GPS Spoofing Detection Based on Decision Fusion with a K-out-of-N Rule

Minhong Sun[1,2], Yuan Qin[2], Jianrong Bao[1,2] and Xutao Yu[1]
(Corresponding author: Minhong Sun)

School of Information Science and Engineering, Southeast University[1]
No.2, Sipailou, Nanjing, Jiangsu Province 210096, P. R. China
School of Communication Engineering, Hangzhou Dianzi University[2]
No. 1, Ave. 2, Xiasha Tertiary Education Zone, Hangzhou, Zhejiang Province 310018, P. R. China
(Email: cougar@hdu.edu.cn)
(Received May 12, 2016; revised and accepted Aug. 3 & Sept. 3, 2016)

Abstract

In order to obtain higher detection probability of the GPS spoofing, a general identification scheme with decision fusion is proposed. Firstly, the singular values of the wavelet transformation coefficients of both spoofing and genuine signal are computed and formed as the feature vectors. Then, the feature vectors are input into three classifiers, which are the support vector machines (SVM), the probabilistic neural networks (PNN) and the decision tree (DT), respectively, for GPS spoofing identification. Finally, the results of the three classifiers are fused with a K-out-of-N decision rule, and the final classification result is obtained. Simulation results exhibit the effectiveness of the proposed scheme, whose detection probability has increased by 3.75%, 5.06% and 12.36% than that of the SVM, the PNN and the DT on average, respectively. Moreover, the false alarm probability of the proposed scheme is lower than that of the three classifiers. In addition, the area under curve (AUC) is given to verify the effectiveness and feasibility of the proposed method.

Keywords: Decision Fusion; Feature Extraction; GPS; Spoofing Detection

1 Introduction

A GPS spoofing is an intentional jamming, which is very similar to a true navigation signal. Spoofing interference deceives a GPS receiver to capture the jamming signal, which may cause serious security problems, such as erroneous synchronization time and false position, or no information output [10]. The key task for GPS receiver against spoofing is to identify it correctly. Existing works focused on the detection of spoofing with many different signal features, such as signal power, pseudorange measurements [13], time of advent, signal parameters estimation [6] etc. However, most of them applied only one classifier/detector. The utilization of multi-classifiers with a decision fusion technique to further improve the detection performance is ignored.

In this paper, several classifiers have been proposed to detect spoofing attack, including the support vector machines (SVM) [9], the probabilistic neural networks (PNN) [11], and the decision tree (DT) [7], etc. Although each classifier functions well, the detection performance can be further improved. Seeking higher detection probability of spoofing, we focus on the multi-classifiers fusion technique with a K-out-of-N decision rule. Due to high reliability, the K-out-of-N rule has a wide and success utilization in many fields [1]. In this paper, we present a GPS spoofing identification method based on the multi-classifiers fusion. The approach is divided into three steps. Firstly, we extract the singular values of the wavelet transformation (WT) coefficients of a signal as a feature vector. By the singular value decomposition (SVD), the quantity of the calculation can be reduced notably [5]. Secondly, based on the same feature vector, three different classifiers, i.e. SVM, PNN and DT, are adopted in the identification of the spoofing, respectively. Thirdly, with the recognition results of each classifier, final identification result is obtained by decision fusion with the K-out-of-N rule.

The rest of the paper is organized as follows. Section 2 describes the feature extraction steps of the received signals. Section 3 introduces three methods of the classifiers briefly. Section 4 illustrates the decision fusion scheme based on the K-out-of-N rule. Simulations and performance analyses are presented in Section 5. Finally, a brief conclusion is given in Section 6.

2 Features Extraction

Two maps are defined in this section for the process of features extraction. The first uses the WT to map a one-

dimensional (1-D) received signal to a two-dimensional (2-D) time-frequency matrix, and the second maps the 2-D signal to a 1-D vector with SVD.

2.1 WT

Assuming the received signal in a navigation receiver is $x(t)$, we can define a map as

$$f[x(t)] \rightarrow \boldsymbol{W}$$

where $f[\cdot]$ is a WT operator, $\boldsymbol{W}$ is a time-frequency matrix and it can be represented as $\boldsymbol{W} = [\boldsymbol{d}_1, \boldsymbol{d}_2, \cdots, \boldsymbol{d}_j, \boldsymbol{a}_j]$. The columns of $\boldsymbol{W}$ are represented by

$$\boldsymbol{d}_j = \boldsymbol{V}_j\, x(t) = \frac{1}{\sqrt{2}} \sum_{n \in \mathbb{Z}} g(n) \boldsymbol{S}_{j-1} x(t - 2^{j-1} n)$$

$$\boldsymbol{a}_j = \boldsymbol{S}_j\, x(t) = \frac{1}{\sqrt{2}} \sum_{n \in \mathbb{Z}} h(n) \boldsymbol{S}_{j-1} x(t - 2^{j-1} n)$$

where n and j denote the filter and decomposition level, respectively; $h(n)$ and $g(n)$ indicate the low-pass and high-pass decomposition filters, respectively; $\boldsymbol{S}_j$ and $\boldsymbol{V}_j$ denote the approximation coefficients and the detail coefficients of level j, respectively.

2.2 SVD

SVD is an effective method to reduce data dimension. Utilizing the SVD of a matrix in computations has the advantage of being more robust to numerical errors. The SVD exposes the geometric structure of a matrix, which is an important aspect in many matrix calculations. Then the second map is defined by the following expression as

$$g[\boldsymbol{W}] \rightarrow \boldsymbol{\theta}.$$

3 Classifiers

Because of their good classification performance and wide applications, three main approaches, i.e. SVM, PNN and DT, are chosen for the identification of the GPS spoofing in our scheme.

3.1 SVM

The SVM is based on the Vapnik-Chervonenks dimension of statistical learning theory and structural risk minimization inductive principle, which can deal with small samples, non-linear and high dimension pattern recognition problems [12]. Moreover, it does not suffer from overfitting and it has good ability of generalization. The decision function of it can be represented as

$$f(x) = \operatorname{sgn}\left(\sum_{i=1}^{l} \alpha_i y_i K(\boldsymbol{x}_i, \boldsymbol{x}) + b\right)$$

where $\boldsymbol{x}_i$ is the support vector, $y_i \in \{-1, 1\}$ is the class label, $K(\boldsymbol{x}_i, \boldsymbol{x})$ is the kernel function, α_i is the Lagrangian multiplier, b is the classification threshold, $\operatorname{sgn}(\cdot)$ is the signum function. Comparing with other kernel functions, radial basis kernel function (RBF) has the advantage of higher precision, less parameters, and better performance [12]. Hence, a RBF is applied in our case and it is expressed as

$$K(\boldsymbol{x}_i, \boldsymbol{x}) = \exp\{-\|\boldsymbol{x}_i - \boldsymbol{x}\|^2 / \sigma^2\}$$

where σ^2 is the kernel parameter.

3.2 PNN

The PNN is a parallel algorithm with supervised learning which uses Bayes decision rule and Parzen window [8]. Especially in the application of solving the classification problems, the superiority of it is obvious. It can use linear learning algorithm to accomplish the work by nonlinear learning algorithm, while it keeps the nonlinear features such as high accuracy of the algorithm.

The output of the output layer can be expressed as

$$if \quad n_j = \max_k(n_k) \quad y_j = 1 \quad else \quad y_j = 0$$

where n denotes the output of summation layer, k is the number of samples in training set, j indicates the number of max layers. The probability value n_j corresponding to the maximum is 1, i.e. $y_j = 1$ and the rest values are 0, i.e. $y_j = 0$.

3.3 DT

A decision tree has a flowchart-like tree structure, where each non-leaf node denotes a test on a pattern attribute, each branch represents an outcome of the test, and each leaf node is labeled by a class [3]. Up to now, many approaches have been proposed for decision trees, such as ID3 and C4.5 [3]. We use C4.5 which is an extension of ID3. C4.5 algorithm selects properties by information gain ratio, which is written as

$$GainRatio(\boldsymbol{S}, \boldsymbol{A}) = \frac{Gain(\boldsymbol{S}, \boldsymbol{A})}{SplitInformation(\boldsymbol{S}, \boldsymbol{A})}$$

where $\boldsymbol{S}$ and $\boldsymbol{A}$ denote the sample set and the properties, respectively. $Gain(\boldsymbol{S}, \boldsymbol{A})$ and $SplitInformation(\boldsymbol{S}, \boldsymbol{A})$ are the information gain and split information, respectively.

4 Decision Fusion

In order to make a more accurate decision for the spoofing detection, a decision fusion approach is presented and capable of overcoming the disadvantage of single classifier, and eliminating the system uncertainty. The K-out-of-N rule is also selected for the decision fusion.

Each classifier is independent. The binary decision at the ith classifier to decide the real signal or the deceptive

jamming is given by

$$\begin{cases} H_0: \ u_i = 0 \\ H_1: \ u_i = 1 \end{cases}$$

where $i = 1, 2, \cdots, N$, H_0 represents the real signal, H_1 represents the spoofing signal, N is the number of classifiers, and u_i is the output of the ith classifier.

The results above are input into the fusion center with the K-out-of-N rule. The following expression describes the K-out-of-N rule, i.e.

$$\begin{cases} H_0: \ u_i = 0 \ if \ \sum_{i=1}^{N} u_i < K \\ H_1: \ u_i = 1 \ if \ \sum_{i=1}^{N} u_i \geq K \end{cases} \quad (1)$$

where u_0 is the final decision. The Equation (1) demonstrates that if the sum of the outputs of N classifiers is larger than or equal to K, the spoofing signal is detected, i.e., H_1. Otherwise, the received signal is a real one, i.e., H_0. Then the OR rule corresponds to the case of $K = 1$ and the AND rule corresponds to the case of $K = N$.

The overall performance of detection is evaluated by two indicators, such as the overall detection probability (PD) and the overall false alarm probability (PF). PD and PF are expressed respectively as follows [1]

$$P_D = \sum_{j=k}^{N} \sum_{\sum u_i = j} \prod_{i=1}^{N} (P_{di})^{u_i} (1 - P_{di})^{1-u_i}$$

$$P_F = \sum_{j=k}^{N} \sum_{\sum u_i = j} \prod_{i=1}^{N} (P_{fi})^{u_i} (1 - P_{fi})^{1-u_i}$$

where P_{di} and P_{fi} represent the detection probability $p(H_1|H_1)$ and false alarm probability $p(H_1|H_0)$ of the ith classifier, respectively.

5 Simulations and Analyses

In this section, the performance of the detection based on decision fusion method is simulated and analyzed, to verify the effectiveness of the proposed algorithm. Both the detection probability and false alarm probability are used in the analyses with numerical computations.

Suppose that a GPS signal is a C/A code signal with QPSK modulation. SNR is set from 2dB to 14 dB with a step of 1dB. Then, the experiments with K-out-of-N rule and three single classifiers are carried out. In order to generate a spoofing jamming signal, which is very similar to a real satellite navigation transmitter, a Hammerstein model is used [2], which is composed of a static nonlinear subsystem followed by a dynamic linear subsystem. A satellite transmitter or a spoofer is regarded as a static nonlinear subsystem, which is modeled as a memoryless polynomial model. The wireless channel is regarded as a dynamic linear subsystem, which is expressed as a FIR filter. The relationship between the input and output of the whole system is given as

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

where M is the number of the polynomial coefficients, $d(n)$ denotes the input signal, b_{2i-1} is the polynomial coefficients, h_k is the channel response coefficient, N denotes the order of FIR filter, $W(n) \sim \mathcal{N}(0, \sigma^2)$ indicates additive Gaussian white noise (AWGN). Different systems are simulated with different vectors of the parameters $[b_{2i-1} \ h_k]$. Two training sets consisting of 1500 sample signals per class, and two test sets consisting of 500 sample signals per class are generated by the Hammerstein model. Each sample signal contains 500 points.

Two sets of parameters are set and shown in Table 1. One is from the satellite transmitter, and the other is from the spoofer. The two models' parameters are set to be very close to each other, for the spoofing signals are very similar to the real ones.

With the foregoing features extraction method, the feature vectors are calculated. The average singular values of the real signal and the jamming signal are shown in Table 2 for the case of the SNR being 10dB.

For each SNR, 200 independent experiments were run. The outputs of each classifier and the final detection results on the basis of the K-out-of-N rule are obtained. The detection curves are illustrated in Figure 1 and Figure 2.

From Figure 1, we can see that the detection probability is increased with the increasing of the SNR values. The average detection probability of the decision fusion method has increased by 3.75%, 5.06% and 12.36% than that of the SVM, the PNN and the DT, respectively. Hence, cooperation among classifiers can be used in order to improve the reliability of the detection results. From Figure 2, it is evident that the false alarm probabilities of the four methods are lower than 0.1. The average false alarm probability of decision fusion method has decreased by 1.25% than that of the SVM, by 3.70% than that of the PNN, and by 7.28% than that of the DT, respectively. Therefore, the detection performance of the three classifiers is improved by the decision fusion method.

Receiver operating characteristic (ROC) curve is commonly used to characterize the detection performance. However, with this metric, the performance comparison with multiple classifiers would be difficult. An alternative metric, based on the area under the ROC curve (AUC) seems appropriate in this situation. The AUC can be calculated by

$$AUC = \frac{S_0 - n_0(n_0+1)/2}{n_0 n_1}$$

where n_0 and n_1 are the numbers of positive and negative samples, respectively, and $S_0 = \sum r_i$, where r_i is the rank of the ith positive example in the ranked list [4].

The larger value of AUC is, the better performance of the classifier will have. The AUC values for the four

Table 1: Parameters configuration

	parameter $\boldsymbol{b}$ of the nonlinear subsystem				parameter $\boldsymbol{h}$ of the linear subsystem		
	b_1	b_3	b_5	b_7	h_1	h_2	h_3
Transmitter	1	-0.0735	-0.0986	-0.0547	0.9906	0.0628	0.0079
Spoofer	1	-0.0728	-0.0976	-0.0542	0.9807	0.0622	0.0078

Table 2: Singular values of signals (SNR=10dB)

	Singular Values								
Real signal	57.43	45.01	36.43	32.50	27.24	23.90	20.95	16.19	9.48
Spoofing signal	56.00	43.89	35.51	31.71	26.56	23.30	20.43	15.78	9.24

methods with different SNR are shown in Table 3. By comparing the AUC, we draw a conclusion that the performance of the decision fusion method is better than the other three methods with a single classifier.

Table 3: AUC comparison

AUC	5dB	10dB	15dB
SVM	0.8931	0.9535	0.9801
PNN	0.8357	0.9401	0.9890
DT	0.7962	0.8731	0.9070
K/N	0.9030	0.9672	0.9900

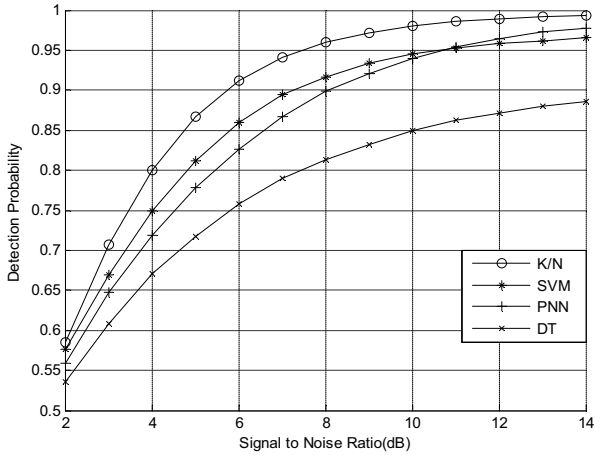

Figure 1: Detection probability comparison between fusion and single classifier

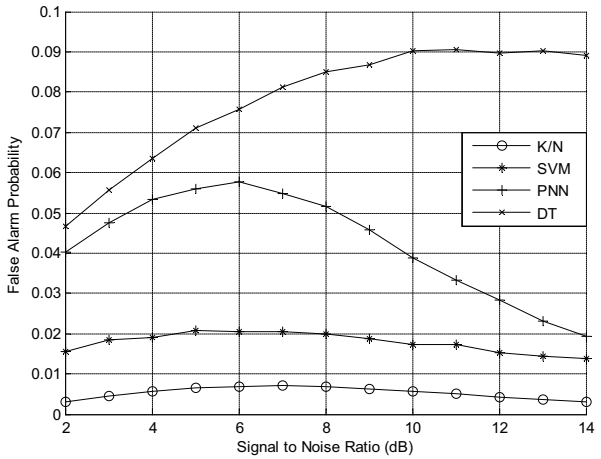

Figure 2: False alarm probability comparison between fusion and single classifier

6 Conclusion

We have shown that the overall detection precision of GPS spoofing jamming is improved by using a decision fusion method with the K-out-of-N rule. A spoofing signal is detected if at least K out of N classifiers have made the same decision. As cooperation among classifiers, the reliability of the detection results is improved. Simulation results are presented to demonstrate the effectiveness of the approach, whose detection probability is higher than that of the three classifiers, i.e. SVM, PNN and DT, and the false alarm probability is lower than that of the three classifiers, in the case of SNR ranging from 2dB to 14dB. Furthermore, it is illustrated with AUC that the proposed method is more effective than the methods with only a single classifier.

Acknowledgments

This work was supported by the Natural Science Foundation of China (No.61271214, No.61471152), by the Postdoctoral Science Foundation of Jiangsu Province (No.1402023C) and by the Zhejiang Provincial Natural Science Foundation of China (No. LZ14F010003).

References

[1] S. Althunibat, M. D. Renzo, and F. Granelli, "Optimizing the k-out-of-n rule for cooperative spectrum sensing in cognitive radio networks," in *IEEE Global Communications Conference (GLOBECOM'13)*, pp. 1607–1611, Atlanta, USA, Dec. 2013.

[2] F. M. Barradas, T. R. Cunha, P. M. Lavrador, and J. C. Pedro, "Polynomials and luts in pa behavioral modeling: A fair theoretical comparison," *IEEE Transactions on Microwave Theory and Techniques*, vol. 62, no. 12, pp. 3274–3285, 2014.

[3] H. W. Chiu, C. S. Ouyang, and S. J. Lee, "Improved c-fuzzy decision trees," in *IEEE International Conference on Fuzzy Systems (Fuzz-IEEE'06)*, pp. 1763–1768, Vancouver, Canada, July 2006.

[4] D. J. Hand and R. J. Till, "A simple generalisation of the area under the roc curve for multiple class classification problems," *Machine Learning*, vol. 45, no. 2, pp. 171–186, 2001.

[5] N. C. Kim and H. J. So, "Comments on svd-based modeling for image texture classification using wavelet transform," *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 5408–5408, 2013.

[6] J. Kou, S. Xiong, S. Wan, and H. Liu, "The incremental probabilistic neural network," in *International Conference on Natural Computation (ICNC'10)*, pp. 1330–1333, Yantai, China, Aug. 2010.

[7] X. Liu and W. Jin, "Performance analysis of bootstrap based distributed detector under correlated k-distributed clutter," in *Asian-Pacific Conference on Synthetic Aperture Radar (APSAR'09)*, pp. 556–559, Xi'an, China, Oct. 2009.

[8] S. Mishra, C. N. Bhende, and B. K. Panigrahi, "Detection and classification of power quality disturbances using s-transform and probabilistic neural network," *IEEE Transactions on Power Delivery*, vol. 23, no. 1, pp. 280–287, 2008.

[9] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving zigbee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 225–230, 2015.

[10] M. L. Psiaki, "Gps spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aeroapce and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[11] Y. Yan, Q. Tian, and Y. Wang, "Performance analysis of detection algorithm for follower noise jamming in nakagami fading channels," *Chinese Journal of Radio Science*, vol. 29, no. 4, pp. 738–744, 2014.

[12] H. Yang, X. Xie, and R. Wang, "Som-ga-svm detection based spectrum sensing in cognitive radio," in *Wireless Communications, Networking and Mobile Computing (WiCOM 2012)*, pp. 1–7, Shanghai, China, Sept. 2012.

[13] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, 2013.

Biography

Minhong Sun received his Ph.D. E.E. degree from the Department of Electronic Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2008. He is with the school of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His main research interests include signal processing and information countermeasures.

Yuan Qin received her M.S.E.E. degree from Hangzhou Dianzi University, Hangzhou, China, in 2016. Her main research interests include machine learning and information countermeasures.

Jianrong Bao received his B.S. degree in Polymeric Materials & Eng., and the M.S.E.E. degree both from Zhejiang University of Technology, Hangzhou, China, in 2000 and 2004, respectively. He received his Ph.D. E.E. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2009. He is with the school of Information Engineering, Hangzhou Dianzi University, Hangzhou, China. His main research interests include wireless communication and so on.

Xutao Yu received the BS and MS degrees from Hohai University, Nanjing, China in 1997 and 2000, respectively, and the PhD degree from Southeast University, Nanjing, China in 2004, all in communication and information systems. Since 2004, she has been with the the State Key Laboratory of Millimeter Waves and is currently a professor there. She has published over 80 papers and issued over 20 patents. Her research area is wireless communication.