International Journal of Control, Automation, and Systems (2015) 13(4):951-959
DOI 10.1007/s12555-014-0347-2

ISSN:1598-6446 eISSN:2005-4092
http://www.springer.com/12555

GPS Spoofing Detection using Accelerometers and Performance Analysis with Probability of Detection

Jung-Hoon Lee, Keum-Cheol Kwon, Dae-Sung An, and Duk-Sun Shim*

Abstract: This paper considers a GPS spoofing detection problem. A GPS spoofing attack attempts to deceive a GPS receiver by broadcasting counterfeit GPS signals. GPS spoofing attacks are very significant since spoofing amounts to intentional interference and the target receiver is not aware of its being attacked by GPS spoofers. We suppose that accelerometers can be used to detect the GPS spoofing signal by comparing the accelerometer outputs with the acceleration estimated from the GPS outputs. In this paper, we analyze the performance based on the probability of detection for the *K*-consecutive alarm method, as well as the modified Tong and modified *M* of *N* methods. The performance of the GPS spoofing detection algorithm is analyzed for two cases: a fixed threshold and a fixed probability of false alarm.

Keywords: Accelerometer, GPS, probability of detection, probability of false alarm, spoofing.

1. INTRODUCTION

The use of the GPS (global positioning system) has increased rapidly in various areas over the last two decades and its modernization has progressed as scheduled. The GPS signal is transmitted from 20,200km above the earth's surface and its strength is as weak as -160 dBW at the earth's surface and thus is vulnerable to various kinds of interference. Nevertheless, there are many good methods for GPS signal acquisition and tracking and some use the concept of control theory (see [1] and references therein). In reality, many GPS application systems have experienced intentional interference such as jamming and spoofing.

The spoofing threat has attracted attention since the initial findings of the 2001 Volpe Report. A GPS spoofing attack attempts to deceive a GPS receiver by broadcasting counterfeit GPS signals. Such attacks are very significant, since spoofing is an intentional interference and the target receiver is not aware of its being attacked by spoofers.

Many researchers have studied spoofing attacks [2] and anti-spoofing methods [3-10]. Spoofing attacks can be classified as simple, intermediate, or sophisticated in terms of their effectiveness and subtlety [9]. In intermediate spoofing attacks, the counterfeit signals are code-phase-aligned with the authentic GPS signals and, thus, the attack is difficult to detect. This type of sophisticated attack involves a network of spoofers and therefore replicates not only the content and mutual alignment of the visible GPS signals, but also their spatial distribution, thus fooling even multi-antenna spoofing defenses [9].

There have been many studies on the spoofing principle, spoofers, and spoofing detection methods. However, few if any spoofing detection methods using inertial sensors such as accelerometers have been reported. The acceleration estimated from the GPS information can be compared with that of accelerometers and used to declare the presence of a spoofing signal. We proposed the *K*-consecutive alarm spoofing detection method using accelerometers in [10], where a fixed threshold is used. In this case, the probability of false alarms decreases as *K* increases. However, the probability of detection also decreases as *K* increases. In this paper, we propose the use of a fixed probability of false alarm instead of a fixed threshold for the *K*-consecutive alarm method, and analyze the performance of this method as well as those of the modified Tong method and modified *M* of *N* method. The performance analysis is based on the probability of detection.

Section 2 describes how to estimate the acceleration from the GPS outputs and how to use the RMSE (Root Mean Square of Error) value of acceleration to detect the spoofing signal. Section 3 describes the three GPS spoofing detection methods using accelerometers, viz. the *K*-consecutive alarm method, modified Tong method, and modified *M* of *N* method. Section 4 describes how to calculate the probability of false alarms and the probability of detection. Section 5 describes the performance analysis of the probability of detection for a fixed threshold and fixed probability of false alarm and the conclusions are drawn in Section 6.

Manuscript received September 11, 2014; revised October 12, 2014; accepted October 21, 2014. Recommended by Associate Editor Sung Jin Yoo under the direction of Editor-in-Chief Young Hoon Joo.

This research was a part of the project titled "Development of Wide Area Differential GNSS" funded by the Ministry of Oceans and Fisheries, Korea. It was also supported by the Chung-Ang University Research Scholarship Grants in 2013.

Jung-Hoon Lee, Keum-Cheol Kwon, Dae-Sung An, and Duk-Sun Shim are with the School of Electrical and Electronics Engineering, Chung-Ang University, 84 Heuksuk-ro, Dongjak-gu, Seoul 156-756, Korea (e-mails: {playmaker5, kckwon, adszzana, dshim}@cau.ac.kr).
* Corresponding author.

2. ESTIMATION OF ACCELERATION FROM GPS VELOCITY AND THE RMSE VALUE

There are many ways to obtain the velocity of the GPS receiver. One can differentiate the position derived from the GPS information or obtain the velocity directly from the Kalman filter by including the velocity as a state variable. In addition, one can also use the Doppler frequency of the carrier wave or relative velocity between satellites and receivers to obtain the velocity of the GPS receiver. The acceleration can be estimated from the velocity obtained using one of these methods.

2.1 GPS N by N-point average acceleration

In this section, we define the terms employed for the velocity and acceleration of the GPS receiver.

Definition 1: The *GPS N-point average velocity* is defined as the average of N velocity outputs from the Kalman filter.

Definition 2: The *GPS N by N-point average acceleration* is defined as the average of N acceleration values obtained from the numerical differentiation of the *GPS N-point average velocity*.

The procedure for obtaining the *GPS N by N-point average acceleration* is shown in Fig. 1.

2.2. Estimation of the acceleration from the GPS information for a circular trajectory

The circular trajectory of the vehicle used for the simulation has a radius of 663.1m and its speed is 60km/h. The velocity and acceleration of the vehicle are expressed in the NED (north-east-down) coordinate system and calculated every 0.01sec for 330sec. Fig. 2 shows the generated trajectory, velocity and acceleration of a circular motion, and Fig. 3 shows the accelerometer output of the circular motion. The accelerometer is a MEMS sensor which has error characteristics of 5,000ug bias and 10,000ppm scale factor error.

The differentiation of the velocity to obtain the acceleration causes much noise and, thus, a lowpass filter can be used to reduce the noise using the N-point average. Fig. 4 shows the estimated velocity and acceleration obtained from the GPS Kalman filter. Fig. 4(a) shows the *GPS 100-point average velocity* and is similar to that in Fig. 1(b) which is the true value. Fig. 4(b) shows the *GPS N by N-point average acceleration* and is similar to that in Fig. 1(b).

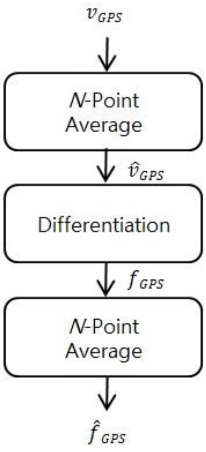
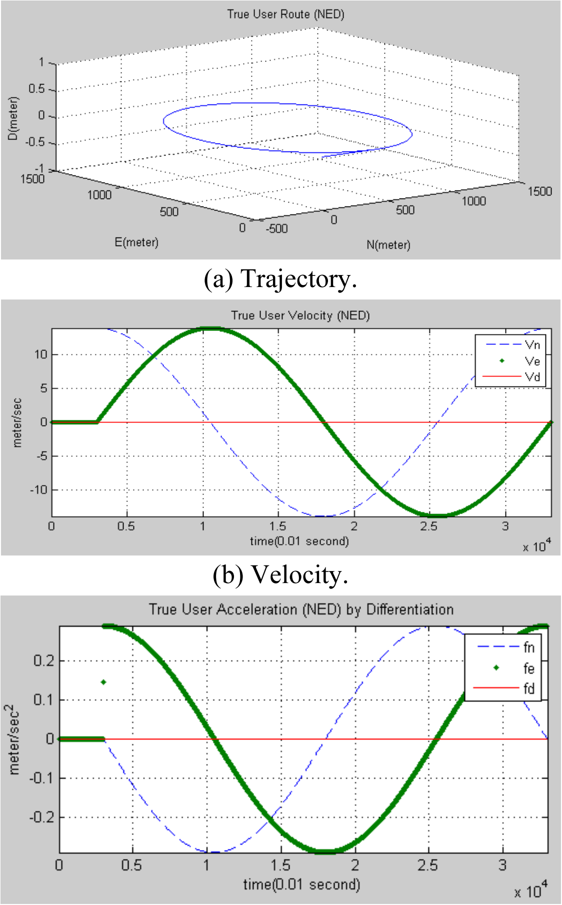


Fig. 1. GPS N by N-point average acceleration.



(a) Trajectory.

(b) Velocity.

(c) Acceleration.

Fig. 2. Trajectory, velocity and acceleration of a circular motion (True value).

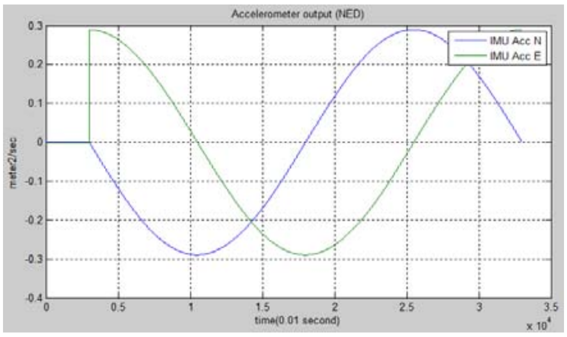
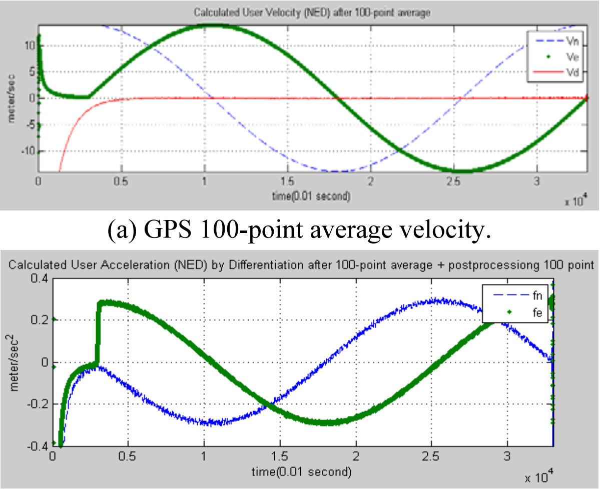


Fig. 3. Accelerometer output for the circular motion in Fig. 2(a).

2.3. RMSE value of acceleration for the circular motion

The RMSE (Root Mean Square Error) value of the acceleration estimated from the GPS velocity is calculated to determine whether there is a spoofing signal. Fig. 5



(a) GPS 100-point average velocity.

(b) GPS 100 by 100-point average acceleration.

Fig. 4. Estimated velocity and acceleration obtained from GPS information (100 point average).

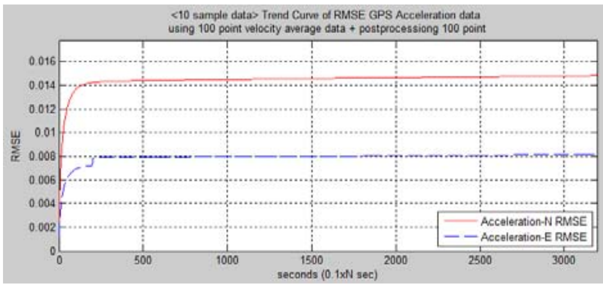


Fig. 5. Acceleration RMSE value for GPS 100 by 100-point average acceleration.

shows that the RMSE value of the *GPS 100 by 100-point average acceleration* converges as time proceeds. This means that the acceleration obtained from the normal GPS information remains around the true value within a certain range of error.

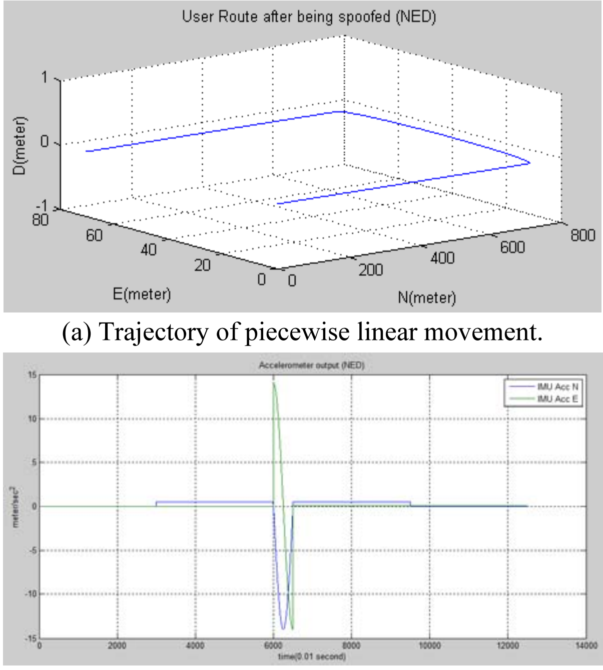
2.4. RMSE value of acceleration from a spoofing attack

The acceleration obtained from the GPS information under a spoofing attack will deviate from the accelerometer output and thus the spoofing signal can be detected.

The trajectory of the piecewise linear movement in Fig. 6 (a) is used to observe the change of the RMSE value in Fig. 5 when a spoofing attack is performed. The spoofing signal consists of three linear segments with constant velocity and two turns in the middle. Fig. 6(b) shows the accelerometer output for the trajectory of Fig. 6(a).

Let us assume that the spoofing attack begins at 210sec for a total period of 330sec. The IMU accelerometer continues to produce the true acceleration plus some noise value for the circular motion after the spoofing attack. Thus, the RMSE value of the acceleration will deviate from the normal range of error.

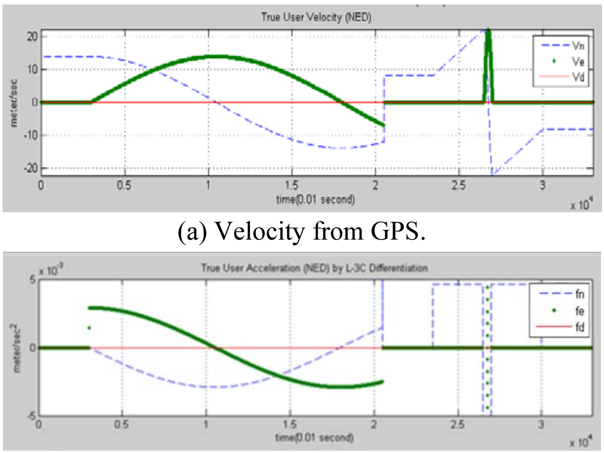
Fig. 7 shows the velocity and acceleration estimated from the GPS information when a spoofing attack is performed in the middle of the path. From 210sec, the velocity and acceleration start to deviate considerably from their normal values.



(a) Trajectory of piecewise linear movement.

(b) Accelerometer output for the trajectory of (a).

Fig. 6. Trajectory information of a spoofing signal.



(a) Velocity from GPS.

(b) Acceleration from GPS.

Fig. 7. Velocity and acceleration from GPS with spoofing attacked in the middle of the path.

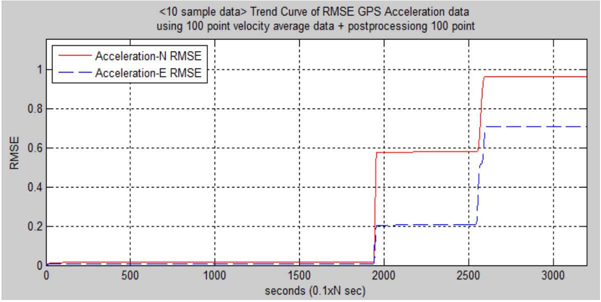


Fig. 8. RMSE value of GPS 100 by 100 point average acceleration ($M = 10$).

Fig. 8 shows that the RMSE value of the *GPS 100 by 100 point average acceleration* becomes large after the spoofing attack.

3. GPS SPOOFING DETECTION METHODS USING ACCELEROMETERS

In this section, the *K*-consecutive alarm algorithm [10] is described, as well as the modified Tong method and *M* of *N* algorithm which were originally used for GPS signal acquisition.

Fig. 9 shows a GPS spoofing signal detection algorithm using IMU accelerometers. First, *GPS N by N-point average acceleration* is calculated and compared with the output of accelerometers, and produces the value of E_k, the magnitude of acceleration error. The standard deviation σ_k is obtained using *M* values of E_k, from E_{k-1} to E_{k-M}. Then *K*-consecutive alarm method is applied.

3.1. *K*-consecutive alarm algorithm for GPS spoofing detection

This section explains the *K*-consecutive alarm algorithm for GPS spoofing detection in detail, as shown in Fig. 10. The threshold *Th* to detect an abnormal signal is *C* times σ_k. A fixed threshold, which means a fixed *C* value, such as $C = 3$, is used in [10]. However, we suggest the use of a fixed probability of false alarm, instead of a fixed threshold, in this paper.

Definition 3: The *K-consecutive alarm* means that the magnitude of the acceleration error E_k is greater than the threshold *Th* on *K* successive occasions, where the subscript *k* in E_k is a time index and the capital letter *K* is a design parameter.

In the case where $K = 1$ (i.e., *1-single alarm* case) and $C=3$, a threshold of 3σ means that the probability of false alarms is 0.135% in the case of a Gaussian distribution. The *K*-consecutive alarm algorithm declares the presence of a spoofing signal when abnormal cases occur *K* times successively. If a normal case, which means that the acceleration error E_k is less than the threshold *Th*, occurs after some abnormal cases which take place less than *K*-1 times, then the algorithm is reset to the very beginning, i.e., $E_{count} = 0$ and Spoof=OFF.

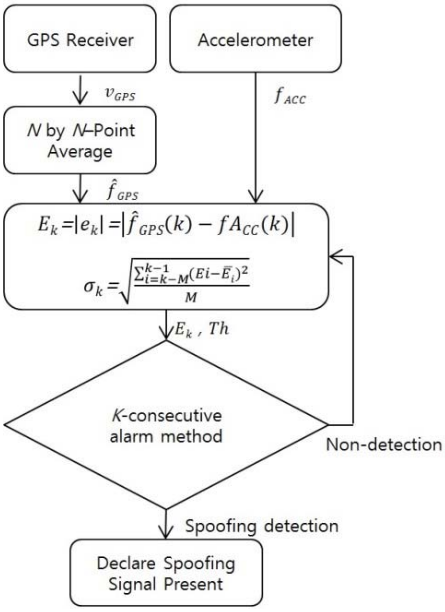

GPS Receiver
Accelerometer
v_{GPS}
f_{ACC}
N by *N*-Point Average
$\hat{f}_{GPS}$
$E_k = |e_k| = |\hat{f}_{GPS}(k) - fA_{CC}(k)|$
$\sigma_k = \sqrt{\frac{\sum_{i=k-M}^{k-1}(Ei - \bar{E}_i)^2}{M}}$
E_k, Th
K-consecutive alarm method
Non-detection
Spoofing detection
Declare Spoofing Signal Present

Fig. 9. GPS spoofing signal detection algorithm using IMU accelerometer sensor.

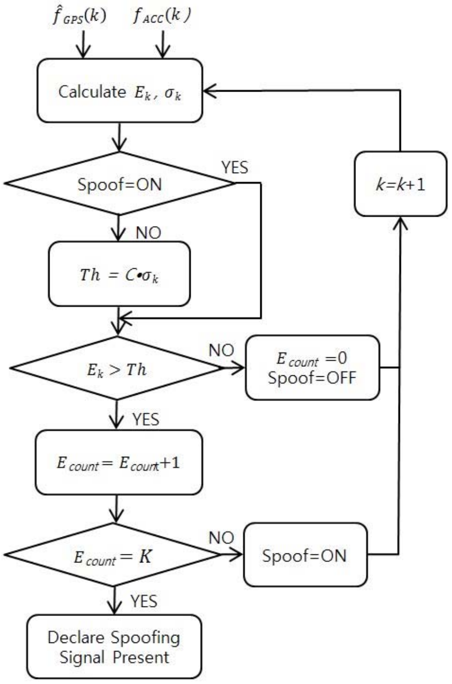


Fig. 10. *K*-consecutive alarm algorithm for GPS spoofing detection.

3.2. Modified tong algorithm for GPS spoofing detection

The Tong search algorithm [11] is used in the GPS signal acquisition algorithm and is modified as shown in Fig. 11 for spoofing detection in this paper.

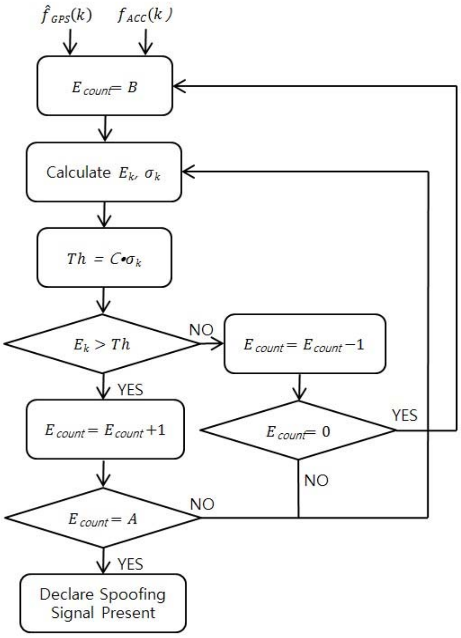


Fig. 11. Modified Tong algorithm for GPS spoofing detection.

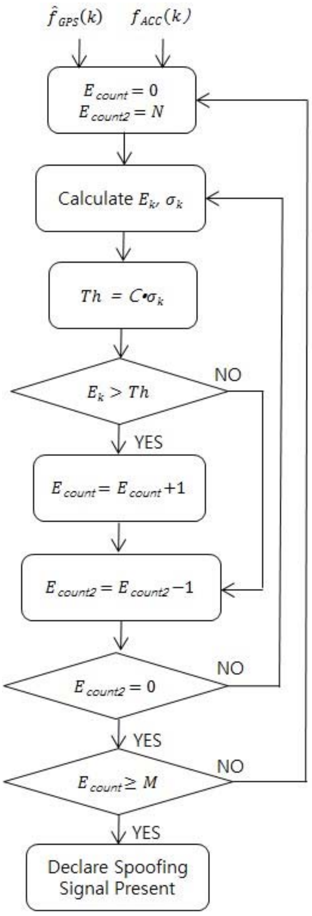


Fig. 12. Modified *M* of *N* algorithm for GPS spoofing detection.

The Tong search algorithm adds +1 to the counter if the test value is greater than the threshold and adds -1 if the test value is not greater than the threshold. If the counter value reaches the pre-determined value, which is *A*, then the algorithm declares the presence of a spoofing signal.

3.3. Modified *M* of *N* algorithm for GPS spoofing detection

The *M* of *N* search algorithm [12] is also used in the GPS signal acquisition algorithm and is modified as shown in Fig. 12 for spoofing detection in this paper. If *M* or more of the test values exceed the threshold, the algorithm declares the presence of a spoofing signal.

4. PROBABILITY OF FALSE ALARM AND PROBABILITY OF DETECTION FOR THREE GPS SPOOFING DETECTION METHODS

This section describes the probability of false alarm and the probability of detection for the three GPS spoofing methods, viz. the *K*-consecutive alarm algorithm, modified Tong algorithm and modified *M* of *N* algorithm.

4.1. Relation between probability of false alarm and probability of detection

Let us assume that the probability density function is Gaussian if there is no signal. Then, the probability of false alarm, probability of detection and threshold have the following relation.

$$P_{fa} = \int_{Th}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{z^2}{2\sigma^2}\right)} dz \tag{1}$$

$$Th = 2erfinv(1-2P_{fa})/\sqrt{2} \tag{2}$$

$$P_d = \int_{Th}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(z-m)^2}{2\sigma^2}} dz \tag{3}$$

4.2. *K*-consecutive alarm algorithm for GPS spoofing detection

The overall probability of false alarm (P_{FA}) and single probability of false alarm (P_{fa}) have the following relation.

$$P_{FA} = P_{fa}{}^{K}, \tag{4}$$

where *K* is the number of times the test value is successively greater than the threshold.

The overall probability of detection (P_D) and single probability of detection (P_d) have the following relation.

$$P_D = P_d{}^{K} \tag{5}$$

4.3. Modified tong algorithm for GPS spoofing detect*i*on

The overall probability of false alarm (P_{FA}) and single probability of false alarm (P_{fa}) have the following relation [11].

$$P_{FA} = \frac{\left(\frac{1-P_{fa}}{P_{fa}}\right)^{B} - 1}{\left(\frac{1-P_{fa}}{P_{fa}}\right)^{A+B-1} - 1}, \tag{6}$$

where *A* is the threshold and *B* is the initial value of the counter.

The overall probability of detection (P_D) and single probability of detection (P_d) have the following relation

$$P_D = \frac{\left(\frac{1-P_d}{P_d}\right)^{B} - 1}{\left(\frac{1-P_d}{P_d}\right)^{A+B-1} - 1}. \tag{7}$$

4.4. Modified *M* of *N* algorithm for GPS spoofing detection

The overall probability of false alarm (P_{FA}) and single probability of false alarm (P_{fa}) have the following relation [12]

$$P_{FA} = \sum_{n=M}^{N} \binom{N}{n} P_{fa}{}^{n} \left(1-P_{fa}\right)^{N-n}, \tag{8}$$

where *M* is the threshold and *N* is the total number of trials.

The overall probability of detection (P_D) and single probability of detection (P_d) have the following relation

$$P_D = \sum\nolimits_{n=M}^{N} \binom{N}{n} P_d^{\,n} \left(1-P_d\right)^{N-n}. \tag{9}$$

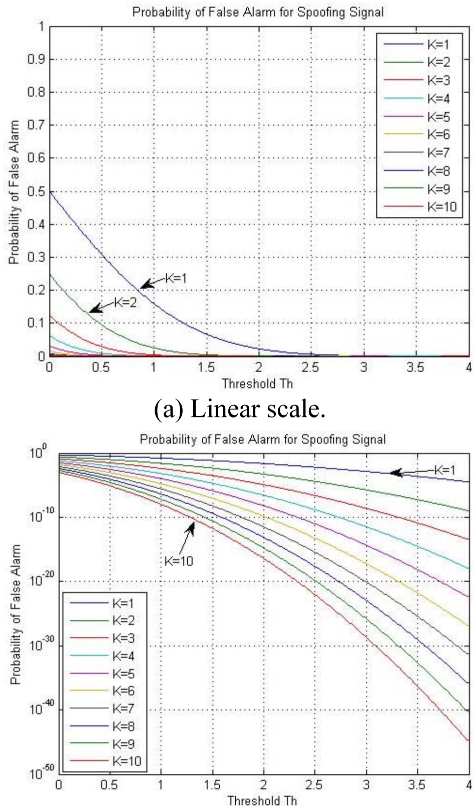
5. PERFORMANCE ANALYSIS OF PROBABILITY OF DETECTION FOR FIXED THRESHOLD OR FIXED PROBABILITY OF FALSE ALARM

We proposed the *K*-consecutive alarm algorithm in [10] for a fixed threshold. As will be seen in this section, there is a problem in the fixed threshold case. When a fixed threshold is used for the *K*-consecutive alarm method, the probability of false alarm decreases as *K* increases. In this case the probability of detection also decreases as *K* increases.

5.1. Performance of fixed threshold spoofing detection method

In this section, the *K*-consecutive alarm algorithm, as well as the modified Tong algorithm and modified *M* of *N* algorithm, will be analyzed with respect to the probability of detection when a fixed threshold is used.

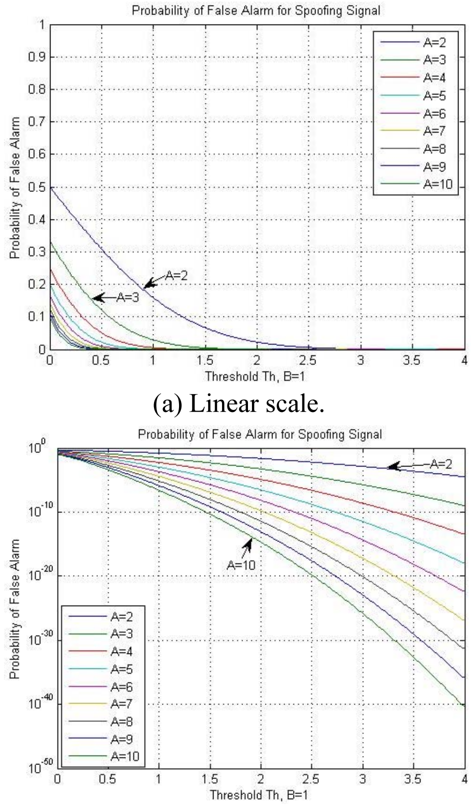
For these three algorithms, the overall probability of false alarm P_{FA} is shown in Figs. 13-15, respectively, with respect to the threshold with a normalized probability density function. A linear scale and log scale (vertical



(a) Linear scale.

(b) Log scale(vertical axis).

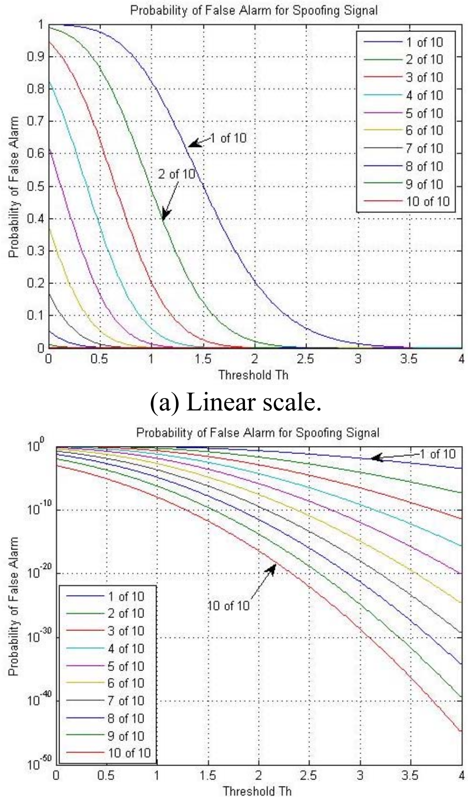
Fig. 13. Probability of false alarm for *K*-consecutive alarm algorithm.



(a) Linear scale.

(b) Log scale(vertical axis).

Fig. 14. Probability of false alarm for modified Tong algorithm.



(a) Linear scale.

(b) Log scale(vertical axis).

Fig. 15. Probability of false alarm for modified *M* of *N* algorithm.

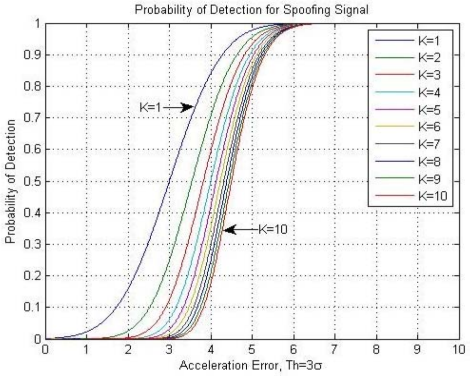


Fig. 16. Probability of detection for K-consecutive alarm algorithm with threshold $Th = 3\sigma$.

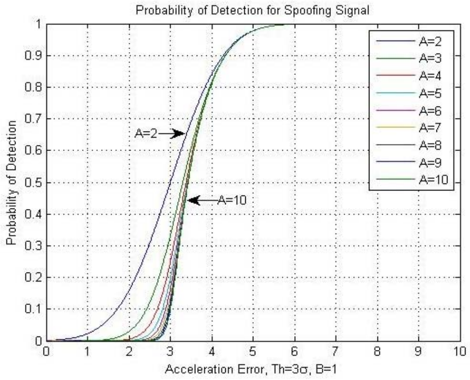
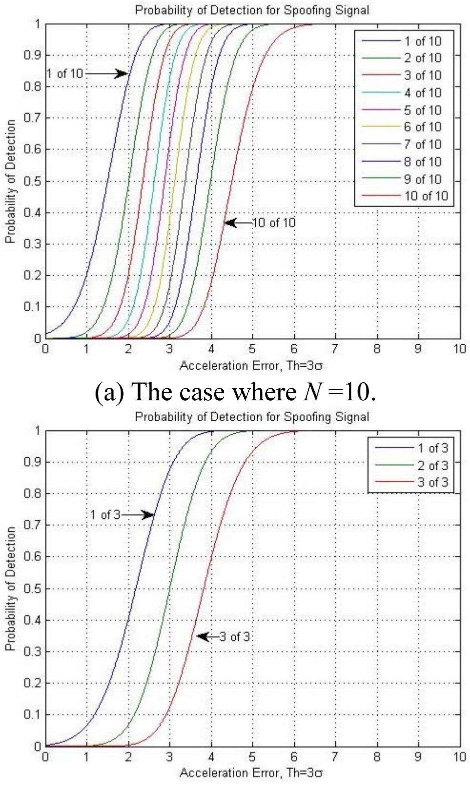


Fig. 17. Probability of detection for Modified Tong algorithm with threshold $Th = 3\sigma$.



(a) The case where N =10.

(b) For the case of N =3.

Fig. 18. Probability of detection for modified M of N algorithm with threshold $Th = 3\sigma$.

axis) are used in each figure. As the threshold increases, the probability of false alarm decreases. As K increases, the probability of false alarm decreases.

Figs. 13 through 15 shows that the probability of false alarm becomes almost zero when the threshold is greater than 3. When the threshold is fixed at $Th = 3\sigma$, the probability of detection is shown with respect to the acceleration error in Figs. 16 through 18.

In case of a fixed threshold, the three algorithms show that the probability of false alarm decreases as K, A, and N increase, which means that the probability of detection also decreases as K, A, and N increase. Thus, the fixed threshold algorithms contain a critical problem for use in spoofing signal detection, since the decision can be made on the basis of a single alarm.

A possible candidate for the performance measure for spoofing signal detection is the probability of detection.

5.2. Performance of spoofing detection method for fixed probability of false alarm.

The overall probability of detection with a fixed probability of false alarm $P_{FA} = 10^{-6}$ is shown in Figs. 19 through 21. Figs. 19 and 20 show that as K or A increases, the probability of detection increases. We can choose the appropriate K or A according to the acceleration error and the probability of detection from Figs. 19 and 20.

The performance of the three algorithms with respect

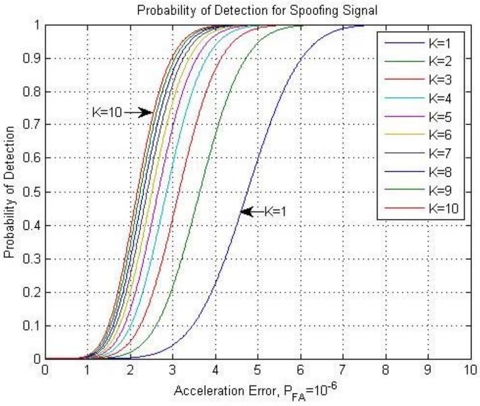


Fig. 19. Probability of detection for K-consecutive alarm algorithm with $P_{FA} = 10^{-6}$.

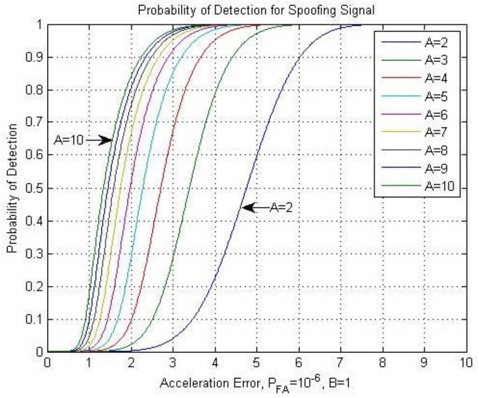


Fig. 20. Probability of detection for modified Tong algorithm with $P_{FA} = 10^{-6}$ and B =1.

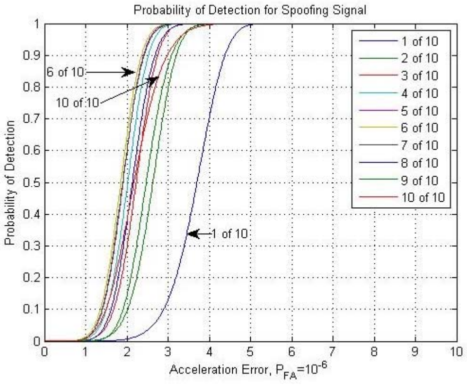


Fig. 21. Probability of detection for M of N algorithm with $P_{FA} = 10^{-6}$ and $N = 10$.

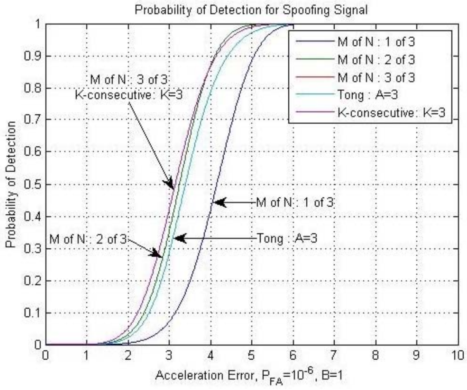


Fig. 22. Comparison of three algorithms with $K = 3$, $A = 3$, $N = 3$, and $P_{FA} = 10^{-6}$.

to the probability of detection differs slightly depending on the values of K, A, M, and N. The performance of the K-consecutive alarm algorithm is best when $K = 3$, $A = 3$, and $N = 3$, as shown in Fig. 22.

6. CONCLUSION

This paper describes several methods of detecting GPS spoofing signals using accelerometers by comparing the acceleration estimated from the GPS outputs with the accelerometer outputs. We proposed the K-consecutive alarm algorithm with a fixed probability of false alarms and analyzed the performance of the spoofing detection methods with respect to the probability of detection. For three algorithms, viz. the K-consecutive alarm method, modified Tong method and modified M of N method, the probabilities of detection are obtained and compared with each other for both fixed threshold and fixed probabilities of false alarm. For a fixed threshold, there is a critical problem in that as the number of measurements used for detecting the spoofing signal increases, the probability of detection decreases. Thus, a fixed probability of false alarm is appropriate for use in a spoofing detection method. The performance of the three algorithms with respect to the probability of detection varies depending on the number of measurements used for detecting the spoofing signal. When the number of measurements is three, the K-consecutive alarm algorithm shows the best performance among the three methods based on the probability of detection.

REFERENCES

[1] S. Jeon, C. Kim, G. Kim, O. Kim, and C. Kee, "Optimal signal tracking algorithm for GNSS signal using moving set-point LQG system," *International Journal of Control, Automation, and Systems*, vol. 11, no. 6, pp. 1214-1222, December 2013.

[2] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," *Proc. of the 18th ACM Conference on Computer and Communications Security*, pp. 75-86, 2011.

[3] Y. Bardout, "Authentication of GNSS position: an assessment of spoofing detection method," *Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, pp. 436-446, September 2011.

[4] S. L. Cho, M. Y. Shin, S. J. Lee, and C. Park, "Performance comparison of anti-spoofing methods using pseudorange Measurements," *The Korea Institute of Military Science and Technology*, vol. 13, no. 5, pp. 793-800, October 2010.

[5] F. Dovis, X. Chen, A. Cavaleri, K. Ali, and M. Pini, "Detection of spoofing threats by means of signal parameters estimation," *Proc. of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation*, pp 416-421, September 2011.

[6] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 1-16, May 2012.

[7] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," *Proc. of International Technical Meeting of the Institute of Navigation*, pp. 868-882, 2010.

[8] H. Wen, P. Y. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," *Proc. of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation*, pp. 1285-1290, 2005.

[9] K. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing: securing the future PNT," *GPS World*, pp. 32-63, January 1, 2012.

[10] K.-C. Kwon, C.-K. Yang, and D.-S. Shim, "Spoofing signal detection using accelerometers in IMU and GPS information," *The Transactions of the Korean Institute of Electrical Engineers* (in Korean), vol. 63, no. 9, pp. 1273-1280, September 2014.

[11] S. Barron, "M of N search detector," *Personal Correspondence, Texas Instruments Incorporated, Dallas, Texas*, 25 May 1995.

[12] P. S. Tong, "A suboptimum synchronization procedure for pseudo noise communication systems," *Proc. of National Telecommunications Conference*, pp. 26D-1-26D-5, 1973.

Jung-Hoon Lee received his B.S. degree in Electronic Engineering from Dan-Kook University, Korea in 2013. He is currently a master student at Chung-Ang University, Korea. His research interests include GNSS and control.

Keum-Cheol Kwon received his B.S. and M.S. degrees in Electrical and Electronics Engineering from Chung-Ang University, Korea, in 2001 and 2003, respectively. He is currently a Ph.D. student at the same school. His research interests include computer architecture, embedded systems, and GNSS.

Dae-Sung An received his B.S. degree in Electrical and Electronics Engineering from Chung-Ang University, Korea in 2014. He is currently a master student at the same school. His research interests include GNSS and control.

Duk-Sun Shim received his B.S. and M.S. degrees from the Department of Control and Instrumentation Engineering in Seoul National University, Korea, in 1984 and 1986, respectively. He received his Ph.D. degree in Aerospace Engineering from the University of Michigan, Ann Arbor, USA, in 1993. He served at the Department of Electrical Engineering and Computer Science in the University of Michigan as a post-doc from January 1994 to January 1995. Since March 1995, he has been with the School of Electrical and Electronics Engineering in Chung-Ang University, Seoul, Korea, where he is currently a Professor. He served as an Editor for JEET (Journal of Electrical and Engineering & Technology) between 2009 and 2011, and has served as an Editor for IJCAS (International Journal of Control, Automation, and Systems) since 2014. His research interests include robust control, robot SLAM, GNSS and inertial navigation systems, fault detection and isolation, and computer vision.