sensors

MDPI

Article

A Method of Detections' Fusion for GNSS Anti-Spoofing

Huiqi Tao, Hong Li * and Mingquan Lu

Department of Electronic Engineering, Tsinghua University, Beijing 100084, China; thq12@mails.tsinghua.edu.cn (H.T.); lumq@mail.tsinghua.edu.cn (M.L.)
* Correspondence: lihongee@tsinghua.edu.cn; Tel.: +86-10-6277-1669

Academic Editor: Vittorio M. N. Passaro
Received: 21 October 2016; Accepted: 14 December 2016; Published: 19 December 2016

Abstract: The spoofing attack is one of the security threats of systems depending on the Global Navigation Satellite System (GNSS). There have been many GNSS spoofing detection methods, and each of them focuses on a characteristic of the GNSS signal or a measurement that the receiver has obtained. The method based on a single detector is insufficient against spoofing attacks in some scenarios. How to fuse multiple detections together is a problem that concerns the performance of GNSS anti-spoofing. Scholars have put forward a model to fuse different detection results based on the Dempster-Shafer theory (DST) of evidence combination. However, there are some problems in the application. The main challenge is the valuation of the belief function, which is a key issue in DST. This paper proposes a practical method of detections' fusion based on an approach to assign the belief function for spoofing detections. The frame of discernment is simplified, and the hard decision of hypothesis testing is replaced by the soft decision; then, the belief functions for some detections can be evaluated. The method is discussed in detail, and a performance evaluation is provided, as well. Detections' fusion reduces false alarms of detection and makes the result more reliable. Experimental results based on public test datasets demonstrate the performance of the proposed method.

Keywords: GNSS; spoofing; detection; fusion; Dempster-Shafer theory; belief function

1. Introduction

The security of the Global Navigation Satellite System (GNSS) is deeply concerned with the rapid development of GNSS applications. Due to the weakness of the power and the openness of the signal characteristics, GNSS receivers are vulnerable to interferences, and the signals are easy to counterfeit. There have been several reports about successful GNSS spoofing, which could cause great damage to important infrastructures, such as the telecommunication network, the power grid, etc. Therefore, anti-spoofing technology attracts researchers' attention [1].

There have been many methods of GNSS spoofing detection and exclusion [1–4]. They can be classified into three categories. The first can be named signal design. The typical method is cryptographic authentication. Encrypted military signals, such as the GPS P(Y) code and M code, could not be duplicated by the spoofer; however, their target user group is limited, and most commercial users do not have the authority to access these signals. Besides, cryptographic authentication is powerless to prevent repeat spoofing, which transmits the delayed copy of authentic signals. The second category can be called external aids. GNSS measurements and solutions can be checked with external systems, such as inertial measurement units (IMU), compass, cellular network positioning, etc. [3,5]. The external systems are independent of GNSS, and they are not affected by GNSS spoofing. However, external aids increase the complexity of the user receiver, and they are expensive to implement in general receivers. The third category can be called GNSS signal processing. There are many methods in this category, such as multi-antenna processing [6,7], signal power monitoring [8], correlation domain

monitoring [9,10], vestigial signal detection, receiver autonomous integrity monitoring (RAIM) [4] and the extended method [11], etc. In addition, some crossing methods are proposed; for example, the authors of [12] propose a method based on machine learning and signal processing to monitor the interference of GNSS. However, there are shortcomings in these methods, and some of them are complementary in anti-spoofing. The cooperation of multiple spoofing detections is necessary to improve the performance of GNSS anti-spoofing.

Information fusion is a key issue of the cooperation of multiple spoofing detections. There are many methods to fuse the information of different detectors, such as Bayesian data fusion, the Kalman filtering method, Dempster–Shafer theory (DST), etc. However, there are some obstacles in the applications. For example, a priori knowledge of the detectors is needed for Bayesian data fusion. The statistical properties of most detectors are known in the case of authentic GNSS signals, but uncertain in the case of spoofing signals, i.e., a priori information of the GNSS spoofing detectors is partially unknown. The uncertainty makes it impossible to apply Bayesian inference to calculate the posterior probabilities of the possible results. For the Kalman filtering method, the precise estimate of the noise covariances, including the covariances of process noise and observation noise, is very important in applications. However, a precise estimate is hard to obtain in the case of spoofing, because the style of spoofing is varied and unknown. DST [13] is a general framework for reasoning with uncertainty, and it provides a solution to combine evidence from different sources. It is suitable for use in situations where a priori information of detectors is partially unknown. The authors of [14] propose the framework of a mathematic model for conjunct GNSS spoofing detection. The model is based on the DST. However, it does not give the way to valuate the basic probability assignment (BPA) or belief function for each possible result of detection. Thus, the method cannot be implemented in practice. This paper focuses on this problem of DST and proposes a method to overcome this difficulty.

Each spoofing detection makes a decision according to the anomaly of the signal. Usually, it is a hard decision to discern the authenticity of the received signals. A hard decision is easy to implement, but it loses some information of measurement. Thus, false decision cannot be rectified. Meanwhile, most spoofing detections are equivalent to hypothesis testings, and the test statistics are quantifications of the anomaly of measurements or signal features. The quantification of the anomaly is equivalent to a soft decision that indicates the degree of anomaly, and the soft decision can be used to evaluate the belief function in binary detection. This makes it possible to implement the DST if the frame of discernment is simplified properly while the belief function is constructed on the basis of the quantification of the anomaly.

This paper proposes a method to deal with this problem. There are two main points for the purpose of implementation. The first is to extract a simplified frame of discernment for spoofing detection. Compared with the existing method, some elements in the complete, but redundant frame of discernment are excluded, and only two basic and mutually exclusive elements are left. This is conducive to the valuation of belief functions. The second point and the main contribution of this work is to construct the belief function for each possible result of detections. The belief function is proposed based on the model of hypothesis testing for a spoofing detector. These two points make it feasible to fuse the information from multiple spoofing detections.

The remainder of this paper is organized as follows. Section 2 describes the method of spoofing detections' fusion, including the model of detections' fusion, the valuation of the belief function and performance of fusion. Section 3 provides a detailed performance evaluation of the proposed method. Simulations based on the fusion of two spoofing detections are given. Finally, the conclusions are provided in Section 4.

2. The Proposed Method of Spoofing Detections' Fusion

A detailed discussion of the proposed method is provided in this section. First, a simplified frame of discernment is given. The simplification is for the purpose of the quantization for detection

results. Then, the valuation of the belief function, which is the key of information fusion, is given and discussed. Finally, the performance of detections' fusion is analyzed briefly.

2.1. The Model of Detections' Fusion

Most of the spoofing detections focus on the anomalies of signal features or measurements. Generally, each detector aims at only one feature, and the result is evidence of the presence of the spoofing attack. However, this evidence would be inadequate and not absolute reliable in some cases. The combination of the results from multiple detectors is an approach to deal with this problem. A method based on DST to fuse multiple detectors is proposed in the following.

According to DST, a complete frame of discernment in spoofing detection should contain all possible mutually exclusive declared propositions, such as the noise, authentic signal, counterfeit signal and the mixture of them. They indicate the identity of the signal. However, this complete frame of discernment sets up obstacles for implementation. The main problem is the evaluation of BPA. Thus, it is necessary to simplify this frame for application. In what follows, the noise, authentic and counterfeit signal are denoted as "N", "A" and "C", respectively, and the frame of discernment is denoted as Θ.

In practice, noise is universal because the environment temperature cannot be absolute zero. The acquisition module of the GNSS receiver would determine the absence of satellite signals if there is only noise. Thus, N is redundant in Θ. In what follows, the object is limited to the satellite signal that has been processed by the receiver, regardless of its authenticity. In a broader sense, C does not only represent the spoofing signal, it also means the abnormal change of the satellite signal. Besides, A and C are exclusive for a signal. If authentic and counterfeit signals are mixed together in a processing channel and cannot be separated by the GNSS receiver, they should be marked as "abnormal", and the identified result should be C. Thus, it is unnecessary to reserve a position for the mixture "AC" in Θ. Therefore, Θ could be simplified as follows:

$$\Theta = \{A, C\} \tag{1}$$

That is, there are only two possible results of spoofing detector, "authentic" or "counterfeit"; the more generalized description is "no spoofing" or "spoofing". This simplification of Θ facilitates the valuation of BPA and the belief functions, it also simplifies the combination rule. According to DST, for a possible result of one detector, the BPA is equivalent to the belief function because there are only two elements in Θ. Herein, the belief function is denoted as $m_i(\cdot)$, which corresponds to detector D_i. $m_i(\cdot)$ follows:

$$\begin{cases} m_i(\phi) = 0 \\ m_i(A) + m_i(C) = 1 \end{cases} \tag{2}$$

where ϕ represents an empty set. $m_i(\cdot)$ implies the believable degree of the evidence from detector D_i. For example, D_i tends to determine the signal as "A" if $m_i(A) > m_i(C)$; otherwise, it tends to determine the signal as "C". The conflict degree of different evidence can be defined as follows:

$$\kappa = 1 - \left(\prod_{i=1}^{N} m_i(A) + \prod_{i=1}^{N} m_i(C) \right) \tag{3}$$

The combination result is reliable if all evidence is coincident, while it is unreliable when the conflict degree is high. $\kappa = 1$ means that some evidence is completely opposite, such as $m_1(A) = 1$ and $m_2(A) = 0$.

Due to the inference of the combination rule of DST [13] in the case of binary detection, the combined $m(\cdot)$ are given as follows:

$$\begin{cases} m(A) = \dfrac{\prod_{i=1}^{N} m_i(A)}{\prod_{i=1}^{N} m_i(A) + \prod_{i=1}^{N} m_i(C)} \\ m(C) = \dfrac{\prod_{i=1}^{N} m_i(C)}{\prod_{i=1}^{N} m_i(A) + \prod_{i=1}^{N} m_i(C)} \end{cases} \tag{4}$$

where N is the number of spoofing detectors. In the case that $\kappa = 1$, there is $\prod m_i(A) + \prod m_i(C) = 0$; $m(\cdot)$ cannot be obtained according to Equation (4). It is necessary to add a rule with Equation (4) in such a case as follows:

$$m(A) = m(C) = 0.5 \qquad \text{when} \qquad \kappa = 1$$

In what follows, they are denoted as Equation (4) together. After the fusion, a final decision must be made to determine the authenticity of the signal. The decision rule is given as follows:

$$\begin{cases} \text{Determine } A \text{ when } m(A) \geq m(C) \\ \text{Determine } C \text{ when } m(A) < m(C) \end{cases} \tag{5}$$

As $m(A) + m(C) = 1$, the rule of Equation (5) determines "A" if $m(A) \geq 0.5$ and determines "C" if $m(A) < 0.5$. That is, 0.5 is the threshold of the final decision after detections' fusion.

Figure 1 shows the diagram of the detections' fusion. Detector D_i points at x_i, which could be any feature of the GNSS signals or measurements, such as signal power, Doppler shifts, code delay, pseudoranges, the results of positioning, etc.

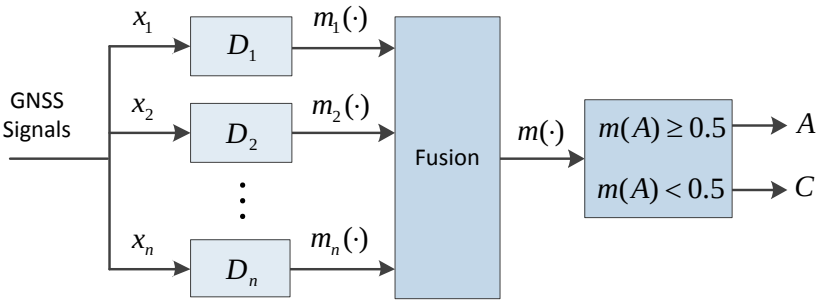

Figure 1. Diagram of the fusion of multiple spoofing detectors.

It should be noted that not the different detection methods, but the different signal features are the key of fusion. The evidence of the spoofing attack is collected from the detectors and fused according to the rule of Equation (4). The fusion makes the result more credible if the evidence from different detections is coincident, while it would give a compromise result according to all evidence if it is conflictive. Two examples are provided in Table 1 as follows to demonstrate the combination of coincident and conflictive evidence.

Table 1. Examples for combination rule.

Coincident Evidence				**Conflictive Evidence**			
	m_1	m_2	$m_1 \oplus m_2$		m_1	m_2	$m_1 \oplus m_2$
A	0.8	0.2	0.903	A	0.8	0.2	0.632
C	0.2	0.3	0.097	C	0.3	0.7	0.368

2.2. Valuation of the Belief Function for GNSS Spoofing Detections

Belief functions are the key to the detections' fusion. They represent the reliability of the corresponding measurement or features of the signal. The belief function is calculated based on the basic probability assignment (BPA) in DST. As previously mentioned, BPA is equivalent to the belief function in the case of binary detections. However, there is no general way to get BPA or the belief function for a detection result. This section proposes a method to valuate the belief function and provides a brief discussion about two spoofing detections.

Most of the spoofing detections are equivalent to hypothesis testings. They can be described as:

$$\begin{cases} H_0: & T(x) \leq \gamma \\ H_1: & T(x) > \gamma \end{cases} \tag{6}$$

where H_0 and H_1 are hypotheses that represent the absence and presence of a spoofing attack, and they are equivalent to A and C of Equation (1), respectively. $T(x)$ is the test statistic of x, which is a measurement of the signal. γ is the threshold of detection. Here, x could be any signal features and measurements, such as the absolute power or carrier-to-noise ratio (C/N_0) of the received signal, Doppler shift, outputs of the correlator, pseudorange measurement, etc.

The detection of Equation (6) makes a hard decision to decide whether the signal is authentic or not. It is easy to implement, but it loses some information and increases the error decision. $T(x)$ is a quantization of the anomaly of x, and it also can be considered as a soft decision of the authenticity of signal. The belief function for the detection results of detector D_i can be defined as:

$$\begin{cases} m_i(A) = f(T_i, \gamma_i) \\ m_i(C) = 1 - f(T_i, \gamma_i) \end{cases} \tag{7}$$

where $m_i(\cdot)$ is the belief function, T_i and γ_i represent the test statistic and threshold of D_i, respectively, and f is the function that maps T_i and γ_i to a real number. The mapping is subject to:

$$\begin{cases} f(T_i, \gamma_i) \in [\,0,\ 1\,] \\ m_i(A) > m_i(C) \ \text{ when } \ T_i < \gamma_i \\ m_i(A) < m_i(C) \ \text{ when } \ T_i > \gamma_i \\ m_i(A) = m_i(C) \ \text{ when } \ T_i = \gamma_i \end{cases} \tag{8}$$

This is in keeping with the decision rule of Equation (6). However, unlike Equation (6), $m_i(\cdot)$ of Equation (7) provides a soft decision of the authenticity of the signal. Compared with the hard decision, it retains more information of x. More than that, Equation (7) makes it possible to fuse the information from multiple detections to reduce the probability of error decisions.

There are many forms of f to meet Equation (8). The p-value of hypothesis testing would have more proper to reflect the reliability of the results than the test statistic and threshold. However, the calculation of the tail probability for each obtained statistics in the method of the p-value is too complicated. Herein, two definitions of f are proposed for simplicity in the application. In what follows, T_i and γ_i are assumed as non-negative, and this is possible in a proper way. One definition of f can be given as:

$$f_1(T_i, \gamma_i) = \left(\frac{1}{2}\right)^{T_i/\gamma_i} \tag{9}$$

$f_1(T_i, \gamma_i)$ is a decreasing function of T_i/γ_i, and it is easy to implement. However, $f_1(T_i, \gamma_i)$ descends slowly even if the anomaly is obvious enough. Besides, $f_1(T_i, \gamma_i)$ is in a half closed interval $[0, 1)$ because the base number of the power function is less than one. Another definition of f is given as:

$$f_2(T_i, \gamma_i) = \begin{cases} 1 - \dfrac{T_i}{2\gamma_i} & T_i < 2\gamma_i \\ 0 & T_i \geq 2\gamma_i \end{cases} \tag{10}$$

$f_2(T_i, \gamma_i)$ meets Equation (8), as well, and it is in a closed interval $[0, 1]$. However, $f_2(T_i, \gamma_i)$ descends quickly, and it makes a decision $m_i(A) = 0$ even if the anomaly is not obvious enough. The decision $m_i(A) = 0$ is strong, and it makes an irrevocable decision while all other detectors are meaningless. Figure 2 shows the curves of $f_1(T_i, \gamma_i)$ and $f_2(T_i, \gamma_i)$, where T_i/γ_i is plotted on the horizontal axis, and the red line is the threshold to determine "A" or "C".

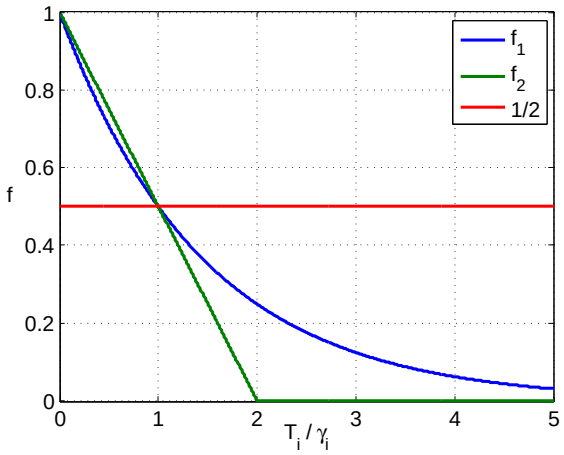

Figure 2. Curves of two $f(T_i, \gamma_i)$.

As mentioned previously, both $f_1(T_i, \gamma_i)$ and $f_2(T_i, \gamma_i)$ have weakness in practice. The linear combination of them would be applicable, and it can be given as follows:

$$f(T_i, \gamma_i) = \alpha \cdot f_1(T_i, \gamma_i) + (1 - \alpha) \cdot f_2(T_i, \gamma_i) \qquad \alpha \in [0, 1] \tag{11}$$

where α is the weight of $f_1(T_i, \gamma_i)$; it can be set according to the actual implementation.

2.3. Performance of Detections' Fusion

A spoofing detection can be fused with others by the method as mentioned previously, as long as it could be depicted by a hypothesis testing as Equation (6). There are two types of errors in hypothesis testings. One is false alarm and the other is missed detection. The former is the incorrect rejection of the true hypothesis H_0, while the latter is the failure to reject the false hypothesis H_1. The probabilities of these two errors can be described as follows:

$$\begin{cases} P_{fa} = P(H_1 | H_0) \\ P_{md} = P(H_0 | H_1) \end{cases} \tag{12}$$

where P_{fa} is the false alarm probability and P_{md} is the missed detection probability. They are contradictory. For a given sample set, P_{md} increases with the reduction of P_{fa}, and vice versa. P_{fa} and P_{md} cannot be reduced simultaneously unless the sample size increases, but this is infeasible especially in practice. Detection aiming at data set for a long time cannot reflect the real-time changes of signals. This limits the performance of single spoofing detection. However, it is different in case that multiple

detections are fused, because the false alarms would not happen simultaneously in different detectors. This means that false alarms of fused detection would be much less than those of each detector.

Herein, a brief derivation of P_{fa} is given in the case that only two detections are fused. The probabilities of $m_i(\cdot)$ under hypotheses H_0 and H_1 are denoted as $P_0^{(i)}$ and $P_1^{(i)}$, respectively. The false alarm probability of detector D_i is denoted as $P_{fa}^{(i)}$, and the corresponding missed detection probability is denoted as $P_{md}^{(i)}$. In the case that only two detections are fused, $m(C) > 0.5$ is equivalent to $m_1(C) + m_2(C) > 1$, and $m(A) \geq 0.5$ is equivalent to $m_1(A) + m_2(A) \geq 1$. The derivation is provided in Appendix A. Based on Equations (4) and (5), P_{fa} of fused detections can be given as follows:

$$\begin{aligned} P_{fa} &= P\left(m(A) < 0.5 \middle| H_0\right) = P\left(m(C) > 0.5 \middle| H_0\right) \\ &= P_0^{(1)}\left(m_1(C) > 0.5\right) \cdot P_0^{(2)}\left(m_2(C) > 1 - m_1(C) \middle| m_1(C) > 0.5\right) \\ &\quad + P_0^{(2)}\left(m_2(C) > 0.5\right) \cdot P_0^{(1)}\left(m_1(C) > 1 - m_2(C) \middle| m_2(C) > 0.5\right) \\ &\quad - P_0^{(1)}\left(m_1(C) > 0.5\right) \cdot P_0^{(2)}\left(m_2(C) > 0.5\right) \\ &< P_{fa}^{(1)} + P_{fa}^{(2)} - P_{fa}^{(1)} \cdot P_{fa}^{(2)} \end{aligned} \tag{13}$$

where 0.5 is the threshold of $m(\cdot)$ to determine the authenticity of the signal. $P_{fa}^{(1)} + P_{fa}^{(2)} - P_{fa}^{(1)} \cdot P_{fa}^{(2)}$ is the false alarm probability of two detectors if their results are not fused together. In such a case, each false alarm would be mistaken for a spoofing attack no matter in which detector it happens. This can be explained as Figure 3.

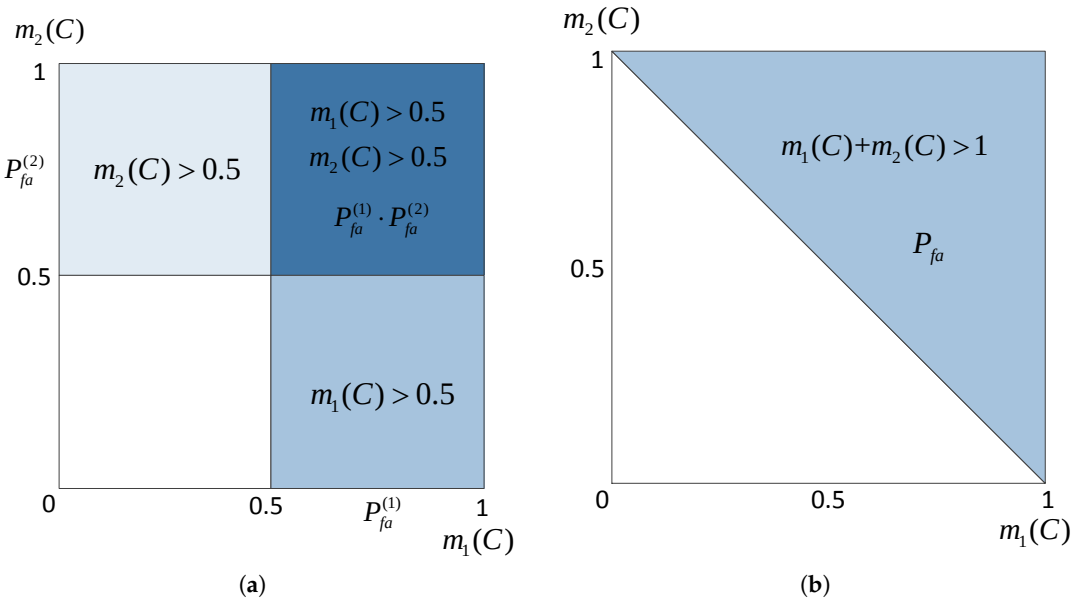

Figure 3. Regions of the false alarm in the case that detections are fused or not fused under hypothesis H_0. (**a**) Two detections are not fused; (**b**) two detections are fused.

The shadow areas in Figure 3a represent the region of false alarms under the hypothesis of H_0 in the case that two detections are not fused, while in Figure 3b, the shaded region is lessened in the case that two detectors are fused together. This is the graphical interpretation of the inequality (13). Meanwhile, the dark shaded area in Figure 3a, denoted as R_1, represents the region in which false

alarms happen simultaneously in both D_1 and D_2. Denoting the shaded area in Figure 3b as R_2, R_1 is a subset of R_2, i.e., $R_1 \subset R_2$. Thus, there is:

$$P_{fa}^{(1)} \cdot P_{fa}^{(2)} < P_{fa} \tag{14}$$

The above inequality can be deduced as follows:

$$\begin{aligned} P_{fa} &= P\left(m_1(C) + m_2(C) > 1 \middle| H_0\right) \\ &= P_0^{(1)}\left(m_1(C) < 0.5\right) \cdot P_0^{(2)}\left(m_2(C) > 1 - m_1(C) \middle| m_1(C) < 0.5\right) \\ &\quad + P_0^{(2)}\left(m_2(C) < 0.5\right) \cdot P_0^{(1)}\left(m_1(C) > 1 - m_2(C) \middle| m_2(C) < 0.5\right) \\ &\quad + P_0^{(1)}\left(m_1(C) > 0.5\right) \cdot P_0^{(2)}\left(m_2(C) > 0.5\right) \\ &\quad > P_{fa}^{(1)} \cdot P_{fa}^{(2)} \end{aligned} \tag{15}$$

Based on Equations (13) and (14), the range of P_{fa} can be given as:

$$P_{fa}^{(1)} \cdot P_{fa}^{(2)} < P_{fa} < P_{fa}^{(1)} + P_{fa}^{(2)} - P_{fa}^{(1)} \cdot P_{fa}^{(2)} \tag{16}$$

Meanwhile, P_{md} of fused detections can be given as follows:

$$\begin{aligned} P_{md} &= P\left(m(A) \geq 0.5 \middle| H_1\right) \\ &= P_1^{(1)}\left(m_1(A) \geq 0.5\right) \cdot P_1^{(2)}\left(m_2(A) \geq 1 - m_1(A) \middle| m_1(A) \geq 0.5\right) \\ &\quad + P_1^{(2)}\left(m_2(A) \geq 0.5\right) \cdot P_1^{(1)}\left(m_1(A) \geq 1 - m_2(A) \middle| m_2(A) \geq 0.5\right) \\ &\quad - P_1^{(1)}\left(m_1(A) \geq 0.5\right) \cdot P_1^{(2)}\left(m_2(A) \geq 0.5\right) \\ &< P_{md}^{(1)} + P_{md}^{(2)} - P_{md}^{(1)} \cdot P_{md}^{(2)} \end{aligned} \tag{17}$$

where $P_{md}^{(1)} + P_{md}^{(2)} - P_{md}^{(1)} \cdot P_{md}^{(2)}$ is the missed detection probability of two detectors if their results are not fused together. Each missed detection cannot be re-examined in the case that two detectors are not fused. Similar to Equation (14), there is:

$$P_{md} > P_{md}^{(1)} \cdot P_{md}^{(2)} \tag{18}$$

Based on Equations (17) and (18), the range of P_{md} can be given as:

$$P_{md}^{(1)} \cdot P_{md}^{(2)} < P_{md} < P_{md}^{(1)} + P_{md}^{(2)} - P_{md}^{(1)} \cdot P_{md}^{(2)} \tag{19}$$

The range of P_{fa} and P_{md}, Equations (16) and (19), just provides rough boundaries of P_{fa} and P_{md}. They clearly show that both P_{fa} and P_{md} in the case of fusion are less than the corresponding values in the case that detections are not fused. The actual ranges depend on the performance of the detectors, which are fused. Monte Carlo simulations based on two detectors are given in the following section to demonstrate the performance of fusion.

The above discussions are based on the fusion of two detectors. Actually, the combination rule of Equation (4) is associative, that is:

$$m_1 \oplus m_2 \oplus m_3 = m_1 \oplus (m_2 \oplus m_3) = m_1 \oplus m_2' \tag{20}$$

where $\oplus$ represents the operation of the combination and m_2' represents the combination of m_2 and m_3. The derivation of the associative law is provided in Appendix B. Equation (20) means that the combination of multiple detections can be equivalent to the combination of two detections after some of them are fused together. Thus, discussions about two detections are sufficient to extend to the cases of multiple detections.

3. Performance Evaluation

A model of detections' fusion has been given, and the valuation of the belief function has been proposed in the above section. In order to evaluate the performance of the method, simulations based on the fusion of two spoofing detections are provided in this section.

3.1. Two Detectors

Herein, two detectors, monitoring the correlator outputs and consistency of Doppler, are given. They aim at different features of GNSS signal and provide different evidence of the authenticity of the signal.

3.1.1. Monitoring of Correlator Outputs

Monitoring of the received signal power is a usual method of spoofing detection, and it can be implemented in several ways, such as the monitoring of absolute power, C/N_0 and the correlator outputs [8]. The anomaly of correlator outputs reflects the abnormal change of the power of received GNSS signals. Some methods have been proposed to monitor the correlator outputs, such as testing the goodness of fit based on the χ^2 distribution [10,15], Herein, another practical way of correlator output monitoring is proposed.

In the case of the spoofing attack, it is difficult for the spoofer to calibrate the power of the spoofing signal to maintain a stable level at the target receiver because of the uncertainty of the relative motion between spoofer and receiver. Besides, correlator outputs may be abnormal because the tracking loop is disturbed by spoofing. Monitoring the stationarity of correlation values is a practical way to detect the anomaly of the signal. Denote the correlator outputs in time k as $r[k]$. There are jumps in correlator outputs because of the change of navigation data. Denote $x[k]$ as:

$$x[k] = D[k] \cdot r[k] \tag{21}$$

where $D[k]$ represent the navigation data and its value is one or -1. Then, $x[k]$ can be approximated as a Gaussian random variable because it is determined by several factors, such as signal power, tracking errors, noise, etc. Assuming that the signal is locked and the parameters of the receiver do not change, the mean value of $x[k]$ reflects the power of the signal while the variance of $x[k]$ represents other effects, such as noise and errors. The outputs of the correlator are steady in the case of authentic signals and unsteady in the case of the spoofing attack. Denote two sample sets of correlator outputs in different times as $X = \{x[1], x[2], \cdots, x[K]\}$ and $Y = \{y[1], y[2], \cdots, y[K]\}$; they conform to a Gaussian distribution as:

$$\begin{cases} X \sim N(\mu_x, \sigma_x^2) \\ Y \sim N(\mu_y, \sigma_y^2) \end{cases} \tag{22}$$

As mentioned previously, the mean value reflects the power of the signal, while the variance represents the effects of random factors. Therefore, the spoofing detection based on the monitoring of correlator outputs can be equivalent to the following hypothesis testing:

$$\begin{cases} H_0: & \mu_x = \mu_y \\ H_1: & \mu_x \neq \mu_y \end{cases} \tag{23}$$

Assuming $\sigma_x^2 = \sigma_y^2 = \sigma^2$ and because σ^2 is unknown, define the test statistic as follows:

$$T = \sqrt{K} \cdot \frac{\bar{x} - \bar{y}}{\sqrt{\hat{\sigma}_x^2 + \hat{\sigma}_y^2}} \tag{24}$$

where $\bar{x}$ and $\bar{y}$ are the mean value of X and Y with a data length of K and $\hat{\sigma}_x^2$ and $\hat{\sigma}_y^2$ are estimations of X and Y, respectively. $(\hat{\sigma}_x^2 + \hat{\sigma}_y^2)/2$ is an unbiased estimation of the variance of sample group $\{X, Y\}$; $\bar{x}$ and $\hat{\sigma}_x^2$ are given as:

$$\begin{cases} \bar{x} = \dfrac{1}{K} \displaystyle\sum_{k=0}^{K-1} x[k] \\ \hat{\sigma}_x^2 = \dfrac{1}{K} \displaystyle\sum_{k=0}^{K-1} \Big(x[k] - \bar{x} \Big)^2 \end{cases} \tag{25}$$

$\bar{y}$ and $\hat{\sigma}_y^2$ can be obtained in the same way. The test statistic as Equation (24) has been used for GPS interference detection [16]. Under hypothesis H_0, the test statistic conforms to Student's t distribution with $2K - 2$ degrees of freedom [17] as follows:

$$T \sim t(2K - 2) \tag{26}$$

Thus, Equation (23) is equivalent to:

$$\begin{cases} H_0: & \Big| T \Big| \leq \gamma \\ H_1: & \Big| T \Big| > \gamma \end{cases} \tag{27}$$

where γ is the threshold of detection, and it can be given as follows:

$$\gamma = Q_{t(2K-2)}^{-1}(1 - P_{fa}/2) \tag{28}$$

where $Q_{t(2K-2)}^{-1}(\cdot)$ represents the inverse function of the cumulative density function (CDF) of Student's t distribution.

3.1.2. Consistency Check of Doppler

Doppler shift is generated by the relative motion of the satellite and receiver. The carrier Doppler shift of the GNSS signal must be consistent with its code Doppler shift. However, this is not satisfied in some cases of the spoofing attack. Thus, the consistency check of Doppler can be used for spoofing detection. A brief introduction of this method is given herein.

As a consequence of the formula of Doppler shift, the pseudo-code Doppler of the GNSS signal is proportional to the carrier Doppler; the proportionality coefficient is given as follows:

$$\alpha = \frac{f_{D\_code}}{f_{D\_carrier}} = \frac{f_{code}}{f_{carrier}} \tag{29}$$

where f_{D_code} is the Doppler shift of pseudo-code and $f_{D\_carrier}$ is the Doppler shift of the carrier and f_{D_code}. f_{code} is the code rate of the pseudo-code, and $f_{carrier}$ is the carrier frequency. For example, the coefficient of the GPS L1 C/A signal is:

$$\alpha = \frac{f_{D\_code}}{f_{D\_carrier}} = \frac{1.023 \times 10^6}{1575.42 \times 10^6} = \frac{1}{1540} \tag{30}$$

Not just the Doppler of the pseudo-code and carrier, but a similar relationship exists between signals of different frequencies from one satellite, so the consistency check can apply to them. Based on Equation (29), define:

$$x = f_{D\_code} - \alpha f_{D\_carrier} \tag{31}$$

The equivalent hypothesis testing of the consistency check of Doppler can be written as follows:

$$\begin{cases} H_0: & x[k] = w[k] \\ H_1: & x[k] = A + w[k] \end{cases} \tag{32}$$

A is a non-zero bias between carrier Doppler and code Doppler, and $w[k]$ represents the noise and error of measurements. Assuming that $w[k]$ conforms to a zero mean Gaussian distribution, $x[k]$ can be described as:

$$x \sim N(\mu, \sigma^2) \tag{33}$$

where μ and σ^2 represent the mean value and variance. Hypothesis testing of Equation (32) is equivalent to:

$$\begin{cases} H_0: & \mu = 0 \\ H_1: & \mu \neq 0 \end{cases} \tag{34}$$

As σ^2 is unknown, define the test statistic as follows:

$$T = \frac{\sqrt{K} \cdot \bar{x}}{\hat{\sigma}} \tag{35}$$

where $\bar{x}$ is the mean value of the observed data of $x[k]$ with data length K, and $\hat{\sigma}$ represents the maximum likelihood estimation (MLE) of σ; they can be obtained as Equation (25). The test statistic conforms to Student's t distribution with $K-1$ degrees of freedom [17] under hypothesis H_0 as follows:

$$T \sim t(K-1) \tag{36}$$

Therefore, the detection as Equation (27) can be used for the consistency check of Doppler, as well as the threshold is obtained by a similar way as Equation (28).

3.2. Simulation Results

There are two parts of the simulations in this section. The first is the Monte Carlo simulation of the performance of fusion, and the second aims at public test datasets. Monitoring of correlator outputs and the consistency check of Doppler shifts, which have been discussed previously, are employed and fused together in what follows. Their test statistics are denoted as T_1 and T_2, which correspond to Equations (24) and (35). The corresponding belief functions are denoted as $m_1(\cdot)$ and $m_2(\cdot)$, respectively. Both detectors adopt the same false alarm probability denoted as $P_{fa}^{(i)}$.

3.2.1. Probabilities of False Alarm and Detection

The performance of a detector can be depicted by the receiver operating characteristics (ROC) curve, which illustrates the relationship of false alarm probability P_{fa} and detection probability P_d. Here, detection probability P_d can be obtained as:

$$P_d = P(H_1|H_1) = 1 - P(H_0|H_1) = 1 - P_{md} \tag{37}$$

In the following Monte Carlo simulations, a dataset that conforms to a standard normal distribution is employed. The false alarm probability of fused detection is counted based on the detection results. Then, a bias, denoted as A, is added to the dataset to simulate the anomaly of measurements. For the first detector, A is added to the difference of mean value $\bar{x} - \bar{y}$. The results of two detectors and fused detection are counted. The results are shown in Figures 4 and 5.

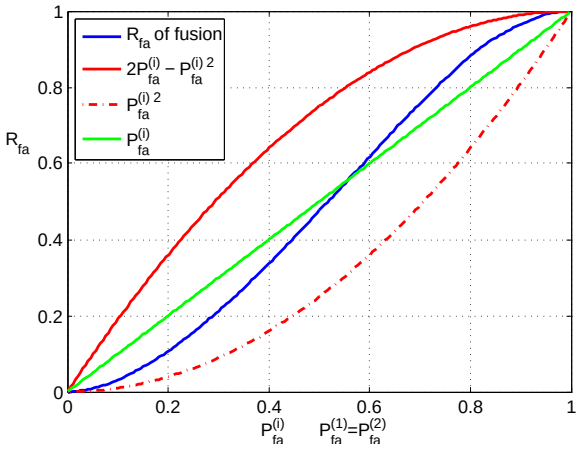

Figure 4. False alarm probability of fusion.

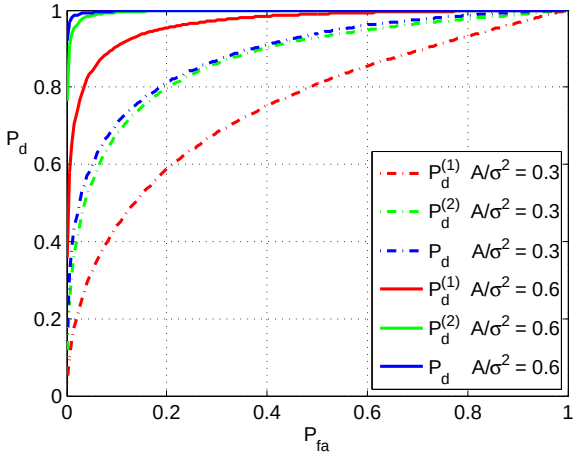

Figure 5. ROC curves of detections.

Figure 4 shows the simulation results of false alarms. The horizontal axis represents $P_{fa}^{(i)}$, while the vertical axis shows the rate of false alarms that happened in simulations. Here, the rate of false alarm is denoted as R_{fa}; it is tallied in Monte Carlo simulations. Two red curves in Figure 4 give the rough bounds of P_{fa}, which has been described in Equation (16). The blue curve is the R_{fa} of fusion. It can be observed that fused R_{fa} is between two boundaries. Moreover, in a practical range, R_{fa} is less than $P_{fa}^{(i)}$, which is plotted in the green curve, and this means that false alarms are reduced by fusion.

ROC curves are plotted in Figure 5. In the simulations, two different normalized biases A are tested, and the corresponding results are plotted in dashed lines and solid lines. In both cases, blue curves are higher than the corresponding red and green curves. This means that the detection performance is improved by the fusion. It should be noted that the ROC curves of fusion take account of the reduction of false alarms, which is shown in Figure 4. Simulation results with other A/σ^2 are similar to them.

Actually, the improvement of detection performance is reasonable, because the data size of multiple detections' fusion is much larger than the data size of single detection, while the fusion does not extend the time of detection.

3.2.2. Test Results on TEXBAT

Simulations of multiple detections' fusion based on the proposed method are provided next. The test data are from TEXBAT, which is a public dataset of eight high-fidelity digital recordings of live static and dynamic GPS L1 C/A spoofing tests. It is conducted by the Radio Navigation Laboratory of the University of Texas at Austin, and each scenario in TEXBAT has been described in detail in [18]. In Scenario 1 of TXBAT, the counterfeit signals substitute all authentic GNSS signals instantaneously; the power of counterfeit signals is much weaker than the authentic. In Scenario 2, the spoofer increases the power of the counterfeit signal, and it has a 10-dB power advantage; this is an obvious power attack. Moreover, the spoofer changes the counterfeit signals' carrier phase proportionally when it shifts the code phase to induce a position or timing deviation in the target receiver. The power advantage of counterfeit signals is common in the next scenarios, but it is reduced. In Scenario 3, the spoofer fixes the carrier phase offset between the counterfeit signals and the authentic signals when it shifts the code phase of counterfeit signals. Scenario 4 is identical to Scenario 3, except that the power advantage of the counterfeit signal is reduced again. Static Scenarios 1∼4 are tested, and the results are discussed in this section. In each scenario, the detection results of just one satellite, GPS PRN 6, is discussed because the results of most satellites in the same scenario are similar.

In the following tests, a software-defined GPS receiver is employed. Common acquisition and tracking algorithms of GPS signals are implemented in the receiver where a phase-locked loop (PLL) is used for carrier tracking and a common delay lock loop (DLL) is used for code tracking. The coherent integration time is 1 ms in the receiver, and a measurement is obtained per one millisecond. The detection time is 50 milliseconds as the sample size is K = 50. The time interval of two sample sets, X and Y, is 1 s. This time interval can be set according to the application scenario. Herein, the short interval is conducive to improve the real-time capability of detectors. Besides, false alarm probabilities or significance levels are set as $P_{fa} = 0.005$ in both detections.

Figure 6 shows the test results of the clean static dataset where the GPS signals are not disturbed by counterfeit signals. It can be observed that there is a small number of false alarms in both two detections, and they disappear in the fused results. Reduction of false alarms is coincident with the curve in Figure 4, and it suggests that higher $P_{fa}^{(i)}$ can be adopted to obtain a lower $P_{md}^{(i)}$ in each detector before the fusion.

Test results of Scenario 1 for GPS PRN 6 are shown in Figure 7. The sudden replacement of the signals and the power difference disturbed the correlator and tracking loop. It can be observed that an obvious change of correlator outputs occurs at about 125 s in the time history, and an anomaly between carrier Doppler and code Doppler is detected at the same time, although the signal is tracked and locked by the receiver in the whole process.

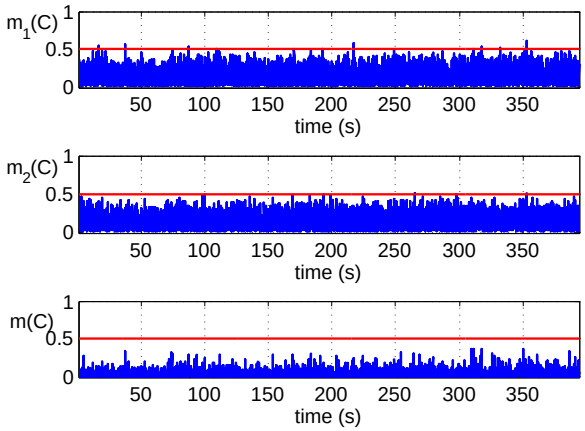

Figure 6. Detections' fusion of the clean static dataset.

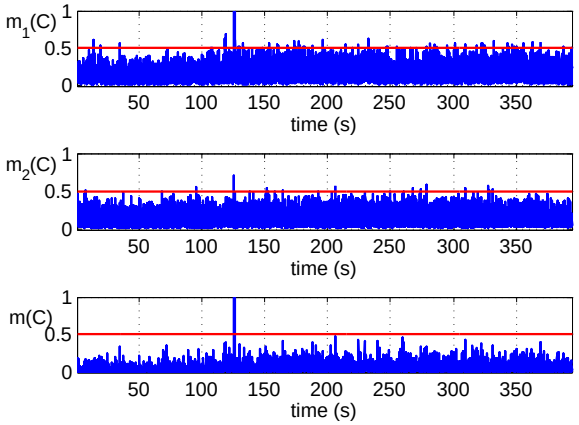

Figure 7. Detections' fusion of the Scenario 1 dataset.

Figure 8 shows the fused results of two detections of Scenario 2. They are similar to the results of Scenario 1; the appearance of counterfeit signals with the power advantage makes two detectors issue alarms simultaneously at about 110 seconds. Moreover, with the shift of the carrier phase and code phase, the consistency of carrier Doppler and code Doppler is not met. Meanwhile, correlator outputs are not stationary because the tracking loop is disturbed. These are reflected in the figure.

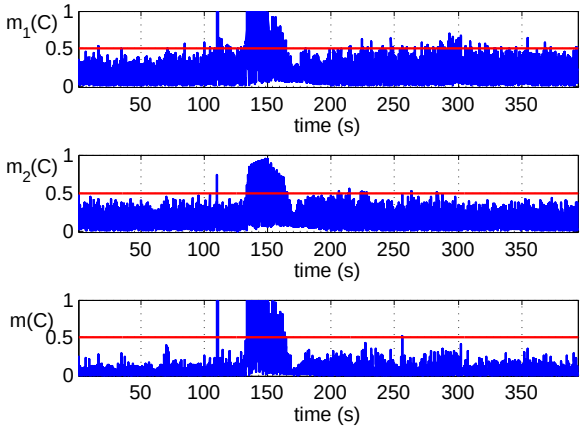

Figure 8. Detections fusion of the Scenario 2 dataset.

The fused results based on Scenarios 3 and 4 are shown in Figures 9 and 10, respectively. In Scenario 3, the spoofer's power advantage is weaker than the case of Scenario 2, but it still can be detected by the monitoring of correlator outputs. Besides, it can be observed in Figure 10 that the fused result exceeds the threshold at about 160 seconds, even though the second detector does not raise the alarm. This shows the robustness of the fusion method.

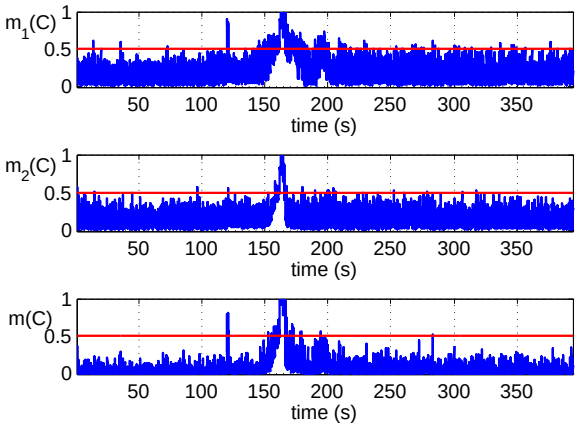

Figure 9. Detections' fusion of the Scenario 3 dataset.

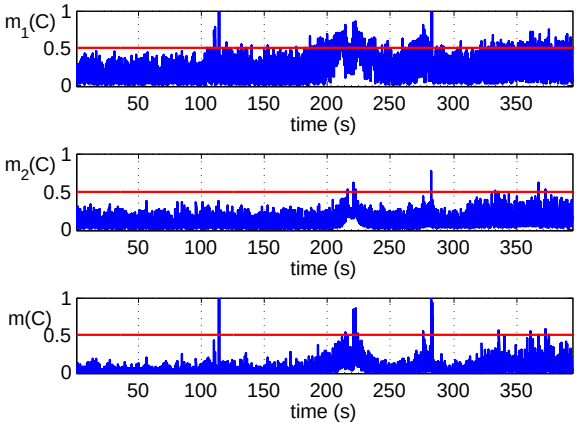

Figure 10. Detections' fusion of the Scenario 4 dataset.

It can be observed from the above results that decisions after the fusion are more distinguishable than before the fusion. It should be noted that stable tracking conditions are crucial to obtain the test statistics; however, the stability of tracking cannot be guaranteed under the spoofing attack. Actually, in the above tests, tracking conditions are stable for most of the time, except sometimes in the tests of Scenarios 3 and 4. In test of Scenario 3, the receiver failed to track and lock the signal for about fifteen seconds at about 160 s in the time history. In this period, the receiver attempted to track and lock the signal; the test statistics based on the outputs of tracking loop cannot reflect the real conditions. However, failure to lock the signal indicates the anomalies of the signal. It is reasonable that detectors issue alarms to declare the unavailability of the signal in this case.

The above simulations illustrate the process and effect of the detections' fusion. It can be observed on them that the fusion of multiple detections reduces the false alarms and makes the results more reliable. Only two detectors are fused in this section. However, a complete anti-spoofing method should employ more detectors and fuse them together.

4. Conclusions

As long as a spoofing detection could be depicted as a hypothesis testing, it can be fused with others by the method that is proposed in this paper. A key point of the fusion method is to simplify the discernment frame in order to assign the belief functions for spoofing detection results. Most of the spoofing detections are equivalent to hypothesis testings. The deviation degree of the test statistic and threshold represents the reliability of the measurement, and it is the basis of the belief function of the spoofing detection result. The performance evaluation and simulations based on two detections are provided in the paper. The proposed method improves the performance of spoofing detection and makes the results more reliable. The root cause of improvement is the increase of the detection data. However, there are some questions to be solved; for example, the evidence from different detections should be independent, but this may not be true in spoofing detections because some measurements are related in the GNSS receiver, such as C/N_0 and correlation values, while some measurements are independent, such as C/N_0 and Doppler shift. Besides, the selection of detectors to be fused in a specific scenario and the assignment of weightings for them are problems to be studied.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (Grant No. 61571255).

Author Contributions: Huiqi Tao and Hong Li discussed this problem and got the ideas to fuse multiple detections together. Huiqi Tao wrote the paper and completed the performance analysis. Hong Li and Mingquan Lu coordinated the study and reviewed the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

In the case that only two detections are fused, $m(C) > 0.5$ is equivalent to $m_1(C) + m_2(C) > 1$, and $m(A) \geq 0.5$ is equivalent to $m_1(A) + m_2(A) \geq 1$. The derivation is given as follows:

$$\begin{aligned} m(C) = \frac{m_1(C)m_2(C)}{m_1(A)m_2(A) + m_1(C)m_2(C)} &> 0.5 \\ \Updownarrow & \\ m_1(C)m_2(C) &> m_1(A)m_2(A) \\ \Updownarrow & \\ m_1(C)m_2(C) &> \Big(1 - m_1(C)\Big)\Big(1 - m_2(C)\Big) \\ \Updownarrow & \\ m_1(C) + m_2(C) &> 1 \end{aligned} \tag{A1}$$

where "$\Updownarrow$" means "be equivalent to". Similarly, there is:

$$m(A) = \frac{m_1(A)m_2(A)}{m_1(A)m_2(A) + m_1(C)m_2(C)} \geq 0.5 \quad \Longleftrightarrow \quad m_1(A) + m_2(A) \geq 1 \tag{A2}$$

Appendix B

The combination rule of Equation (4) is associative. The derivation is given as follows:

$$
\begin{aligned}
& m_1(A) \oplus \Big(m_2(A) \oplus m_3(A) \Big) \\
&= \frac{m_1(A) \dfrac{m_2(A)m_3(A)}{m_2(A)m_3(A) + m_2(C)m_3(C)}}{m_1(A) \dfrac{m_2(A)m_3(A)}{m_2(A)m_3(A) + m_2(C)m_3(C)} \; + \; m_1(C) \dfrac{m_2(C)m_3(C)}{m_2(A)m_3(A) + m_2(C)m_3(C)}} \\
&= \frac{m_1(A)m_2(A)m_3(A)}{m_1(A)m_2(A)m_3(A) + m_1(C)m_2(C)m_3(C)} \\
&= \; m_1(A) \oplus m_2(A) \oplus m_3(A)
\end{aligned}
\tag{B1}
$$

Similarly, there is:

$$
m_1(C) \oplus \Big(m_2(C) \oplus m_3(C) \Big) = m_1(C) \oplus m_2(C) \oplus m_3(C) \tag{B2}
$$

References

1. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270.
2. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *Int. J. Navig. Obs.* **2012**, *2012*, 127072.
3. 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. In Proceedings of the 2009 International Technical Meeting of the Institute of Navigation, Anaheim, CA, USA, 26–28 January 2009.
4. Ledvina, B.M.; Bencze, W.J.; Galusha, B.; Miller, I. An in-line anti-spoofing device for legacy civil GPS receivers. In Proceedings of the 2010 International Technical Meeting of the Institute of Navigation, San Diego, CA, USA, 25–27 January 2010.
5. Khanafseh, S.; Roshan, N.; Langel, S.; Chan, F.-C.; Joerger, M.; Pervan, B. GPS spoofing detection using RAIM with INS coupling. In Proceedings of the Position, Location and Navigation Symposium—PLANS 2014, 2014 IEEE/ION, Monterey, CA, USA, 5–8 May 2014; pp. 1232–1239.
6. Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandon, A.; Lachapelle, G. A low-complexity GPS anti-spoofing method using a multi-antenna array. In Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012; pp. 1233–1243.
7. Magiera, J.; Katulski, R. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *J. Appl. Res. Technol.* **2015**, *13*, 45–57.
8. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191.
9. Pini, M.; Fantino, M.; Cavaleri, A.; Ugazio, S.; Lo Presti, L. Signal Quality Monitoring Applied to Spoofing Detection. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 20–23 September 2011; pp. 1888–1896.
10. Jafarnia-Jahromi, A.; Lin, T.; Broumandan, A.; Nielsen, J.; Lachapelle, G. Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver. In Proceedings of the International Technical Meeting of the Institute of Navigation, Newport Beach, CA, USA, 30 January–1 February 2012; pp. 790–800.
11. Han, S.; Luo, D.; Meng, W.; Li, C. Antispoofing RAIM for dual-recursion particle filter of GNSS calculation. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 836–851.
12. Li, W.; Huang, Z.; Lang, R.; Qin, H.; Zhou, K.; Cao, Y. A Real-Time Interference Monitoring Technique for GNSS Based on a Twin Support Vector Machine Method. *Sensors* **2016**, *16*, 329.

13. Yager, R.R.; Liu, L. *Classic Works of the Dempster–Shafer Theory of Belief Functions*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 1–34.
14. Yuan, D.; Li, H.; Lu, M. A Framework of Mathematic Model and Performance Evaluation for Conjunct GNSS Spoofing Detection. In *China Satellite Navigation Conference (CSNC) 2015 Proceedings: Volume I*; Springer: Berlin/Heidelberg, Germany, 2015.
15. Gamba, M.T.; Truong, M.D.; Motella, B.; Falletti, E.; Ta, T.H. Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets. In *GPS Solutions*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–13.
16. Balaei, A.T.; Dempster, A.G. A Statistical Inference Technique for GPS Interference Detection. *IEEE Trans. Aerosp. Electron. Syst.* **2009**, *45*, 1499–1511.
17. Kay, S.M. *Fundamentals of Statistical Signal Processing: Detection Theory*; Prentice Hall: Upper Saddle River, NJ, USA, 1998.
18. Humphreys, T.E.; Bhatti, J.A.; Shepard, D.P.; Wesson, K.D. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques. In Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012; pp. 3569–3583.