In-car GNSS Jammers Tracking System Evaluation Results

E.N. Boldenkov, I. V. Korogodin, I. V. Lipa, National Research University "Moscow Power Engineering Institute"

BIOGRAPHY

Evgeny N. Boldenkov is a docent of Radio Engineering Systems department of Moscow Power Engineering Institute since September 2010. He received his Ph.D. (candidate of sciences) in Radar and Radio-Navigation technologies at the Moscow Power Engineering Institute in 2007. The field of his scientific interests includes digital and analog signal processing in GNSS receivers, in particular, signal acquisition and optimal signal tracking algorithms.

Ilya V. Korogodin is a postgraduate student in Moscow Power Engineering Institute since July 2010. He received his M.S. in Radar and Radio-Navigation technologies at the Moscow Power Engineering Institute in 2007. His research interests include digital signal processing in GNSS receiver, primarily in the field of phase measurements.

Ivan V. Lipa is a postgraduate student in Moscow Power Engineering Institute since July 2012. He received his M.S. in Radar and Radio-Navigation technologies at the Moscow Power Engineering Institute in 2012. His research interests include both analog and digital processing systems design and signal acquisition algorithms.

ABSTRACT

A time-difference of arrival (TDOA) approach to locate active jammer source has been evaluated. The discussed monitoring system consists of several receivers distributed in space. In the proposed system time and frequency synchronization of monitoring receivers is implemented using GNSS observations. To achieve high accurate measurements both jammer and GNSS signals from all receivers are processed together simultaneously. Baseband processing block implements cross-correlation delay determination algorithm and calculates jammer position. This approach provides a possibility of determining a comparatively high accurate jammer location.

Both computer simulation and experiments were used to test jammer monitoring system. The result of the study has shown that pseudorange-based jammer location technique can be implemented in practice.

INTRODUCTION

GNSS equipment is widely used nowadays in many fields. One of the major concerns is the vulnerability of GNSS equipment to radio interferences, especially active jammers.

Despite to the significant progress in anti-jamming techniques today not all types of user equipment can be properly protected. There are several approaches [1] to provide high anti-jamming capabilities. They are spatial processing, integration with additional sensors and reception of wide-band signals like GPS L5. The game in this field focuses on maximizing the distance between jammer and navigation receiver where the latter is able to operate for given jammer power. An obligatory condition of success is for the application scenario to suggest a considerable distance between the jammer and the receiver where the required jammer power will be inappropriately high.

The situation in an automotive navigation field is completely different. The major problem here is the availability of hand-held and in-car jammers which today are very easy to buy. The key difference of this application scenario is that the distance between the jammer and the receiver is very small. Provided that both jammer and navigation receiver are in the same car, this distance can make from one to three meters. So even a high-linear receiver front-end can be easily overdriven with relatively low-power jammer. In this mode the navigation signal will be suppressed on a front-end non-linearity which makes no sense for any latter processing. Another problem is that for some reason these advanced anti-jamming techniques are nothing to do in mass commercial products for some reasons. So in everyday life one had to rely on a standard receiver with low anti-jamming capabilities.

The vulnerability of automotive GNSS receivers makes them difficult to rely on in car alarm systems. These systems became popular several years ago which raised demand for in-car jammers. This demand has been completely fulfilled - now it is very easy to buy a GNSS

jammer. Future applications comprise intelligent transport systems where GNSS is suggested to be used for driving a car which is impossible in the current jammer threat situation.

But on the other hand the jammer itself can be located by the signal it generates. Therefore, an interference monitoring system is required. In order to be effective this system should provide a real-time jammer location with the accuracy within tens of meters. As for the car alarm application, despite the fact that the car alarm will not be able to report its coordinates, it will be possible to determine the location (and even the entire track) of the stolen vehicle by the jammer signal.

There are several jammer location techniques. A promising approach consists in the same pseudorange method as the one used in the GNSS system. Despite some difficulties, this method can provide high-accurate position and velocity determination as well as require simple hardware similar to the one used in the GNSS receiver.

The key difference between the jammer tracking and the standard position determination in GNSS systems is that the jammer signal is regarded to be unknown. We only suggest that it has considerable power and the band of the jamming signal is the same as the one of the navigation signal. The jammer signal can be extracted using a cross-correlation technique.The quality of this algorithm will determine performance of the system as a whole.

The aims of this study include experimental evaluation of pseudorange-based jammer location technique, investigation of cross-correlation jammer detection method and maximum achievable jammer detection distance.

IN-CAR JAMMER PERFORMANCE TEST

As it was mentioned above, it is very easy today to buy an in-car jammer. An extended report listing such jammers can be found in articles [2], [3]. For our tests we bought one of the most common jammers priced at just twenty five dollars. The results for the jammer we used in our tests are provided in this article.

Figure 1. In-car jammer used for tests.

The tested jammer generates chirp-modulated signal with deviation of about 20 MHz which covers both GPS and GLONASS L1 frequency range. The center frequency of its spectrum is quite unstable and changes in time in a range of 5 MHz.

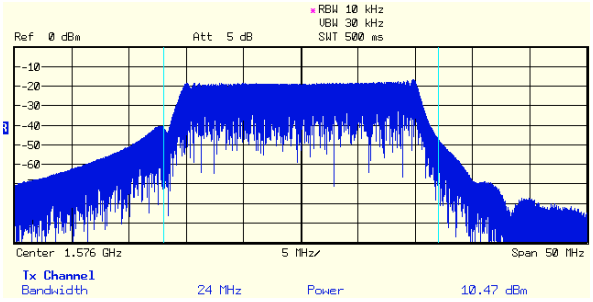

Figure 2. Jammer signal spectrum.

We analyzed frequency sweep time. As it can be seen in Figure 3, the period of modulation is 41 microsecond. Thus, the frequency modulation speed is 488 GHz/s.

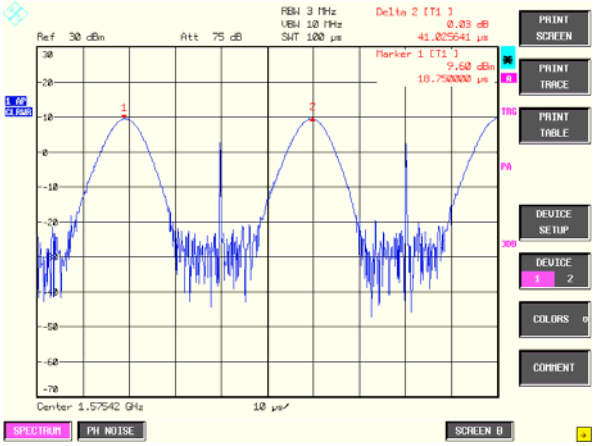

Figure 3. Jammer modulation period analysis

The power of the tested jammer is typical for the equipment of this class +10 dBm (see Fig. 1). Only one tenth of this power lays in GPS signal band, but it is quite enough for operation. The manual for the jammer claims its operation distance to be just two meters.

This was verified by experiment. When the jammer is put to its correct place – into a cigarette lighter receptacle - all navigation equipment in the car can't operate. The range of jamming is of a significant interest for our study. In order to be closer to the real conditions, we used commonly distributed commercial PND for this test. When approaching the jammer, the navigation receiver on average lost its solution 10 meters from the car with the jammer. Reaquisition took place in the distance of 50 meters when moving away from the car with the jammer.

.The result of the test showed that despite the common concerns, the operating range of the jammer is really small.

The dependence of the received jammer signal power from the distance to the car with the jammer is shown in Figure 4.

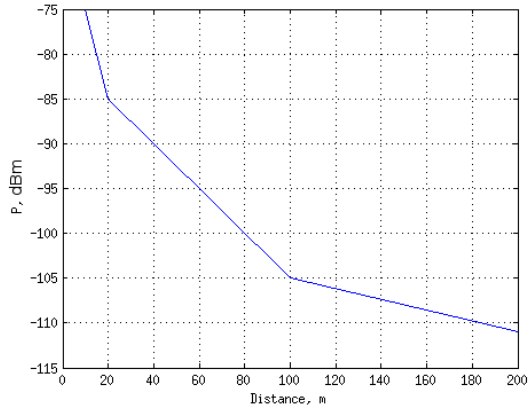

Figure 4. The received jammer power.

Another thing which makes it difficult to rely on the received power in distance measurement is the fact that the antenna radiation pattern is affected by the car it is placed in. The radiation pattern of the jammer placed into the car is shown in Figure 5. In this figure one can see that the variation of the power is about 15 dB depending on the angle. This is equivalent to the variation of the jamming distance more than five times.

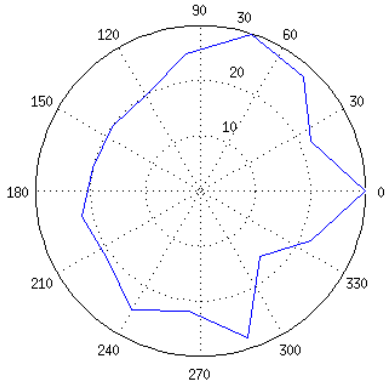

Figure 5. Radiation pattern of the jammer placed in the car.

MONITORING SYSTEM STRUCTURE

The aim of our study is to evaluate a TDOA technique of jammer positioning. The method under consideration is almost the same as in GNSS systems – that is a pseudorange method. In GNSS systems several navigation satellites with the known coordinates synchronously transmit navigation signals. User equipment having received these signals, can calculate its position. Jammer location system operates vice versa. One jammer source transmits its signal which should be received synchronously with several monitoring receivers placed at the known positions. If the bandwidth of the jamming signal is of the same order as one of the navigation signal while its power is higher, we can expect comparable level of positioning accuracy.

The structure of the system is shown in Figure 6.

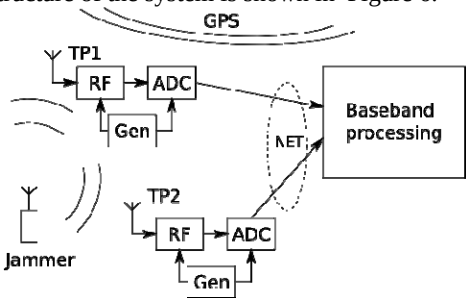

Figure 6. Jammer monitoring system structure.

This system has two main problems . The first one is that we expect the jamming signal to be unknown, so we need some algorithm to receive it and estimate its relative delays in different receivers. We suggest using a cross-correlation technique which will be discussed further.

The second problem is time and frequency synchronization of monitoring receivers, which is critical point for this system. We used GPS signals to perform this synchronization. GNSS system design provides for its receivers are capable to estimate reference generator time shift and frequency drift with the same accuracy order we see in its navigation solution. One can say the GPS signals will be jammed in this system. But as it was shown before, the operating range of the jammer we intend to track, is about ten meters. The expected positioning accuracy is worse than ten meters. If one of the monitoring receivers is jammed, we will determine that the jammer is close to this receiver. As we know the coordinates of all our receivers, we will therefore establish the coordinates of the jammer with the respective accuracy.

CROSS-CORRELATION ALGORITHM

As it was stated before, we suggest the jamming signal to be unknown. We have three suggestions about the jammer. The first is that the jamming signal has significant power. That is true, as otherwise it would not affect the operation of the navigation equipment. The second suggestion is that the jamming signal has a broad frequency band. This is critical for relative delay estimation. The proposed algorithm will not operate with narrow-band interference. The third suggestion is that the jamming signal period is long enough to allow us to solve the range ambiguity. For the jammer we tested, the period was 41 microseconds which is equivalent to 12.3 km of the range ambiguity. This is quite enough for our purposes.

The monitoring system consist of several receivers. Each receiver performs usual super heterodyne signal processing with 4 MHz band followed by analog-to-digital conversion with sampling

frequency $f_d = \frac{1}{T_d} = 16.369 MHz$. Observations of these receivers can be expressed as:

$$y^{(m)}{}_i = J_i\left(\tau^{(m)}\right) + \sum_{k=1}^{N} s^{(m)}{}_{k,i} + n^{(m)}{}_i$$

where $J_i\left(\tau^{(m)}\right)$ - is a jammer signal on the m-th receiver input with the corresponding delay $\tau^{(m)}$, $s_{k,i}{}^{(m)}$ - is a k-th navigation signal, $n^{(m)}{}_i$ - is a m-th receiver own thermal noise.

One can see that the jammer signal is common for all receivers and differs only in terms of the propagation delay. Thermal noise is unique for every receiver, all of them are uncorrelated. Navigation signals of the different receivers are correlated, but they are below the noise level.

The proposed algorithm suggests calculation of cross-correlation of observations from all pairs of the receivers to detect the jamming presence and estimate its relative delay. It is slightly more difficult to implement it in real receivers due to the reference generator frequency drift.
The cross-corelation algorithm in the monitoring receiver operates on a intermediate frequency which contains this frequency drift. Like in conventional navigation receiver there is another source of frequency difference – the Doppler effect due to the movement of the jammer source. Thus we have to perform two-dimensional cross-correlation function calculation like in conventional GNSS receiver. The algorithm can be expressed as:

$$R^{(a,b)}{}_{n,m} = \sum_{r=1}^{NN} I^{(a,b)}{}_{n,m,r}{}^2 + Q^{(a,b)}{}_{n,m,r}{}^2 ,$$

$$I^{(a,b)}{}_{n,m,r} = y^{(a)}{}_{r,i} \cdot y^{(b)}{}_{r,i-n} \cdot \cos\left(2\pi f_m t_{r,i}\right),$$

$$Q^{(a,b)}{}_{n,m,r} = y^{(a)}{}_{r,i} \cdot y^{(b)}{}_{r,i-n} \cdot \sin\left(2\pi f_m t_{r,i}\right),$$

where (a) and (b) denote the number of the receivers to be analyzed, "n" is a current delay index, "m" is a current frequency f_m index. Here a double-index time designation sheme is used. "r" index denotes current coherent integration interval number while "i" index denotes the number of sample within this interval. This time can be expressed with double indices as
$t_{r,i} = r \cdot T + i \cdot T_d$,
where T is coherent integration time while T_d is a signal sampling interval. "NN" is non-coherent integration number as in a usual GNSS signal acquisition algorithm.

SIMULATION RESULTS

One of the major concerns is a sensitivity of the proposed algorithm. The limitation to sensitivity is the presence of GNSS navigation signals which - like jamming signals - are also correlated for different receivers. The maximum expected GNSS signal level is -150 dBWt. So the sensitivity should not be better than -140 dBWt, otherwise we will mess GNSS signals with the jammer. The results of jammer detection simulation with Neuman-Pearson criteria are shown in Figure 7. Simulation was performed in a 4 microsecond search range for delay and 5 kHz range for frequency. It can be seen that the right detection probability for -140 dBWt signal can be achieved within 1 ms coherent integration time and 4 non-coherent integrations.

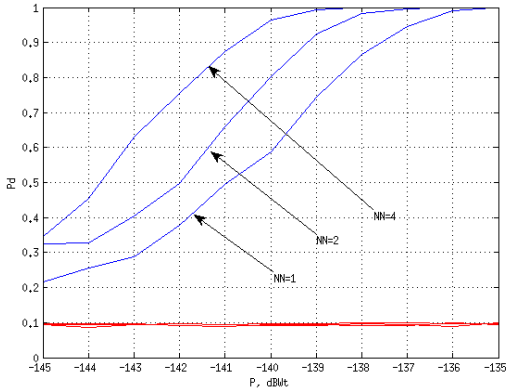

Figure 7. Jammer detection probability.

OPERATING RANGE EVALUATION

The sensitivity algorithm is known, the measurements of the received jamming signal power were given above. Unfortunately it was impossible to measure directly the power of the jamming signal below -100 dBWt with a spectrum analyzer. So the jammer detection distance was verified by experiment.

The test site where we were allowed to carry out our experiment was a field surrounded by a forest. The maximum distance for a test on this field, which limited our experiment, was about 1 km. In Figure 8 one can see a cross-correlation peak obtained at the distance of 1 km. It seems that 1 km is close to the maximum distance of the jammer monitoring operation. Still it is necessary to collect accurate statistic data of the jamming detection in future.

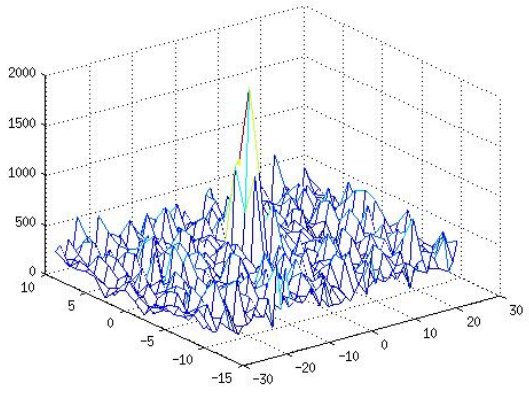

Figure 8. Correlation peak at the distance of 1 km.

PSEUDORANGE MEASUREMENT ACCURACY

To perform the pseudorange measurement test we placed two monitoring receivers and a jaming source in a line. The distance between two monitoring receivers measured with the use of GPS (with no jamming) was 116 m. The distance from the jammer to the nearest monitoring receiver was 124 m.

In Figure 9 the jamming signal relative delay (red) and receivers' time scale shift measured with the use of GPS (blue) are shown. The main problem is that receivers' time scales are not synchronized - there exist time shift and frequency drift. Both these unknowns were compensated using GPS signals.

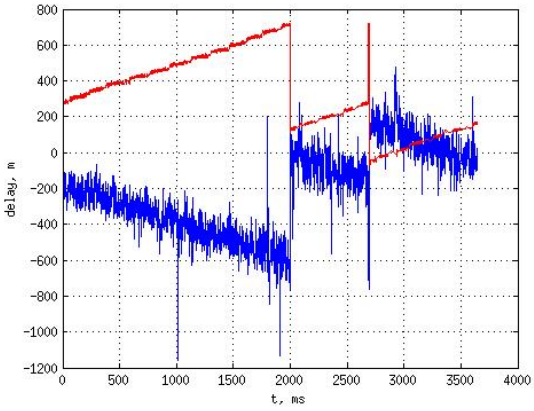

Figure 9. Raw 1 kHz delay non-compensated measurements.

The resulting raw 1 kHz cross-correlation delay measurement with compensation is shown in Figure 10.

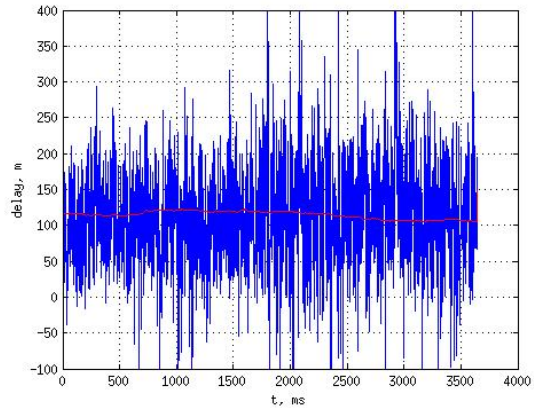

Figure 10. Raw 1 kHz compensated measurements

The mean value is 111 mm, which is very close to the right answer (116 m). In this figure one can see that the raw measurements are quite noisy mainly for GPS measurement. But we don't need precise measurement at 1 kHz rate. After additional integration and decimation to 10 Hz rate the RMS of delay measurement error made up 8 m.

POSITIONING ACCURACY ESTIMATION

The final experiment covered jammer track determination. Three monitoring receivers were distributed over the test site to achieve the best geometry. The height suggested to be known so it was 2D solution. The result of the measurement is shown in Figure 10.

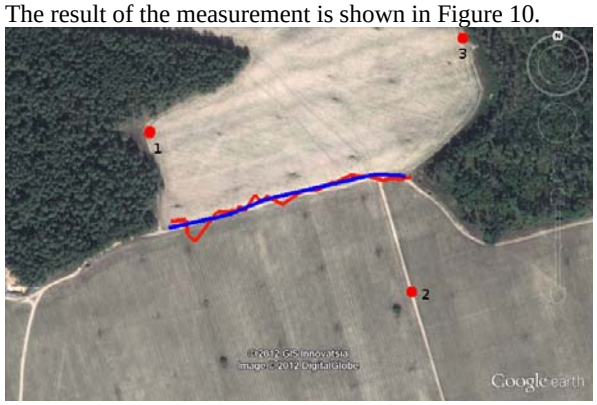

Figure 10. The result of jammer tracking.

Red dots represent the placement of the monitoring receivers. Red line shows the measured jammer track. Blue line shows the track recorded with the use of the GPS receiver without jamming. It can be seen that the red track is less accurate but nevertheless, it corresponds to the right one. The maximum positioning error didn't exceed 20 meters.

CONCLUSION

The study proved that TDOA approach can be used for jammer source location. A cross-correlation technique of the unknown signal reception was used. The computer simulation and experiment results showed that the distance of jamming signal detection is by order of magnitude more than the jamming radius. During the experiments the jamming signal was detected at the distance of 1 km.

The technique of monitoring receivers synchronization by GPS signals was demonstrated. This technique allowed to solve one of the most difficult problems using TDOA jamming location approach.

The track of the jammer movement was measured. The accuracy of jammer location demonstrated in this test satisfies practical purposes.

At the same time many questions remain open. The main one is the accuracy of jammer location system in urban environment. Our experience in the usual GNSS use shows that the urban environment causes a lot of problems due to signal reflections. Indirect signal propagation is the source of the major positioning error in urban environment. The jammer monitoring system is considered to have much fewer receivers in-view comparing to the satellites in-view of navigation

receivers. Thus this problem should affect this system even more.

Unfortunately it is not allowed to test the jammer location system in the urban area. However, due to the nature of its application, specific operation in urban condition is one of the most important issues. That's why we hope to find another way to verify and adapt this system for operation in urban environment.

ACKNOWLEDGMENTS

The authors would like to acknowledge professor Perov A.I. and other people from the Moscow Power Engineering Institute who took part in the preparation of this article.

REFERENCES

[1] GLONASS. Principles of design and operation / Ed. by Perov A.I., Kharisov V.N. - Moscow: Radiotechnika, 2010.

[2] Bauernfeind R, Kraus T., Dötterböck D., Eissfeller B., Löhnert E., Wittmann E., Car Jammers: Interference Analysis. – GPS world, October, 2011.

[3] Mitch R. H., Dougherty R. C., Psiaki M. L., Powell S. P., O'Hanlon B. W., Bhatti J. A., Humphreys T. E., Signal Characteristics of Civil GPS Jammers. – Proc. ION GNSS-2011, pp. 1907-1919.