Journal of Southeast University (English Edition) Vol. 33, No. 1, pp. 1 − 4 Mar. 2017 ISSN 1003—7985

GNSS spoofing detection based on uncultivated wolf pack algorithm

Sun Minhong[1,2] Shao Zhangyi[2] Bao Jianrong[2] Yu Xutao[1]

([1]School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

([2]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: In order to solve the problem that the global navigation satellite system (GNSS) receivers can hardly detect the GNSS spoofing when they are deceived by a spoofer, a model-based approach for the identification of the GNSS spoofing is proposed. First, a Hammerstein model is applied to model the spoofer/GNSS transmitter and the wireless channel. Then, a novel method based on the uncultivated wolf pack algorithm (UWPA) is proposed to estimate the model parameters. Taking the estimated model parameters as a feature vector, the identification of the spoofing is realized by comparing the Euclidean distance between the feature vectors. Simulations verify the effectiveness and the robustness of the proposed method. The results show that, compared with the other identification algorithms, such as least square (LS), the iterative method and the bat-inspired algorithm (BA), although the UWPA has a little more time-complexity than the LS and the BA algorithm, it has better estimation precision of the model parameters and higher identification rate of the GNSS spoofing, even for relative low signal-to-noise ratios.

Key words: global navigation satellite system (GNSS); spoofing detection; system identification; uncultivated wolf pack algorithm

DOI: 10.3969/j.issn.1003 −7985.2017.01.001

Spoofing interference[1] is similar to a global navigation satellite system (GNSS) signal. It is produced by a spoofer and it can mislead satellite navigation receivers into wrong navigation and positioning. This kind of interference and the satellite signal can be overlapped in time, frequency and spatial domains. So, the spoofing can obtain the same processing gain as well as the real signal and it is difficult to detect. Existing works mainly aimed at identification of spoofing by utilization of signal features, such as absolute power[2], time-of-arrival[3], angle-of-arrival[4], etc. Recently, wireless transmitter identification based on model parameters has made great progress[5−6]. The results show that the model parameters are effective, even for relatively low signal-to-noise ratio (SNR) and small samples. There are some classical methods for the estimation of model parameters, such as the LS algorithm[5] and the iterative method[6]. However, there are some disadvantages for the LS algorithm and the iterative method in estimating the model parameters. For the LS, it is sensitive to noise and fails to estimate parameters if the added noise is not white[7]. Similarly, the iterative method suffers from a convergence problem[8].

The swarm intelligence algorithm has been proved to be an efficient method for many global optimization problems and has been successfully applied to many areas. Inspired by the hunting behavior and distribution mode of the wolf pack, a new swarm intelligence algorithm, uncultivated wolf pack algorithm (UWPA), was developed in Ref. [9]. Moreover, the convergence of UWPA was proved in Ref. [10]. In this paper, a transmitter or a spoofer and their wireless channels are modeled as Hammerstein models. Motivated by its successful applications, we put forward a novel approach of nonlinear system identification by using the UWPA, which is stable, convergent and robust. For the purpose of performance comparison, experiments are also carried out using the LS, the iterative method and the BA.

1 System Modelling

The block diagram of a typical spoofer or a satellite transmitter is shown in Fig. 1. According to the structure illustrated in Fig. 1, the nonlinearity distortion of the transmitter is modeled as a memoryless nonlinear polynomial[11]. It is sufficient to consider only odd terms because the frequency components produced by the even terms are filtered out by RF bandpass filters[6]. So, this model is expressed as

$$x(n)=b_1d(n)+b_3d(n)\left|d(n)\right|^2+\ldots+b_{2m-1}d(n)\left|d(n)\right|^{2m-2}=\sum_{i=1}^{M}b_{2i-1}d(n)\left|d(n)\right|^{2i-2} \tag{1}$$

where M is a positive integer; $2M-1$ is the order of the polynomial; $d(n)$ is the input signal; and b_k is the polyn-

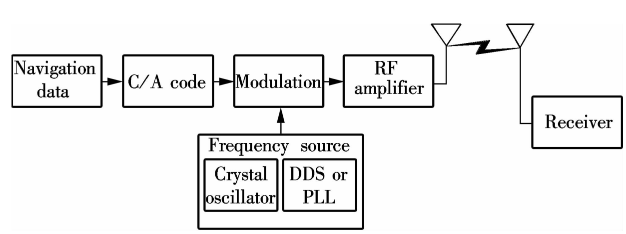

Fig. 1 Structure of a typical spoofer/transmitter

Received 2016-09-12.

Biography: Sun Minhong (1974—), male, doctor, associate professor, cougar@hdu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 61271214, 61471152), the Postdoctoral Science Foundation of Jiangsu Province (No. 1402023C), the Natural Science Foundation of Zhejiang Province (No. LZ14F010003).

Citation: Sun Minhong, Shao Zhangyi, Bao Jianrong, et al. GNSS spoofing detection based on uncultivated wolf pack algorithm. [J]. Journal of Southeast University (English Edition), 2017, 33(1): 1 −4. DOI: 10.3969/j.issn.1003 −7985.2017.01.001.

omial coefficient.

The radio channel is modeled as a discrete-time linear time invariant system[6]. So, the channel can be regarded as a FIR filter as follows:

$$y(n) = \sum_{k=0}^{N-1} h_k x(n-k) + w(n) \quad (2)$$

where N is the order of the FIR filter; h_k is the coefficient of channel impulse response; $w(n)$ is the additive Gaussian white noise and $w(n) \sim N(0, \sigma^2)$; $y(n)$ is the received signal.

Substituting Eq. (1) into Eq. (2), the whole system can be written as

$$y(n) = \sum_{k=0}^{N-1} h_k \sum_{i=1}^{M} b_{2i-1} \mid d(n-k) \mid^{2i-2} d(n-k) + w(n) \quad (3)$$

Eq. (3) represents a Hammerstein model[12] which is composed of a static nonlinear block followed by a dynamic linear block. In a GNSS receiver, the transmitted signal $d(n)$ can always be acquired by demodulation and dispreading once the received signal $y(n)$ is available, and thus the input and the output signal of Eq. (3) are both accessible. Hence, the identification of this system is feasible.

2 Uncultivated Wolf Pack Algorithm

The advantages, components, basic theory and steps of the UWPA are briefly introduced in this section and the pseudo code of the UWPA is represented.

The UWPA is an evolutionary computation technique which possesses superior performance in terms of accuracy, stability, convergence speed and robustness. It has three artificial intelligent behaviors including scouting behavior, calling behavior, and besieging behavior and two intelligent rules, i. e., the winner-take-all generating rule for the lead wolf and the stronger-survive renewing rule for the wolf pack. First, the scouting behavior accelerates the possibility that the UWPA can fully traverse the whole solution space. Secondly, the winner-take-all rule and the calling behavior cause the wolves to move towards the lead wolf whose position is the nearest to the prey. They also cause wolves to arrive at the neighborhood of the global optimum only after a few iterations have elapsed, since the step in the calling behavior is the largest one. Thirdly, with the smallest step, besieging behavior ensures the ability to open up a new solution space and carefully search for the global optimum in a good solution area. Fourthly, with the stronger-survive renewing rule, the algorithm obtains several new wolves whose positions are near the lead wolf. Also, it allows for more latitude of search space to find the global optimum, while maintaining population diversity in each iteration.

The steps of the algorithm are described as follows:

Step 1 Initialization. Initialize the following parameters: The initial position of wolf X_i; the number of the wolves N; the maximum number of evaluations $k_{\max}$; the maximum repetition number in scouting behavior $T_{\max}$; the step coefficient S; the distance coefficient w; and the population renewal coefficient β.

Step 2 The wolf with the best smell concentration is regarded as the lead wolf. The rest of the $N-1$ wolves first act as the scout wolves to take the scouting behavior until $Y_i < Y_{\text{lead}}$, where Y_i is the smell concentration of prey perceived by wolf i; or the maximum repetition number $T_{\max}$ is attained and then go to Step 3.

Step 3 Except for the lead wolf, the rest of the $N-1$ wolves secondly act as the ferocious wolves and gather towards the lead wolf according to

$$X_i^{k+1} = X_i^k + \frac{\text{step}_b (G^k - X_i^k)}{\mid G^k - X_i^k \mid} \quad (4)$$

where step_b is the step size in calling behavior; G^k is the position of the artificial lead wolf at the k-th iteration; and X_i^k is the position of wolf i at the k-th iteration. If $Y_i < Y_{\text{lead}}$, go back to Step 2; otherwise, the wolf i continues running until $L(i, l) < L_{\text{near}}$, where L_{near} is the distance determinant coefficient; then go to Step 4.

Step 4 The position of wolf who takes the besieging behavior is updated according to

$$X_i^{k+1} = X_i^k + \lambda \, \text{step}_c \mid G^k - X_i^k \mid \quad (5)$$

where step_c is the step length in besieging behavior; λ is a random number uniformly distributed at the interval $[-1, 1]$.

Step 5 Update the position of the lead wolf under the winner-take-all generating rule and update the wolf pack.

Step 6 If the program meets the precision requirement or reaches the maximum number of evaluations, the position and function value of the lead wolf, and the optimal solution of the problem are outputted; otherwise, go to Step 2.

3 System Identification with UWPA

The approach of the system identification with UWPA is represented in this section. Assuming that the number of the polynomial coefficients is seven and the order of the FIR filter is three, the real model parameters form a feature vector and it is expressed as

$$\boldsymbol{\theta} = [b_1 \quad b_3 \quad b_5 \quad b_7 \quad h_1 \quad h_2 \quad h_3] \quad (6)$$

and the estimated parameters are written as a vector

$$\hat{\boldsymbol{\theta}} = [\hat{b}_1 \quad \hat{b}_3 \quad \hat{b}_5 \quad \hat{b}_7 \quad \hat{h}_1 \quad \hat{h}_2 \quad \hat{h}_3] \quad (7)$$

The objective of the identification of the Hammerstein model is to find the optimal parameter vector to minimize an objective function with the known input $d(n)$ and the output data $y(n)$. The objective function can be defined based on a least-mean-square-error criterion (LMSE) as follows:

$$f(\hat{\boldsymbol{\theta}}) = \frac{1}{D} \sum_{i=1}^{D} \mid y(k-i) - \hat{y}(k-i) \mid^2 \quad (8)$$

where D is the signal sample length; $y(k)$ is the true output; and $\hat{y}(k)$ is the estimated output. The value of the objective function is regarded as the smell concentration of prey. Therefore, the identification of the model with UWPA is transformed into a minimization problem of the MSE.

4 Spoofing Interference Detection

Since the parameters have been estimated by the UWPA, we utilize a naive method for the detection of spoofing, which directly compares the Euclidean distance between the estimated parameter vector and the real parameter vector. The decision rule can be written as

$$|\hat{\boldsymbol{\theta}} - \boldsymbol{\theta}_1| \underset{H_1}{\overset{H_0}{\gtrless}} |\hat{\boldsymbol{\theta}} - \boldsymbol{\theta}_2| \tag{9}$$

where H_0 means that the received signal is a spoofing signal; H_1 means that the signal is a genuine GNSS signal.

5 Experiments

To demonstrate the identification performance of the algorithms, simulations are carried out. We assume that the GNSS signal is a GPS C/A signal and the modulation method is QPSK. The parameters of the nonlinear static block and the linear dynamic block are set, as shown in Tab. 1. Suppose that the spoofing is generated by a repeater. So, the spoofing signal is very similar to the genuine GNSS signal and the two vectors of parameters in Tab. 1 are set to be very close to each other.

Tab. 1 Parameters configuration

Coefficients	Nonlinear subsystem				Linear subsystem		
	b_1	b_3	b_5	b_7	h_1	h_2	h_3
Transmitter	1	−0.013 5	−0.008 6	−0.001 7	0.990 6	0.062 8	0.007 9
Spoofer	1	−0.018 7	−0.005 3	−0.001 9	0.972 3	0.116 3	0.019 4

Suppose that the parameter vector $\boldsymbol{\theta}_1$ comes from a GPS transmitter and $\boldsymbol{\theta}_2$ comes from a spoofer. Then the similarity between them can be calculated by $\cos\alpha = (\boldsymbol{\theta}_1^{\mathrm{H}}\boldsymbol{\theta}_2)/(|\boldsymbol{\theta}_1||\boldsymbol{\theta}_2|)$, where α is the angle between the two parameter vectors. The cosine value of the angle between the two parameter vectors listed in Tab. 1 is 0.998 4 and the angle is 3.284 4°, which means a high similarity.

For the purpose of comparison, simulations are also executed using the LS algorithm, the iterative method and the BA[13]. For each algorithm, 1 000 independent experiments are conducted. The maximum iterative number of the iterative method is 5 000. The maximum evaluation number and the population size of the UWPA and the BA are 5 000 and 50, respectively. The parameters of BA are set as follows: the initial loudness $A_0 = 1$; the initial emission rate $r_0 = 0.5$; $\alpha = 0.95$; $\gamma = 0.9$; and the frequency range is $[0, 2]$. The parameters of UWPA are set as follows: the maximum repetition times in scouting behavior $T_{\max} = 20$; the distance determinant coefficient $w = 100$; the step coefficient $S = 300$; and the population renewal proportional coefficient $\beta = 3$.

All the algorithms are tested in Matlab 2014a using the same computer with a Dual-Core 2.80 GHz processor, running Windows 7 operating system with over 4 GB of memory.

Tab. 2 shows the runtime of these four algorithms. The runtime of the UWPA and BA is shorter than that of the iterative method, because the iterative method does not converge when it reaches the designated maximum number of iterations. The LS is the fastest one as it is a non-iterative method. The runtime of the BA is shorter than that of the UWPA since the UWPA has more intelligent behaviors than the BA.

Tab. 2 Runtime of four algorithms

Algorithms	UWPA	BA	Iterative	LS
Runtime/s	514.48	120.25	1207.50	0.37

Fig. 2 illustrates the curves of the average relative error (ARE) vs. SNR. The relative error can be calculated by $0.5(|E(\hat{\boldsymbol{\theta}}_1) - \boldsymbol{\theta}_1|/|\boldsymbol{\theta}_1| + |E(\hat{\boldsymbol{\theta}}_2) - \boldsymbol{\theta}_2|/|\boldsymbol{\theta}_2|)$. Not surprisingly, the AREs of these four algorithms decrease with the increase in SNR. The AREs of the LS approach and the iterative method are much greater than those of the UWPA and the BA, because these two methods are much more sensitive to noise than the UWPA and the BA. Moreover, the ARE of the UWPA is 0.026 8 lower on average than that of the BA when SNR ranges from 2 to 16 dB.

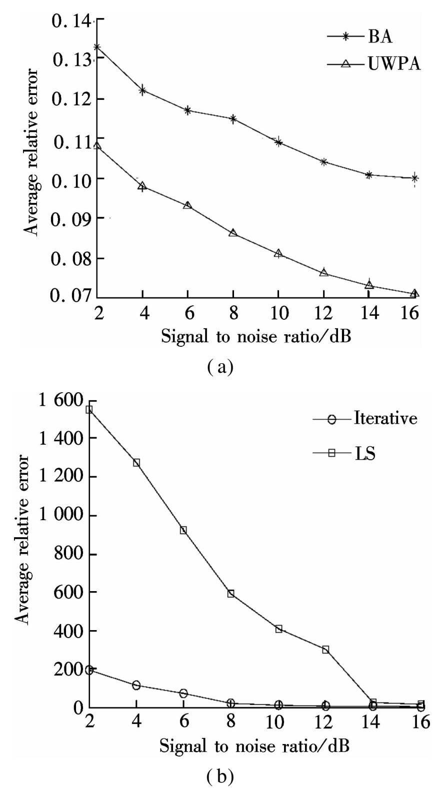

Fig. 2 Identification average relative error vs. signal to noise ratio. (a) UWPA and BA; (b) Iterative and LS

Fig. 3 illustrates the curves of the GNSS spoofing detection rate vs. the SNR. The range of the SNR is set to be 2 to 16 dB. As expected, the detection rates of the UWPA and the BA increase with the increase of the SNR, and reach 1 when the SNR is 14 dB. However, the performances of the iterative method and LS are poor. In addition, the average detection rate of the UWPA is 4.93% higher than that of the BA when the SNR ranges from 2 to 14 dB. The reason is that the cooperation among the lead wolf, scout wolves and ferocious wolves makes nearly perfect predation. Additionally, the three artificial intelligent behaviors makes UWPA not only fully traverse the whole solution space but also carefully search the global optimum point in the feasible solutions area. Therefore, conclusion can be drawn that the identification approach with the UWPA is much more effective, even for relatively low signal-to-noise ratios where the iterative method and the LS approach failed to identify the spoofing signal.

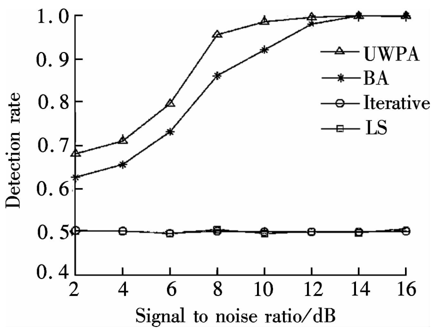

Fig. 3 Detection rate vs. signal to noise ratio

6 Conclusion

In this paper, we propose a GNSS spoofing identification approach based on the UWPA. The Hammerstein model is employed for modeling the real GNSS transmitter, the spoofer and the wireless channel. The experimental results show that the proposed method can obtain a higher spoofing detection rate and less ARE than the BA, LS and iterative methods. Our method can also work effectively on relatively low SNRs.

References

[1] Basker S. Jamming: A clear and present danger[J]. *GPS World*, 2010, **21**(4):8 − 9.

[2] Nielsen J, Broumandan A, Lachapelle G. Spoofing detection and mitigation with a moving handheld receiver[J]. *GPS World*, 2010, **21**(9):27 − 33.

[3] Humphreys T E, Ledvina B M, Psiaki M L, et al. Assessing the spoofing threat: Development of a portable GPS civilian spoofer[C]// *ION GNSS Conference*. Savanna, USA, 2008:2314 − 2325.

[4] Montgomery P Y, Humphreys T E, Ledvina B M. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer[C]// *Proceedings of the Institute of Navigation International Technical Meeting*. Anaheim, USA, 2009: 124 − 130.

[5] Polak A C, Dolatshahi S, Goeckel D L. Identifying wireless users via transmitter imperfections[J]. *IEEE Journal on Selected Areas in Communications*, 2011, **29**(7): 1469 − 1479. DOI:10.1109/jsac.2011.110812.

[6] Liu M W, Doherty J F. Nonlinearity estimation for specific emitter identification in multipath channels[J]. *IEEE Transactions on Information Forensics and Security*, 2011, **6**(3):1076 − 1085.

[7] Lennart Ljung. *System identification—theory for the user* [M]. Beijing: Tsinghua University Press, 2002.

[8] Bai E W, Li D. Convergence of the iterative Hammerstein system identification algorithm[J]. *IEEE Transactions on Automatic Control*, 2004, **49**(11):1929 − 1940. DOI:10.1109/tac.2004.837592.

[9] Wu H S, Zhang F M. A uncultivated wolf pack algorithm for high-dimensional functions and its application in parameters optimization of PID controller[C]// *IEEE Congress on Evolutionary Computation.* Beijing, China, 2014: 1477 − 1482.

[10] Wu H S, Zhang F M, Wu L S. New swarm intelligence algorithm—wolf pack algorithm[J]. *Systems Engineering and Electronics*, 2013, **35**(11): 2430 − 2438. (in Chinese)

[11] Barradas F M, Cunha T R, Lavrador P M, et al. Polynomials and LUTs in PA behavioral modeling: A fair theoretical comparison[J]. *IEEE Transactions on Microwave Theory and Techniques*, 2014, **62**(12): 3274 − 3285. DOI:10.1109/tmtt.2014.2365188.

[12] Hong X, Chen S, Gong Y, et al. Nonlinear equalization of Hammerstein OFDM systems[J]. *IEEE Transactions on Signal Processing,* 2014, **62**(21): 5629 − 5639. DOI: 10.1109/tsp.2014.2355773.

[13] Yang X S. A new metaheuristic bat-inspired algorithm [J]. *Nature Inspired Cooperative Strategies for Optimization*, 2012, **284**: 65 − 74. DOI: 10.1007/978-3-642-12538-6_6.

基于狼群算法的 GNSS 欺骗干扰识别

孙闽红[1,2] 邵章义[2] 包建荣[2] 余旭涛[1]

([1] 东南大学信息科学与工程学院,南京 210096)
([2] 杭州电子科技大学通信工程学院,杭州 310018)

摘要:为解决卫星导航接收机在受到欺骗干扰时难以识别欺骗干扰这一问题,提出了一种基于模型的欺骗干扰识别方法. 首先将干扰机/卫星发射机以及通信信道建模为 Hammerstein 模型,然后使用一种新的模型辨识方法——狼群算法来进行模型参数辨识. 将估计得到的模型参数作为特征参数,使用欧氏距离比较法实现欺骗干扰的识别. 仿真实验验证了所提方法的有效性和鲁棒性. 结果表明:狼群算法与最小二乘法、迭代法和蝙蝠算法等其他模型辨识算法相比,虽然在算法时间复杂度上比最小二乘法和蝙蝠算法略高,但具有更高的模型参数辨识精度和欺骗干扰识别率,甚至在信噪比较低时识别性能也最优.

关键词:全球卫星导航系统;欺骗干扰检测;系统辨识;狼群算法

中图分类号:TN973