Iranian Journal of
Marine Technology
Marine Science University of Imam Khomeini

High-Sensitivity GPS Spoof Data Classification based on Fuzzy Logic

A. Sadr[1], M. R. Mosavi[2], M. Moazedi[3]

m_mosavi@iust.ac.ir

1,2- The authors are with the Department of Electrical Engineering, Iran University of Science and Technology
3- Department of Engineering Sciences, Faculty of Advanced Technologies, University of Mohaghegh Ardabili, Namin, Iran

Abstract: The Global Positioning System (GPS) receiver is vulnerable to variety of interferences, inclusive of intentional and unintentional ones. This accordingly decreases the navigation accuracy of receiver, and thus causes the receiver cannot work correctly in presence of interference. Consequently, a research effort has begun to study detection and mitigation of GPS spoofing approaches as a serious interference. For the question of GPS spoofing detection, the guidelines are usually raw-based and hard to mathematically model. This make the use of a fuzzy design for the GPS data ideal. A fuzzy logic system is introduced in this paper to analyze and examine the vulnerability of civil GPS receivers towards different kinds of spoofing attacks. This system improves decision-making capability of the receiver from inexact data. The proposed method utilizes the fuzzy set and then the theory of statistical test to recognize fake signals. The studied parameters as input variables are selected from tracking and navigation stage of the GPS receiver.

Key words: GPS, Spoofing, Detection, Fuzzy Logic.

Received Date : 1398-08-27
Accepted Date : 1399-03-19

pp. 105-116

1. Introduction

Spoofing is one of most important attacks in Global Positioning System (GPS) that disturb or decrease the efficiency of navigation process. Spoofing occurs when the counterfeit GPS signals spreading through the receivers as genuine signals, allowing terrorists and hackers to control GPS navigation devices [1]. Time and position coordinates achieved by a GPS receiver in presence of such counterfeit signals is wrong, while the receiver does not detect the fault. The subject of spoofing in navigation is currently open to hackers tried to exploit it.

Spoofing interferences are categorize into three groups: intermediate, simplistic and sophisticated [2]. The second group join an antenna and a power amplifier to a GPS signal simulator. Intermediate spoofing called receiver-spoofer, combines a RF front-end transmitter with the GPS receiver. Finally, the third group comprise various receiver-spoofers that everyone is adopted to the one target antenna utilizing a common communication link and a reference oscillator. Simplistic spoofing assembles valid GPS signals, which are not synchrone with the broadcasted authentic GPS signals. Moreover, physical constraints to put the hacker antenna toward the target GPS receiver cause implementation of sophisticated attack more complicated and sometimes not possible on account of target receiver's mobility. Nevertheless, intermediate spoofer can be such small to place unclearly close the target receiver. Based on these reasons, we selected the intermediate spoofing to study where the source GPS signal is delayed distinctly and then re-sent to the victim receiver.

In recent years, various methods have been proposed to countermeasure spoofing [3-10]. An important and powerful approach in this field is Signal Quality Monitor (SQM), which consistently investigates the GPS signal for deformation to raise a warning flag. Indeed, a SQM algorithm performs some computations at the output of correlators and make a decision by comparing computation results with previously defined thresholds [3]. This method is not useful when the spoofing attack has no effect on the shape of the correlation output when the authentic and counterfeit signals are mostly aligned. Furthermore, this technique cannot determine the multi-path or receiver noise from the spoofing signals. To increase efficiency of the SQM approach, some techniques have been proposed. For example, Vector Based (VB), Vestigial Signal Defense (VSD) and combined techniques are SQM based ones.

VSD method generates more correlators to improve the accuracy of prediction on the degradation rate of the complex correlation function [4], which will be a time continuous signal when a set of delays for correlator are available. The VB tracking approach combines the tracking signal and the navigation solution. It is an analytical technique to study the interaction between counterfeit and authentic correlation peaks throughout the time of attacks. When this distribution deviates from the standard shape spoofing attack is detected. The combined technique "sandwiches" a hacker between monitoring of a total in-band power and a correlation function distortion [5]. Moreover, Ref.s [6-10] have presented anti-spoofing approaches that continuity compare the external and internal data and then estimate the valid signal.

This paper have presented a novel approach using fuzzy logic, to detect spoofing interference by examining the features of received signal. Fuzzy logic provides an uncomplicated manner to extract precise results out of non-specific information [11]. Compared to any other setups the fuzzy sets are more reliable to improve the system performance. In this research, we present a fuzzy logic system to investigate the vulnerability of a civil GPS receiver against spoofing interference based on the parameters that most important researchers have recognized.

This paper is organized as follows. After the short introduction of fuzzy logic theory in section 2, section 3 presents the development of a new spoof detection strategy. Section 4 proceeds with simulation results. After explaining the data collection process, there is an examination of the proposed method. Moreover, this section expresses a qualitative comparison between earlier and proposed methods. In the end, some important outcomes are expressed in section 5.

2. Fuzzy Logic Theory

Fuzzy logic theory introduced in 1965 [12] is an approach of control system that affects software, hardware or both. Moreover, a kind of multi-valued science analyze approximation rather than precise values. Fig.1 demonstrates architecture of a standard fuzzy logic. Fuzzification is the operation of transforming real variables (crisp values) into linguistic variables. Indeed, it maps quantified input values to functions of fuzzy membership, which explains mapping positions of the input space onto membership values within 0 and 1. A base of fuzzy rule collects data in the If-Then format. It explains the correlation of output and fuzzy input parameters. In other words, it prepares the system based on logical conception. Some of important types of membership functions are piecewise, triangular, Gaussian, bell-shaped, trapezoid, and etc. [13].

Fuzzy inference step is obtaining a decision from the rule base, which determines the controller's primary operation. It is an artificial intelligence tool based upon If-Then rules of mapping the input space to the output space. Inference basic structure includes three basic components; a rule base that selects the fuzzy rules, a database that determines membership functions and a reasoning procedure that performs inference process upon agreed facts and finally the rules to achieve a proper output. In other sides, the fuzzy inference contains two main components.

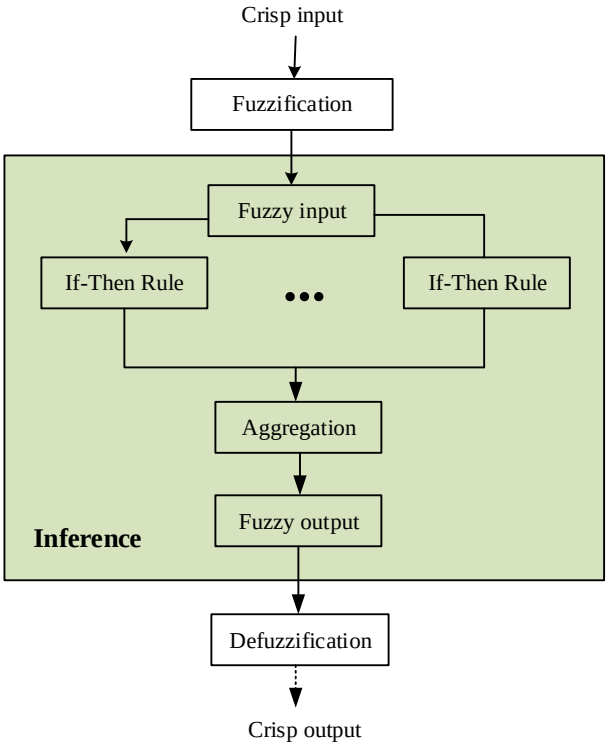


Fig.1 General fuzzy logic structure.

The first is aggregation as the If-part of every rule, appraisal of the degree of condition truth. The second is composition as the Then-part, weighting or evaluating of the outcome. If a single scalar value is the output of a fuzzy process, it will be required to transfer the results into a real value by the defuzzification process depicting the crisp margin of the control parameter [14].

A fuzzy set is extracted of a fuzzy process defined as the output variable after utilizing If-Then rules and the approximation logic. This set not involve a crisp margin but includes a systematic conversion by membership functions. Imprecision is due to lack of principle of category membership defined sharply rather than random parameters. The fuzzy set yields a normal way to deal with these issues. A fuzzy set *S* is usually indicated as elements *x* of measurements *U*, continuous and discrete respectively [15]:

$$S = \{(x, \mu_s(x))\} = \sum_{x_i \in U} \mu_s(x_i)/x_i, \mathrm{x} \in \mathrm{U} \qquad (1)$$

Where the symbol "/" indicates "related to x_i, and the x_i is the i*th* finite element of a discrete collection (*U*). A membership degree μ_s *(x)* to a member in the fuzzy set. The membership function maps the *U*(*x)* members to a membership level within 0 and 1. A linguistic term usually demonstrates realizing the fuzziness of the fuzzy set. Fuzzy logic is also implementable in dynamic environments, using real-time approaches by the fast commercial off-the-shelf GPS boards and microcontrollers [16]. Particularly, fuzzy control techniques are proper for handling systems with some problems for classical control.

3. Proposed Fuzzy based Classification Method

Fuzzy logic subsumes a rule-based, straightforward procedure to find the solution to a control problem, instead of trying to model the system in mathematical way [17]. In this paper, for a first time the fuzzy inference system is employed for performing the reasoning procedure of fuzzy approach for classification of GPS data.

Fuzzy logic variables contains a truth-value in ranges within 0 and 1. In order to function, it requires numerical parameters. The values dedicated to each membership function is based on the expert knowledge of the issue. In our application, an overlap of vectors belongs to the input feature exists between different classes. Moreover, the features are used to demonstrate the spoofing error. Therefore, the input data include inherently imprecise and uncertain elements, which limits the applicability of classification approach of the hard or crisp data [18]. On occasion, we may have informal information about a problem domain where we try to design a classifier. The utilized algorithm in fuzzy classification is to generate so-called "fuzzy category memberships functions," which transform an objectively measurable parameter into a subjective "category memberships". Unquestionably, the term "categories" used by fuzzy practitioners relates not to the final class, but instead just overlapping ranges of feature values. After that, we need a way to convert an objective measurement in several features into a category decision. To take the "category memberships" and obtain a number to be utilized for making the final decision, we require a merging or conjunction rule [19].

The suggested fuzzy logic system of Fig. 2 contains two blocks: block 1 is available to obtain a set of signal values from acquisition and tracking. These values are investigated and explored based on the block fuzzy rules. In block 2, the fuzzy system is likely implemented for navigation stage. Each navigation solution that calculates the location of the receiver outer side of environment space is recognized as outlier and is eliminated from the positioning solution. It is worth to note that these blocks are paralleled conducted in order to increase detection speed and decrease implementation time.

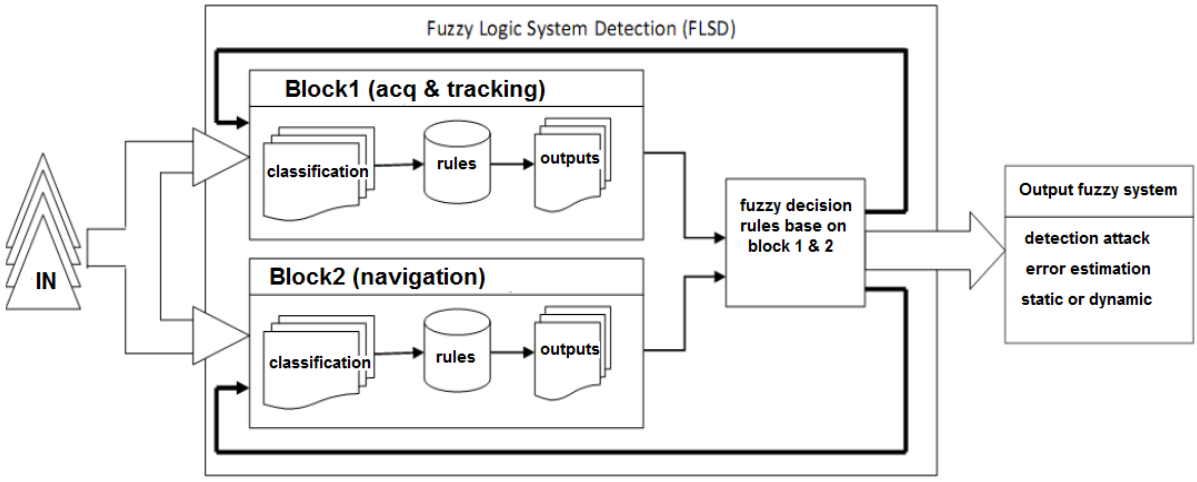


Fig. 2 Proposed fuzzy based classification of GPS signal.

In this approach, by collecting the values of parameters, various levels of signals are evaluated. The different membership functions specified have been arranged for the fuzzy logic system with one output factor and four input factors. The membership functions and rules together determine the result of a system. The rules take the combined effect of the input variables on each of the output variables. These rules are the essence of the method, as they capture the expert knowledge of how the receiver should be adapted given the measured data.

Explaining the correlation of the output and the input, some rules were introduced, as obvious in Tables 1 and 2. Test results of the field and common-sense reasoning are basis of the rules determination.

Table 1. Fuzzy rules of block 1.

		Doppler Frequency		
		Low	Medium	High
Carrier Phase	Low	**High**	**High**	**High**
	Medium	**Low**	**Low**	**Medium**
	High	**Medium**	**Medium**	**Low**

Table 2. Fuzzy rules of block 2.

		Pseudo-range		
		Low	Medium	High
PDOP	Low	**Medium**	**High**	**High**
	Medium	**Low**	**Medium**	**High**
	High	**Low**	**Low**	**Medium**

Defined fuzzy rules determines evaluation of the signal differences and placement of the output in [0, 1] in three groups of {High, Medium, Low}. If received signals are spread out and setting interspace for the received data is hard, the mean and standard deviation of data are utilized to determine intervals of membership function and their grouping.

In block 1, the input parameters, achieved from the receiver, utilized in designing the fuzzy controller are the carrier phase and Doppler frequency. Similarly, the corresponding inputs in block 2 are PDOP and Pseudo-Range (PR) of the satellites linked with three membership functions named “low”, “medium”, and “high”. Figures 3 and 4 show the selected membership functions for output and input fuzzy variables. The output fuzzy variable is an estimation for the solution quality, described in a range 0 to 10 and depicted linguistically by three triangular membership functions, named, “low”, “medium”, and “high”.

As demonstrated in figures, the core amounts of every data set demonstrating the average of the counterfeit signal under low, medium, and high deviation situations were related to the center values of the correlated membership functions. The average values indicate data classification core, because they were computed from considerable size of sampling signal. For the membership functions of the output, three triangles were used with even segmentation from zero to one and even overlaps among sets. Here, GPS data is classified into three classes.

A series of If-Then rules expound how input fuzzy-set-membership maps to output fuzzy-set membership. Matrix form of the rule base controller is represented in Tables 1 and 2. The rule base consists of nine rules and the two-input, one-output. As illustrated in tables, the elements of the matrix, the implication part (then) and the input variables with the related fuzzy sets, or μ-functions, address each consequent of the rule. Only the rules 4, 7 and 8 contain the OR connective. OR PDOP is medium, if PR is low. Therefore, output is low (first column, second row, rule 4). The “low” is related to an improved form of the μ-function “low”, $\mu_L(x)$, with the concentration operator.

$$\mu_{con(VL)}(x) = [\mu_L(x)]^2 \qquad (2)$$

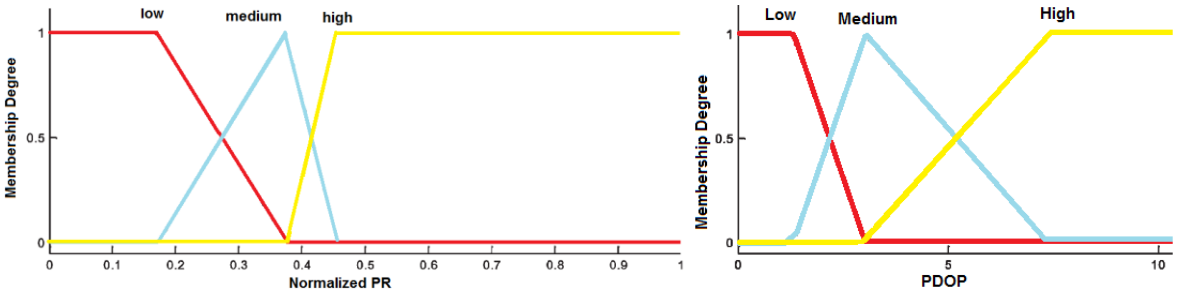


Fig. 3 Membership functions used in fuzzy inference system for the (a) PR and (b) PDOP.

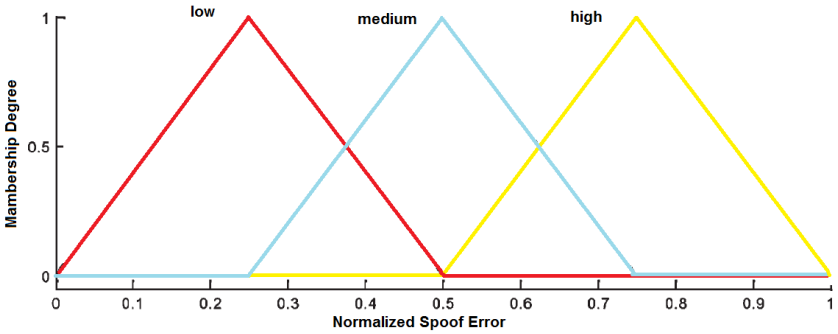


Fig. 4 Membership functions used in fuzzy inference system for the output variable.

Various rule bases have been performed, for optimizing the sensitivity of the output through the input changes. For instance, "output" of a rule base including only AND-connected antecedents gives upper limit of maximum PR and minimum PDOP. The defuzzification phase uses the criterion that is the CoA (centroid). The result obtained from the aggregation of the fuzzy sets are connected with the rules activated by the crisp input values.

$$CoA = \frac{\int_U x\mu_k(x)dx}{\int_U \mu_k(x)dx} \qquad (3)$$

Where $\mu_k(x)$ is the membership function of the *k-th* input, and U is the variable universe. For the defuzzification step, the *Mean of Maximum* technique is suited for pattern recognition and classification. It yields a stepped output/input feature of the controller. For considering more precise observation with a test statistic near to the statistical test crucial value. Along the statistical tests, a technique based on fuzzy logic could be utilized. The observation errors made the last decision about counterfeit signals in the fuzzy logic method. Membership functions is essential in spoof recognition. The counterfeit signals are outputs of the technique. Relation between residuals and errors demonstrates that the observation errors determine residual magnitudes.

$$v = -Q_V P\Delta \qquad (4)$$

Where the multiplication $Q_V P$ equals to redundancy matrix R in navigation stage of the receiver. Equation (5) presents the extended formation of equation (4) and R.

$$\begin{bmatrix} V_1 \\ V_2 \\ \mathrm{M} \\ V_n \end{bmatrix} = \begin{bmatrix} r_{11} & \mathrm{r}_{12} & \cdots & \mathrm{r}_{1n} \\ r_{21} & \mathrm{r}_{22} & \cdots & \mathrm{r}_{2n} \\ \mathrm{M} & \mathrm{M} & & \mathrm{M} \\ r_{n1} & \mathrm{r}_{n2} & \cdots & \mathrm{r}_{nn} \end{bmatrix} \begin{bmatrix} \Delta_1 \\ \Delta_2 \\ \mathrm{M} \\ \Delta_n \end{bmatrix} \qquad (5)$$

Other observation errors cause that the normal observation be regard as a fake one. For this reason, utilizing the observation errors the final judgment is realized. Values of fuzzy memberships are appointed to them and the observation is judged (whether fake or authentic) by the amplitude of these membership values. The introduced process to this step will be explained here.

At first step, a statistical test divides the output values into two main groups: normal vales $\mu_D(v_i)$ that are successful on the test, and abnormal values $\mu_C(v_i)$ that are unsuccessful on the test. Therefore, values of membership function are placed in one of the classes:

$$\mu_C(V_i) = \begin{cases} 0 & \mathrm{T_i} \le \mathrm{q} \\ \dfrac{1.0}{1.0 + (\dfrac{e}{T_i - q})^2} & \mathrm{T_i} \ge \mathrm{q} \end{cases} \qquad (6)$$

Where, e is the standardization element. Complementation characteristic of fuzzy sets help that related values of set D be given after determination of membership values of set C.

$$\mu_D(V_i) = 1 - \mu_C(V_i) \qquad (7)$$

The redundancy matrix is utilized besides the membership values, for the membership values of the observation errors. All row values of R are divided to the biggest element in the corresponding row.

$$\tilde{r}_{ij} = \frac{|r_{ij}|}{\max_j(|r_{ij}|)} \qquad (i, j = 1,2,\ldots,n) \tag{8}$$

We say relative redundancy matrix to the new generation matrix.

$$\begin{bmatrix} V_1 \\ V_2 \\ M \\ V_n \end{bmatrix} = -\begin{bmatrix} \tilde{r}_{11}\Delta_1 & \tilde{r}_{12}\Delta_2 & \ldots & r_{1n}\Delta_n \\ \tilde{r}_{21}\Delta_1 & \tilde{r}_{22}\Delta_2 & \ldots & r_{2n}\Delta_n \\ M & M & M & \\ \tilde{r}_{n1}\Delta_1 & \tilde{r}_{n2}\Delta_2 & \ldots & r_{nn}\Delta_n \end{bmatrix} \tag{9}$$

A considerable point is that the most influenced observations due to spoof attack have the minimum participation to the most likely normal outputs and have the maximum participation to the most likely unmoral outputs.

L is the set of the observation errors with minimum efficacy on the most normal output values and *G* is the set of the observation errors with maximum efficacy on the most abnormal output values. The observation errors we called 'spoof errors' are placed in the set *H*. The corresponding observation to the $\mu_G(\Delta i) = \tilde{r}_{ji} \times \mu_C(v_j)$ error in set *H* is presented as spoof attack.

When the output and input parameters are explained for the system, the next stage is planning the membership functions that describe the fuzziness in a fuzzy set. Devotion of functions or membership values to fuzzy parameters are based on some logical operations or algorithms [19]. In order to simplicity of computational, the triangle membership functions were utilized. The outcomes of the different spoof data sets define the variables of input membership functions. Designing membership functions may be clearly extracted from common sense reasoning or human knowledge. Triangular membership functions are effective over a wide range of estimation and control problems. The maximum relative contribution of the i_{th} observation error to the residuals that have membership values greater than 0.5 or equal in the set *C* is searched for obtaining the membership values of the observation errors of the set *G*. After that, the membership value of the related residual is multiplied by this corresponding value as:

$$\tilde{r}_{ji} = \max_{k=u,v,\ldots,w}(\tilde{r}_{ki}) \tag{10}$$

$$\mu_G(\Delta_i) = \tilde{r}_{ji} \times \mu_C(v_j) \tag{11}$$

Comparably, for sets *D* and *L*, the complementary amount of this corresponding value is multiplied by the membership value of the related output values as:

$$\tilde{r}_{mi} = \max_{k=x,y,\ldots,z}(\tilde{r}_{ki}) \tag{12}$$

$$\mu_L(\Delta_i) = (1.0 - \tilde{r}_{mi}) \times \mu_D(v_m) \tag{13}$$

Fuzzy sets have intersection feature that makes the membership values of the observation errors in the intersection set *H* be obtained.

$$\mu_H(\Delta_i) = \min(\mu_G(\Delta_i), \mu_L(\Delta_i)) \quad (i = 1,2,\ldots,n) \tag{14}$$

Calculation of the critical value ($C\mu H$) executes whereas values of relative effects utilized throughout calculating corresponding membership values in the set *H* and the membership values of observation errors, can be:

$$p \Rightarrow \begin{cases} P_i = \tilde{r}_{ji} & \text{if} \quad \mu_H(\Delta_i) \in \mu_G(\Delta_i) \\ P_i = 1 - \tilde{r}_{mi} & \text{if} \quad \mu_H(\Delta_i) \in \mu_L(\Delta_i) \end{cases} \tag{15}$$

$$C\mu H = \frac{\sum P_i \, \mu_H(\Delta_i)}{\sum P_i} \tag{16}$$

If membership values of an observation error is larger than the critical value, it will be considered as spoof fault. However, this presumption must be attested. After that, the error magnitudes over than the critical value are approximated and their signification are examined. Ref. [20] has suggested a procedure explained here:

$$K_{n\times m} = \begin{bmatrix} 0 & 0 & K & 0 \\ 0 & 1 & K & 0 \\ 0 & 0 & K & 0 \\ M & M & M & M \\ 1 & 0 & K & 0 \\ 0 & 0 & K & 1 \end{bmatrix} \tag{17}$$

Where, *K* is the location matrix of spoof errors, and *n* and *m* are the number of observations and observation errors over than critical value, respectively. The corresponding row for each spoof error is *1*. This location matrix is basis of calculating the weight matrix and the spoof error values.

$$Pss = K^T PK - K^T PA(A^T PA)^{-1} A^T PK \tag{18}$$

$$\nabla_S = -Pss^{-1} K^T P_V \tag{19}$$

In equations (18) and (19), $P_{n\times n}$ and $Pss_{m\times m}$ are weight matrix of observations and spoof errors, respectively. $A_{n\times u}$ is matrix of the design, $v_{n\times 1}$ is the residuals vector, and $\nabla s_{m\times 1}$ is the spoof errors vector. Based on above mentioned rule, the spoof errors values (∇s) are examined though a statistical test to decide about their significance.

The total fuzzy inference system has a numeric output named *SE* in a range between 0 and 1. The *SE* value, which defines the degree of position error, is moreover employed to categorize GPS data. A greater value shows a more likelihood of large spoof error.

This study uses the Mandeni-type fuzzy inference system with max-min composition [17]. After that, the CoA defuzzification procedure is performed for extracting a crisp value, *SE*, as an indicative magnitude from the output fuzzy set. A GPS data are categorized into three groups: low, medium, and high data collected spoof errors. The values in the middle of close classes are pointed to the medium among the related membership functions. Moreover, it is an inherent pattern for fitting the output of the CoA defuzzification. Specifically, data are categorized as low-spoof-error if *SE* is smaller than 0.33 (the average of "Small" and "Medium" membership functions core

values). Data are classified as high-spoof-error if the value of *SE* is larger than 0.66 (the average of the "Medium" and "Large" membership functions core values). As the obtained results reflect, as a first time poisoning susceptibility of a civil GPS receiver can be estimated by the suggested system.

4. Results

The performance of the proposed technique has been evaluated on a number of real spoof data collections. At first, the process of spoofing data collection is explained briefly. Therefore, the performance of the proposed algorithm will be analyzed in different ways. The simulation results are extracted via a laptop with Core i7 processor through 2012 version of MATLAB software.

4.1. Data Collection

Assessing the performance of the proposed spoofing countermeasure by three rooftop collected data sets. At first, generation of the delay spoofing data set will briefly explained. Earlier, saving and delaying the GPS signal is introduced [2] and the scenario is named relay deception. A spoofer software with spreading equipment is added to the typical GPS receiver to form a practical sample of intermediate spoofer.

In another aspect, spoofer transmits the fake signal to target receiver in either synchronous or asynchronous manner. In the case of synchronous attack, spoofing signal with aligned correlation peaks will be generated. In the asynchronous attack, a GPS signal simulator transmits higher power forgery correlation peak that is not aligned with authentic peak towards the target receiver. Synchronous attack is still difficult to implement and then asynchronous one is a more realistic scenario. Delay spoof is an asynchronous type spoofing by a generation mechanism that provides a data pack to investigate the proposed method. Total view of implementing system has been appeared in Fig. 5. At the left part of the figure, a transmitting RF front-end has been combined with a GPS software receiver to practically implement an intermediate attack. A GPS signal simulator is utilized to combine the RF signals instead of IF signals. Spoofing data were made in different scales by varying the runtime of data. Different scenarios have delays in range of 4, 6 and 8 seconds. The degenerated signal of this scenario can be written as:

$$d(n)=S(n)+\alpha S(n-\tau) \quad (20)$$

Here "α" is amplification factor which assumed to be 2 here. Based on the previous-mentioned scenario, "αS(n-τ)" is actually considered as interference element or "S(n)". When the analog RF input signal is transformed to the digital IF signal and before satellite acquisition, spoofing attack applies to the data.

Moreover, dynamic delay spoofing is produced as 3rd data pack for testing the suggested method in more realistic situation. In this scenario, the authentic signal of a moving car transmits its GPS signals to the victim receiver. Indeed, the spoofer is static but the victim receiver is mobile. At last, in a best real scenario, both of counterfeit and authentic signals are moving. The victim receiver goes on straight route while the spoofer deviates that in halfway.

Acquisition results of fake and authentic signals are shown in Fig. 6. In this shape, the green color denotes detected valid satellites. The parallel code phase search algorithm is used in the function acquisition of Software Receiver (SR) in 0.5 KHz frequency steps [21].

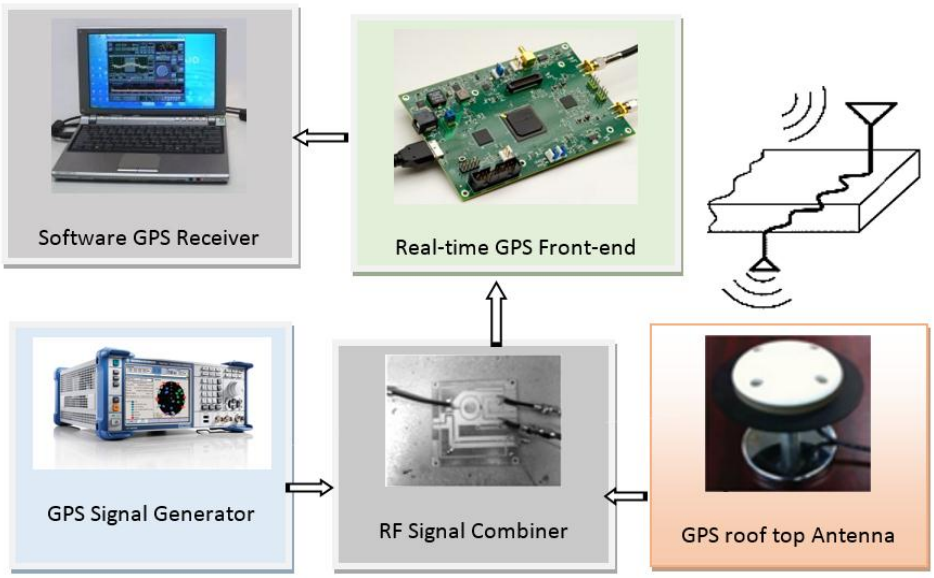


Fig. 5 Top level model for implemented system.

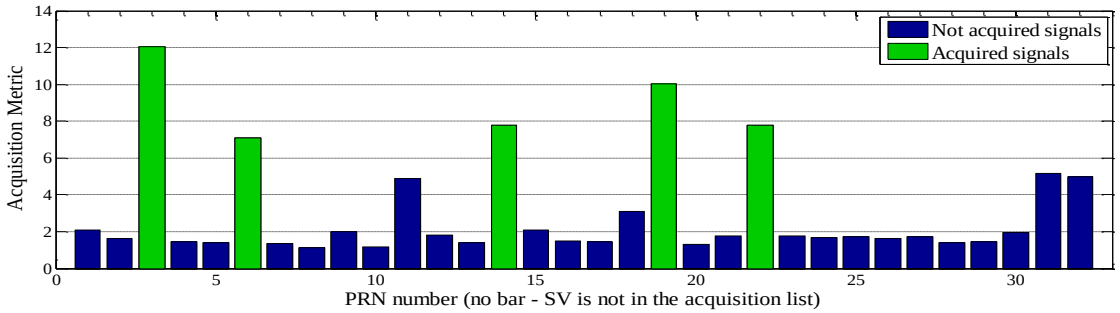
The fake signal includes three authentic satellites and the other two satellites are prevented from passing the tracking loop.

As can be seen, spoofing attacks lose the PRN3 and changes the acquisition level of the others. Histogram and frequency domain for a sample signal are shown in Fig.s 7 and 8, respectively. As can be observed, features of two signals have no obvious difference.

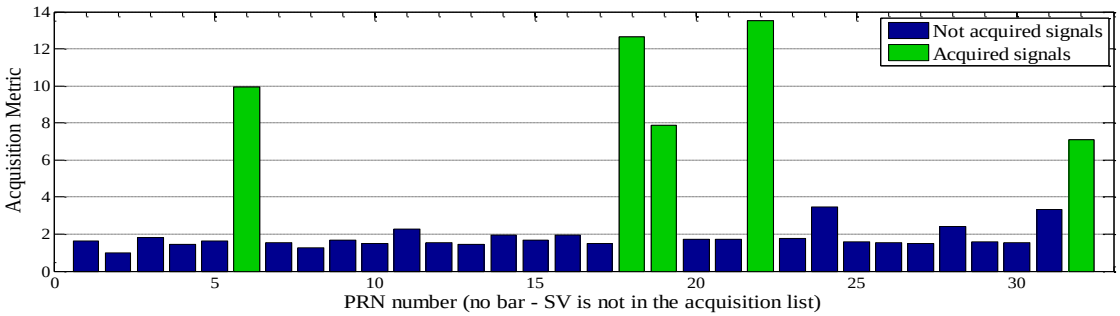
The correlation output of authentic signal is illustrated in Fig. 9(a) with quadrature and in-phase component variations. As can be seen, it is symmetric, and in-phase component is much bigger than quadrature component. Fig. 9(b), (c) and (d) demonstrate three different states of counterfeit and authentic signals interactions. In all of them, the in-phase and quadrature components have been asymmetric and the distance between them have been decreased. Characterizing these destructions is realized by proposed method.

4.2. Simulation Outputs

It is worth to note that the randomness attended by probability theory is not the same with the fuzziness attended by fuzzy set theory. In the happening of occurrence, the uncertainty is shown by randomness, while the ambiguity of an event is represented by the fuzziness. For tuning the controller of agreeable results, different choices of the membership functions have been examined. Fig. 10 demonstrates the output degree of three various controllers, resulted from the membership functions and combinations of the rule base.



(a)



(b)

Fig. 6 Acquisition results for (a) authentic and (b) fake signals.

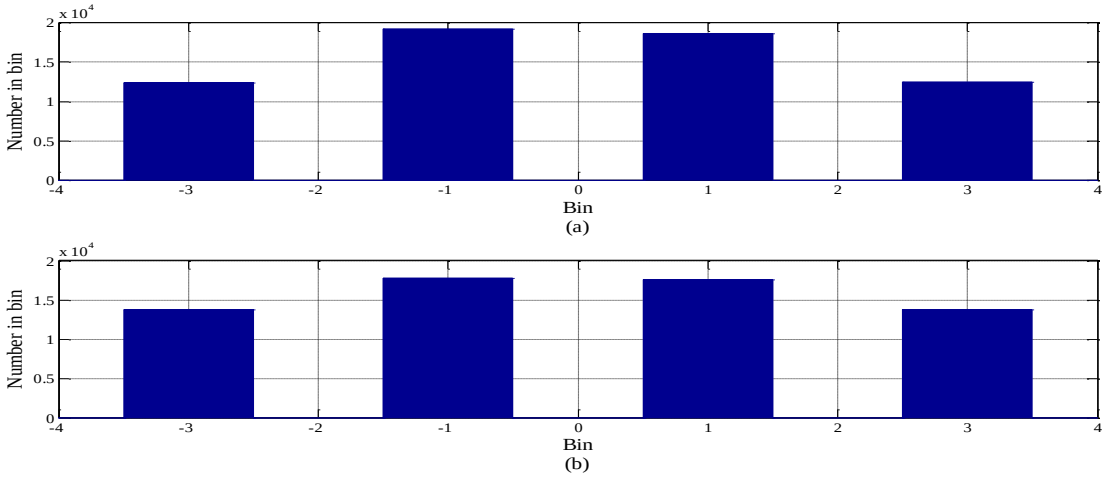


Fig. 7 Histogram (a) authentic signal and (b) spoofing signal.

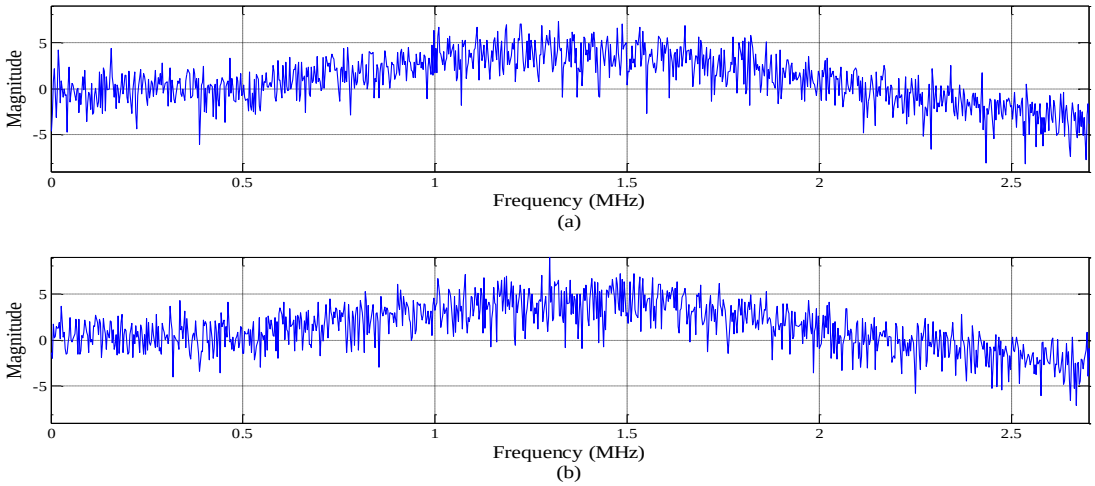


Fig. 8 Power density (a) authentic signal and (b) spoofing signal.

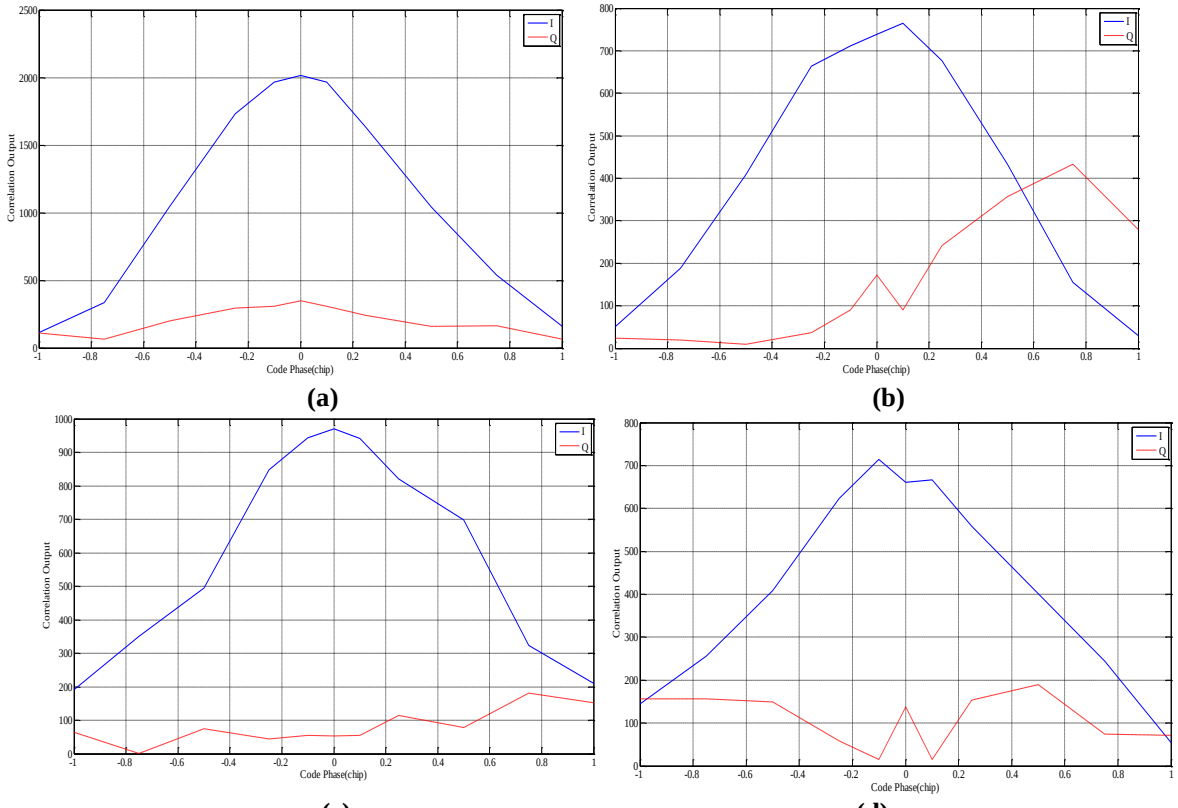


Fig. 9 Correlation output of (a) authentic signal, (b) spoofed signal (case 1), (c) spoofed signal (case 2), and (d) spoofed signal (case 3).

According to Table 3, the duration time of detecting attack was 18 seconds, detection rate was acquired over than 90% and erroneous detection are of 0.01. It is obvious from the obtained results that the output is more influenced every time there is a little change in the input values of navigation parameters, which are more important parameters between the chosen input parameters. Overhand, a considerable alter in low priority input parameters in acquisition and tracking has less effect on the output. Therefore, the system provides the expectancies properly.

Because of unsimilarity of proposed detection and mitigation methods with existing ones, accurate comparison with prior works is difficult. Table 4 produces a comparative evaluation of new and previous detection methods based on necessary equipment, advantages and disadvantages [10,22]. In order to reliable and correct judgment, we assigned a numerical value to any feature. For this purpose, for

any feature, worst and best case is considered; 0 score is dedicated for worst sate and 5 score for the best state. After that, a number from 0 to 5 is pointed to any feature depends on algorithm performance. For example, about "necessary equipment" characteristic, a method takes 5 scores, if needed no extra equipment, and earns 0 scores in case of need to basic changes in receiver building. Result of numbering is illustrated in Fig. 11. It is clear the suggested algorithm gets 12 points that is better that others.

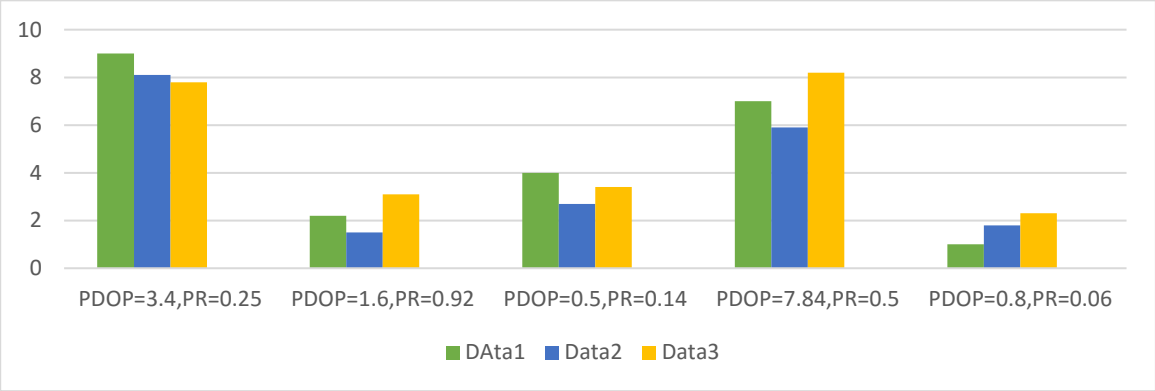


Fig. 10 Output rating in three extreme cases for the three controllers designed.

Table 3. Input and output values for ten sample data.

Inputs				Normalized output
PDOP	Normalized PR	Carrier phase	Doppler frequency	
3.4	0.25	5034	71	9
1.6	0.92	2322	74	2.1
0.5	0.14	2384	16	4
7.8	0.5	1013	47	7
0.8	0.06	778	69	1
9.3	0.33	326	58	9.5
2.4	0.65	2239	16	5
1.9	0.18	950	48	3.5
0.2	0.8	773	69	0.5
8	0.43	1643	22	8

Table 4. Comparing previous methods and proposed algorithm.

Detection techniques	Considered feature	Necessary equipment	Advantages	Disadvantages
Power monitoring	Power and amplitude	Hardware for power measurement	Simplicity	Large vulnerability and high implementation cost
TOA	Time of signal arrival	Software upgrading	Simple implementation	Unreliable and predictability of TOA
Spatial processing	Correlation	Antenna array	No need for previous information	High cost and inefficiency in multi-antenna spoofer
SQM	Correlation	Software upgrading	Simple detection	Inefficiency in multi-path and need to past information
VSD	Correlation	Software upgrading	Efficient in multi-path	Inefficiency in synchronous spoofing, need prior data
VB	Correlation	Extra tracking loop	High accuracy	High implementation cost
This work	Correlation	Software upgrading	Reliable, accurate and no need to past information	Computational complexity

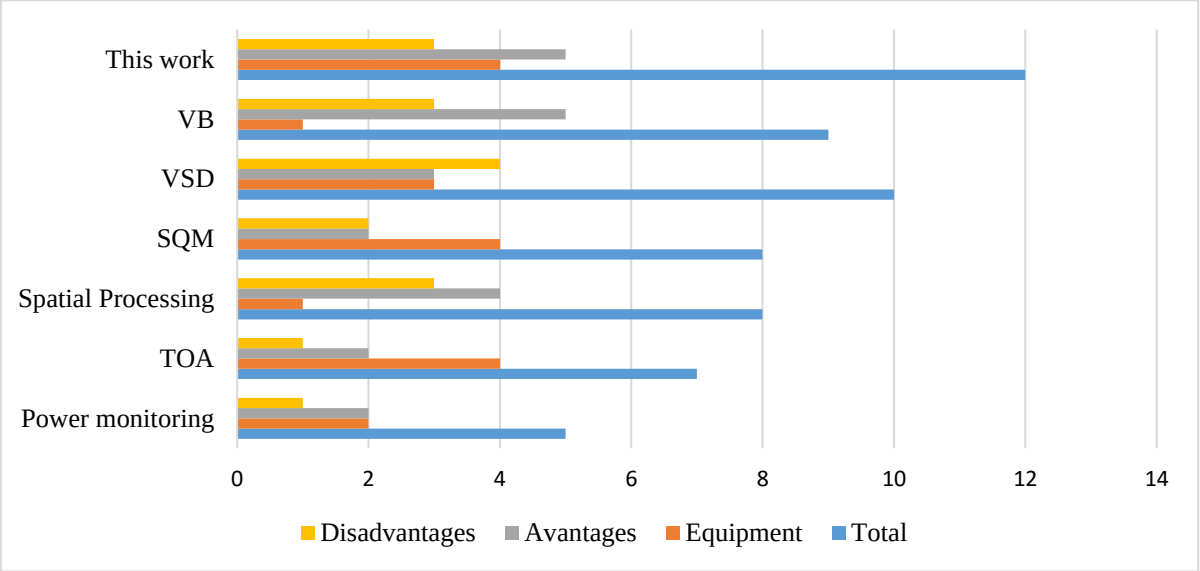


Fig. 11 Performance comparison of spoofing detection algorithms.

5. Conclusion

GPS spoofing is today a serious world threat because of a mostly academic effort, limited to navigation experts with noticeable learning and resources to hand. Fuzzy logic is a methodology to compute considering truth degree unlike Boolean logic as false or true. Fuzzy logic appears near to the manner that human mind thinks. We gather data form partial truths. After overreaching settled threshold it can be further aggregated into higher truths. In our proposed approach based on fuzzy logic, the statistical tests and fuzzy set relations are utilized together for detecting the spoofing attack. Suggesting data classification using fuzzy theory, we could picked out GPS positions with low, medium and large errors. The proposed detection method results in decrease of running time and false detection rate and increase of truly detection rate rather common approaches. Our study take advantage of the fuzzy logic theory: facility of modelling, non-linear input-output mapping, real-time implementation to enhanced the receiver performance and capability of managing various kinds of uncertainty simultaneously.

6. Reference

[1] C. Günther, "A Survey of Spoofing and Counter-Measures", Journal of the Institute of Navigation, Vol.61, No.3, pp.159-172, 2014.

[2] A. R. Baziar, M. Moazedi, and M. R. Mosavi, "Analysis of Single Frequency GPS Receiver under Delay and Combining Spoofing Algorithm", Wireless Personal Communications, Vol.83, No.3, pp.1955-1970, 2015.

[3] A. Farhadi, M. Moazedi, M. R. Mosavi, and A. Sadr, "A Novel Ratio-Phase Metric of Signal Quality Monitoring for Real-Time Detection of GPS Interference", Journal of Wireless Personal Communications, Vol.97, No.2, pp.2799-2818, 2017.

[4] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing", The 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, pp.1-11, Sep. 2011.

[5] Y. Guo, L. Miao, and X. Zhang, "Spoofing Detection and Mitigation in a Multi-correlator GPS Receiver Based on the Maximum Likelihood Principle", Sensors, Vol.9, No.1, pp.37-54, 2019.

[6] M. R. Mosavi, A. R. Baziar, and M. Moazedi, "De-noising and Spoofing Extraction from Position Solution using Wavelet Transform on Stationary Single-Frequency GPS Receiver in Immediate Detection Condition", Journal of Applied Research and Technology, Vol.15, No.4, pp.402-411, 2017.

[7] B. Shin, M. Park, S. Jeon, H. So, G. Kim, and C. Kee, "Spoofing Attack Results Determination in Code Domain using a Spoofing Process Equation", Sensors, Vol.19, No.2, pp.293-311, 2019.

[8] L. Baoa, R. Wub, W. Wangb, and D. Lub, "Spoofing Mitigation in Global Positioning System Based on C/A Code Self-coherence with Array Signal Processing", Journal of Communications Technology and Electronics, Vol.62, No.1, pp.66-73, 2017.

[9] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation", GPS Solution, Vol.104, No.6, pp.1-12, 2016.

[10] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network

in Single-Frequency GPS Receivers", Journal of Navigation, Vol.71, No. 1, pp.169-188, 2018.
[11] M. R. Mosavi, A. Khavari, A. Tabatabaei, and M. J. Rezaei, "Jamming Mitigation using an Improved Fuzzy Weighted Least Square Method in Combined GPS and GLONASS Receiver", International Journal of Electronics and Communications, Vol.76, No.6, pp.107-116, 2017.
[12] L. A. Zadeh, "Fuzzy Sets", International Journal of Information Control, Vol.8, pp.338-353, 1965.
[13] M. R. Mosavi, "Comparing DGPS Corrections Prediction using Neural Network, Fuzzy Neural Network and Kalman Filter", Journal of GPS Solutions, Vol.10, No.2, pp.97-107, May 2006.
[14] C. J. Lin, Y. Chen, and F. R. Chang, "Fuzzy Processing on GPS Data to Improve Position Accuracy", IEEE Symposium on Soft Computing Intelligent Systems and Information Processing, pp. 557-562, 1996.
[15] S. Stubberud and R. Pudwill, "Feature Object Extraction – A Fuzzy Logic Approach for Evidence Accrual in the Level Fusion Classification Problem", Proceedings of CISMA, Lugano, Switzerland, pp.181-185, July 2003.
[16] S. C. Stubberud and K. A. Kramer, "Fuzzy Evidence Accrual Applied to Sustainable Manufacturing," Proceeding of the FUZZ-IEEE 2010, Barcelona, Spain, pp.1-7, May 2010.
[17] M. Rasoulzadeh, "Facial Expression Recognition using Fuzzy Inference System", International Journal of Engineering and Innovative Technology, Vol. 1, No.4, pp.1-5, 2012.
[18] J. H. Wang and Y. Gao, "Evaluating the Accuracy of GPS Positions under Severe Signal-Degradation using Adaptive-Network-based Fuzzy Inference Systems (ANFIS)", in Proc. 50th CASI Annu. Gen. Meeting and Conf., Montréal, QC, Canada, Apr. 2003.
[19] D. Borio and C. Gioia, "A Sum-of-Squares Approach to GNSS Spoofing Detection", IEEE Transactions on Earospace Electronic Systems, Vol.52, No.4, pp.1756-1768, 2016.
[20] A. Javaid, F. Jahan, and W. Sun, "Analysis of Global Positioning System-based Attacks and a Novel Global Positioning System Spoofing Detection/Mitigation Algorithm for Unmanned Aerial Vehicle Simulation", Simulation: Transactions of the Society for Modeling and Simulation International, Vol.93, No.5, pp.427-441, 2017.
[21] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, "A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach", Birkhäuser Boston, 2007.
[22] M. R. Mosavi, Z. Nasrpooya, and M. Moazedi, "Advanced Anti-Spoofing Methods in Tracking Loop", Journal of Navigation, Vol.69, No.4, pp.883-904, 2016.