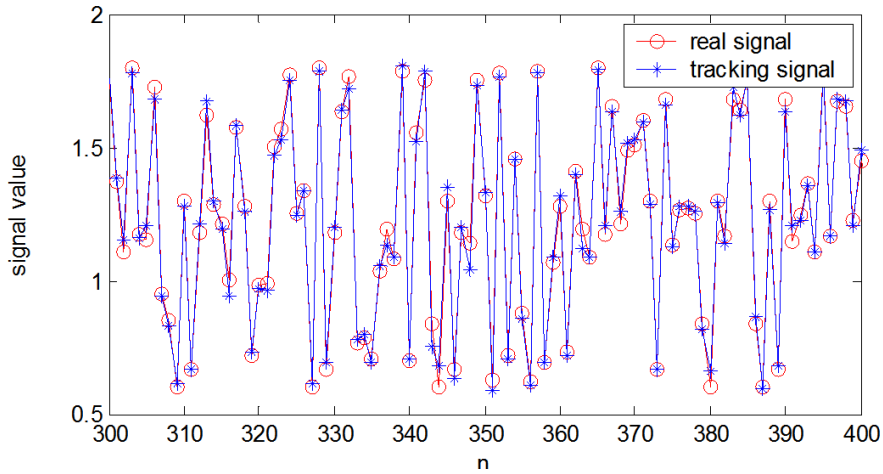

FIGURE 4. Comparison between the optimal value and real value

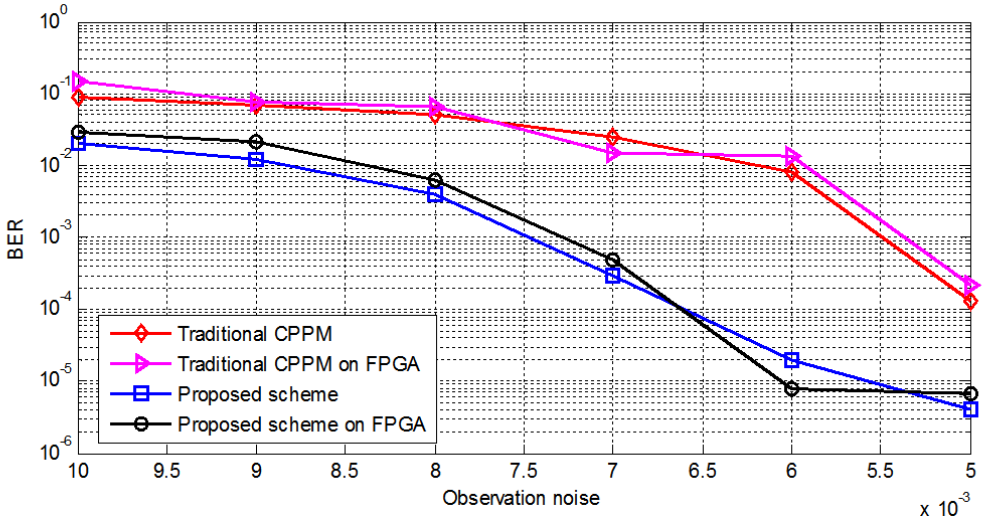

FIGURE 5. BER with the observation noise

We make a comparison about BER between the proposed system based on particle filter and traditional CPPM. In this part, we use the FPGA platform to design the proposed system based on particle filter and traditional CPPM. In simulation and experiment, the variance of noise is in $10^{-2} - 10^{-3}$, the number of particles is 10^3 and the bit of signal is 10^5. Other simulation conditions are the same as above conditions. After many repeated experiments in average, the results are shown in Figure 5. From Figure 5, the BER of proposed system is smaller than traditional CPPM obviously, and with the noise variance decreasing, the gap of the error rate increases.

The delay of CPPM is in the feedback, and it will lead to divergence of chaotic system. The mismatch's problems of parameters always exist in actual receiver and transmitter system. The synchronization of transmitter and receiver is not ideal, when the system is interfered by noise. Therefore, it will lead to the wrong judgment of data, propagation of error in feedback, and result in high BER. It can be seen in Figure 4, when the synchronization is not ideal, the particle filter's ability in random walks can track the real signal well. It can reduce the wrong judgment of data and propagation of error. So it can be seen in Figure 5, the performance of the CPPM based on particle filter is better than the traditional CPPM.

5. **Conclusions.** The chaotic Ultra-wideband covert communication was proposed in this paper. It uses ultra-wideband pulse to improve signal anti-intercepted rate and uses CPPM modulation scheme to increase the communication confidentiality. Particle filtering is adopted to track the received signal in demodulation. The quantum key distribution ensures the parameters security of chaotic map and delay time in the communication. The proposed system has lower BER compared with the traditional CPPM system.

Acknowledgment. This work is supported by Doctor Fund of Henan Polytechnic University (Grant No. 648735) and Henan Province Open Laboratory for Control Engineering Key Disciplines (Grant No. KG2009-20).

REFERENCES

[1] N. F. Reddell, T. B. Welch and E. M. Bollt, A covert communication system using an optimized wideband chaotic carrier, *Proc. of IEEE Military Communications Conference*, pp.1330-1334, 2002.

[2] H. X. Zhang, Z. Y. Zhang and P. L. Qiu, Novel algorithm of covert communication, *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol.31, pp.514-517, 2003.
[3] J. P. Sun, S. G. Ju and L. Y. Su, A novel covert communication algorithm with chaos and FCM, *Journal of Sichuan University (Natural Science Edition)*, pp.498-504, 2010.
[4] V. I. Kalinin and V. V. Chapursky, Wireless covert communications with code spectrum modulation of UWB noise signals, *The 20th International Crimean Conference Microwave and Telecommunication Technology*, pp.366-367, 2010.
[5] Y. Du, Application prospect analysis of UWB communication technology in concealed communication, *Shipboard Electronic Countermeasure*, vol.30, pp.54-56, 2007.
[6] R. Nada, Z. Ghada et al., Chaotic UWB communications for low rate WPAN applications, *The 2nd International Conference on Signals, Circuits and Systems*, 2008.
[7] S. M. Han, M. H. Son and Y. H. Kim, Chaotic UWB communication system for low-rate wireless connectivity applications, *IEICE Transactions on Communications*, vol.E90-B, no.10, pp.2891-2896, 2007.
[8] S. Rajagopal, N. G. Kang, S. H. Park et al., Chaotic UWB based system design for ultra-low power body area networks, *The 8th IEEE Dallas Circuits and Systems Workshop: Energy Efficient Circuits and Systems*, pp.15-18, 2009.
[9] P. Grigorios, Chaotic UWB quadrature chaos shift keying for wireless sensors and coexistence with direct sequence spread spectrum systems, *Proc. of the 7th International Symposium on Computer Networks*, 2006.
[10] K. Lee, K. Soocheol, J. Kim et al., A chaotic UWB system for home networks, *International Conference on Hybrid Information Technology*, 2006.
[11] S. Y. Lee and W. C. Yang, A non-coherent UWB direct chaotic indoor positioning system using fuzzy logic algorithm, *International Conference on Advanced Communication Technology*, 2007.
[12] M. M. Sushchik, N. F. Rulkov, L. Lawrence, L. S. Tsimring, H. Abarbanel, K. Yao and A. R. Volkovskii, Chaotic pulse position modulation: A robust method of communication with chaos, *IEEE Commun. Letters*, vol.4, pp.128-130, 2000.
[13] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring and A. R. Volkovskii, Digital communication using chaotic-pulse-position modulation, *IEEE Transactions on Circuits and Systems*, vol.12, pp.1436-1444, 2001.
[14] A. Doucet, S. Godsill and C. Andrieu, On sequential Monte Carlo sampling methods for Bayesian filtering, *Statist. Comput.*, vol.10, pp.197-208, 2000.
[15] A. Doucet, S. Godsill and C. Andrieu, Particle methods for change detection, system identification, and control, *Proc. of the IEEE*, vol.92, pp.423-438, 2004.
[16] C. H. Bennett and G. Brassard, An update on quantum cryptography, *Advances in Cryptography: Proc. of Crypto*, pp.475-480, 1984.
[17] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Letters*, vol.67, pp.661-664, 1991.
[18] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Letters*, vol.68, pp.3121-3124, 1991.
[19] W. Wootters and W. Zurek, A single quantum cannot be cloned, *Nature*, vol.299, pp.802-803, 1982.
[20] D. Cao and Y. L. Song, Multi-party quantum covert communication with entanglement private-keys, *Journal of Applied Sciences*, vol.30, pp.52-58, 2012.
[21] Y. H. Zhao and X. J. Wen, A covert communication protocol based on quantum dense coding, *Proc. of International Conference on Electronic and Mechanical Engineering and Information Technology*, pp.3376-3379, 2011.
[22] X. Liao, Q. Y. Wen, Y. Sun and J. Zhang, Multi-party covert communication with steganography and quantum secret sharing, *Journal of Systems and Software*, vol.83, pp.1801-1804, 2010.
[23] D. Mayers, Unconditional security of quantum cryptograph, *Journal of the ACM*, vol.48, pp.351-406, 2001.