International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.447-456
http://dx.doi.org/10.14257/ijsia.2016.10.8.39

Research on Anti-Spoofing and Detection Technology in Satellite Positioning Section

Liu You-ming[1], Feng Qi[1] and Li Ting-jun[1]

[1]*Department of Electronic and Information Engineering, Naval Aeronautical University, Yantai 264001, China*
15615659977@163.com

Abstract

The detector performance depends on the clock accuracy and the model, the clock parameters estimation error will lead to a decline in the performance of the detectors. Therefore, in order to reach the detector achieves a set of performance, it need to adjust the receiver of the crystal quality. In this paper, the method of detecting the clock states of the satellite navigation receiver is used to detect the receiver. The clock state model of the receiver is established in the static and motion mode, and the time variation of the clock state is analyzed.

Keywords: *Satellite; Receiver; Clock state; Deception technology; Detection*

1. Introduction

For the simple deception attack by the non synchronous GNSS signal simulator, the pseudo range measurement results are not synchronized with the real pseudo range observation. Therefore, the deception signal and real signal will show a very different correlation peak in the correlation function. In this case, in order to synchronize the receiver with the false signal, the power of the deception signal should be adjusted to make it more power than the real signal [1]. As the receiver in the tracking state is tracking the true signal correlation peak, unless the power adjustment to the level of the signal to the noise level, it can not be a serious threat to the non simultaneous deception attack. This type of receiver employs an omni-directional antenna to interfere with a receiver in the capture range of several kilometers. Based on the receiver of the source it can be implemented to implement the synchronous deception. The two major part of this type of deception by: GPS receiver and deception signal generator. In this case, the parameters of the current GPS constellation and real signal are extracted from the GPS receiver measurements, which are used to generate false signals to mislead the GPS receiver [2, 3].

2. Scenario Analysis

To successfully mislead the target receiver, the source must be able to synchronize the synthesis of several GNSS signals, and then the pseudo range observed by the deception source will get a false PVT results. Can be the target of the T receiver of the first I deception pseudo range observation results of the model is simplified to the following form:

$$\hat{PR}_i(t) = \underbrace{\hat{\rho}_i(t) + c\,d\hat{t}_i(t)}_{\text{PRN part I}} + \underbrace{c\,dT_i(t) + \rho_{ai}(t) - c\,dT_i(t)}_{\hat{c}(t):\text{Common part of all PRN}} + \hat{\eta}_i(t) \quad (1)$$

ISSN: 1738-9976 IJSIA

$\hat{\rho}_i(t)$ Is at time t of the satellites and spoofing of source between the pseudo range is time t I of the satellite clock error, $d\hat{t}_i(t)$ clock difference of users, $dT_u(t)$ for users transmit antenna to the receiver antenna distance, $\rho_{su}(t)$ is to compensate spoofing source object and $dT_s(t)$ the antenna receiver antenna transmission delay and signal transmission in a wish to join the time advanced quantity. This should be constant, or to follow a predefined clock model, which is to GNSS receiver and expected clock changes the characteristics of consistent (otherwise, cheating the pseudo range measurement results may be GNSS receiver refused). C is the propagation velocity of light in the atmosphere, $\hat{\eta}_i(t)$ is which indicates other error sources, such as environmental noise and multi-path.

The pseudo range measurement results from the first I real PRN stripping can be simplified as follows:

$$PR_i(t) = \underbrace{\rho_i(t) + c\,dt_i(t)}_{\text{PRN part I}} + \underbrace{c\,dT_u(t)}_{C(t):\text{Common part of all PRN}} + \eta_i(t) \tag{2}$$

$\rho_i(t)$ Is the user antenna and the distance of the I satellite, dt_i the satellite clock bias of the I, dT_u is the user's clock bias, said other error sources, such as environmental noise and multipath.

The synchronous deception attack is designed to mislead the receiver in the tracking state. First, the correlation peak of the deception signal is matched with the correlation peak of the real signal of the target receiver, and then the correlation peak of the false signal is gradually moved to snatch the tracking points of the receiver. The process is shown in Figure 1. It is assumed that the implementation of the deception of the attacker knows that its transmission antenna to the target receiver of the approximate distance, so that the source of the false correlation peak with the target receiver's true correlation peak matching.

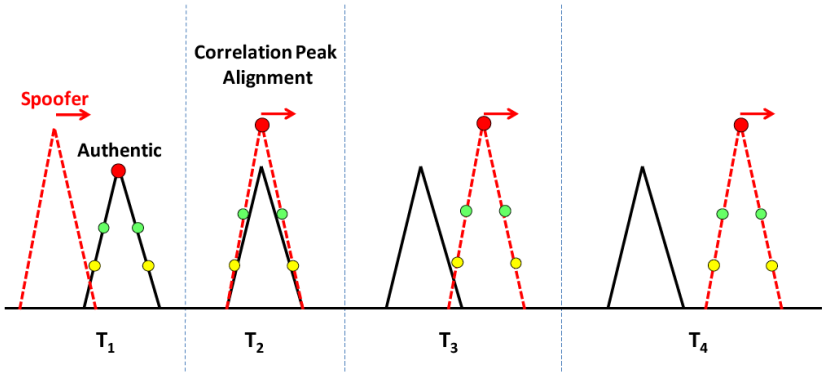

Figure 1. A Demonstration of the Implementation of the Attack Process based on the Receiver

In order to match the real signal and the correlation peak of the deception signal (1) and (2) the determination of the pseudo range observation is the same, t_I so that in the pull off time should meet the following:

$$\underbrace{\hat{\rho}_s(t_{su}) + c\,d\hat{t}_s(t_{su})}_{\text{PRN part I}} + \underbrace{c\,dT_s(t_{su}) + \rho_{su}(t_{su}) - c\,dT_s(t_{su})}_{\text{Common part of all PRN}} \tag{3}$$

$$= \underbrace{\rho_s(t_{su}) + c\,dt_s(t_{su})}_{\text{PRN part I}} + \underbrace{c\,dT_s(t_{su})}_{\text{Common part of all PRN}}$$

As shown in (3), each side of the equation is made up of two parts, one part of which is a specific PRN proprietary part and the other part which is the common part of all PRN. Effective deception should be able to synchronize these items at the same time, the same means that the PRN part of the same, the false distance measurement and the measurement of the true signal is equivalent to that of the false distance measurement. It is the same as that of the transmission antenna and the target receiver antenna transmission delay (otherwise, the correlation peak of the deception signal and real signal can not be matched). In partial success, cheat source can gradually change the item, making the receiver gradually deviate from the real results of PVT.

Based on receiver spoofing of source may use directional antenna to attack a contains receiver target specific space. At the same time, similar to the non synchronous spoofing attack, if this type of deception source meet the target receiver beam type and power coverage area, capable of acting in many of the trapped state of GNSS receiver (receiver on the outside of the target receiver, correlation peak can not match).

3. Detection Technology for Mobile Receiver

3.1. Deception Detection

The relative movement between the source and the target receiver can change the relative distance between the two. Short term clock changes of the GNSS receiver can be modeled as a linear function of time. The receiver motion can change all of the common parts of the PRN. Therefore, if the receiver and the PRN synchronization, when the receiver from the initial position to start, the receiver clock state will deviate from its expected model. This feature can be used to detect the PVT results generated by deception.

Discrete first order expansion of the state of the clock is shown below:

$$c\tau[n] = c\tau_{u,0} + c\dot{\tau}_{u,0}n + \eta[n] \tag{4}$$

Here $\tau_{u,0}$ and $\dot{\tau}_{u,0}$ represent receiver initial clock bias and clock drift rate $\eta[n]$ is additive Gaussian process at time n values, the spectral density is determined by the characteristics of the receiver oscillator. In order to avoid being found by the target receiver, the receiver needs to be characterized by the deception signal to imitate the true signal as far as possible, so that it is assumed that the cheat source follows the real signal of the clock state mode. In addition, if the fool does not know the target receiver, the receiver can not change the clock mode of the target receiver in the mobile state. We can detect the clock by monitoring the results of the mobile receiver PVT.

Which can define the detection problem as follows:

$$\begin{aligned} H_0 &: \quad x[n] = c\tau_{u,0} + c\dot{\tau}_{u,0}n + \eta[n] \\ H_1 &: \quad x[n] = \Delta\rho_{su}[n] + c\tau_{u,0} + c\dot{\tau}_{u,0}n + \eta[n] \end{aligned} \tag{5}$$

Among them, n=1,2,... N. H_0 The presence of a non deceptive H_1 signal indicates the presence of a cheat signal, and the N indicates the number of samples for hypothesis testing. Assuming that the amount of time that $c.dT_s(n)$ is intentionally added to the user is also followed by the user's local clock state change mode, then all short-term clock changes can be modeled as a first order polynomial. As a result, the only difference between H_0 and H_1 is that the distance between the source and the target receiver is varied $\Delta\rho_{su}[n]$: this amount is as follows:

$$\Delta\rho_{su}[n] = \rho_{su}[0] - \rho_{su}[n] = \left\|P_u[0] - P_s[0]\right\| - \left\|P_u[n] - P_s[n]\right\| \quad (6)$$

$P_{U,s}[n]$ Is the time n target receiver of the three-dimensional position, $\|\bullet\|$ the norm of the vector (see Figure 2). In the next sub sections, the assumption that the cheat source is static or the motion of the receiver can be ignored, thus $P_s[n] \approx P_s[0]$, n=1,2,... N.

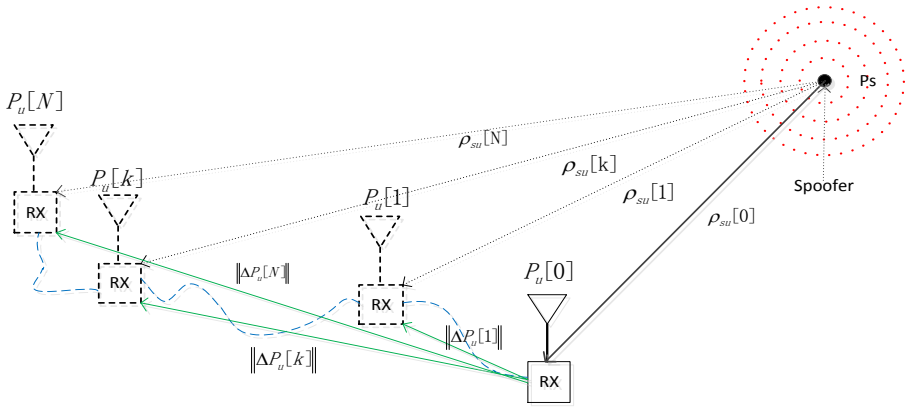

Figure 2. Schematic Diagram of the Deception Detection Scene known as the Motion State

3.2. Track Movement

In this case, we assume that the receiver motion trajectory ($P_u[n]$) is known, and the distance between the user and the user is much greater than the change in the user's position, so we can rewrite the equation (6) as follows:

$$\Delta\rho_{su}[n] = \underbrace{\left\|P_u[0] - P_u[n]\right\|}_{\left\|\Delta P_u[n]\right\|} \cos(\phi_u[n] - \phi_s)\cos(\theta_u[n] - \theta_s) \quad (7)$$

In which, $\varphi_u[n]$ said at the moment n users to move φ_s the azimuth angle, $\theta_u[n]$ which represents the azimuth angle of the source of the deception, n users at the time of moving the elevation, θ_s which indicates that the angle of deception. In this, the detection formula (5) can be written in the form of a classical linear model:

$$x = H\theta + w \qquad \begin{cases} H_0 : A\theta = b \\ H_1 : A\theta \neq b \end{cases} \quad (8)$$

Here the N is order design matrixN×6, the matrix elements$[H]_{n,p}$ can be listed as follows:

$$
\begin{aligned}
[\mathrm{H}]_{n,1} &= \left\|\Delta \mathrm{P}_u[n]\right\| \cos(\varphi_u[n]) \cos(\theta_u[n]) \\
[\mathrm{H}]_{n,2} &= \left\|\Delta \mathrm{P}_u[n]\right\| \cos(\varphi_u[n]) \sin(\theta_u[n]) \\
[\mathrm{H}]_{n,3} &= \left\|\Delta \mathrm{P}_u[n]\right\| \sin(\varphi_u[n]) \cos(\theta_u[n]) \\
[\mathrm{H}]_{n,4} &= \left\|\Delta \mathrm{P}_u[n]\right\| \sin(\varphi_u[n]) \sin(\theta_u[n]) \\
[\mathrm{H}]_{n,5} &= 1 \\
[\mathrm{H}]_{n,6} &= n
\end{aligned} \tag{9}
$$

The remaining parameters of the equation (8) are as follows:

$$
\theta = \begin{bmatrix} \cos(\phi_s)\cos(\theta_s) \\ \cos(\phi_s)\sin(\theta_s) \\ \sin(\phi_s)\cos(\theta_s) \\ \sin(\phi_s)\sin(\theta_s) \\ c.\tau_u \\ c.\pi_u \end{bmatrix}, b = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, w = \begin{bmatrix} \eta[1] \\ \eta[2] \\ \mathrm{M} \\ \eta[N] \end{bmatrix} \tag{10}
$$

$$
\mathrm{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} x = \begin{bmatrix} x[1] \\ x[2] \\ \mathrm{M} \\ x[N] \end{bmatrix}
$$

So if

$$
T(x) = \frac{(A\hat{\theta}_1 - b)^T [A(H^T H)^{-1} A^T]^{-1} (A\hat{\theta}_1 - b)}{\sigma^2} > \gamma \tag{11}
$$

GLRT detector will choose H_1, in which

$$
\hat{\theta}_1 = (\mathrm{H}^T \mathrm{H})^{-1} \mathrm{H}^T x \tag{12}
$$

$\hat{\theta}_1$ Under the assumption H_1 that the maximum θ likelihood estimate γ is the detection threshold, σ^2 the noise process vector variance (assuming σ^2 that the observation interval is constant), the detection performance of this detector is as follows:

$$
P_D = Q_{\chi_q'^2(\lambda)}(Q_{\chi_q^2}^{-1}(P_{FA})) \tag{13}
$$

P_D The probability of false alarm P_{FA} is the probability of false alarm, and $Q_{\chi_q'^2(\lambda)}(\bullet)$ the tail probability of the non central parameters of the non central tower $Q_{\chi_q^2}^{-1}(\bullet)$ is Q, which is the reciprocal of the tail probability of the central tower under the Q degree of freedom. Here, q=4, the number of the matrix A is 4, and the central parameter can be written in the form of a document [10]:

$$\lambda = \frac{(A\theta_1 - b)^T [A(H^T H)^{-1} A^T]^{-1} (A\theta_1 - b)}{\sigma^2} > \gamma \tag{14}$$

θ_1 Is the exact value of the argument.

3.3. Circle Movement

The scene considered is a receiver along a circular track with constant velocity motion, assuming that the angular velocity of the motion is known, whereas the initial angle of the receiver and the motion radius of the R are unknown. Figure 3 describes the motion scene.

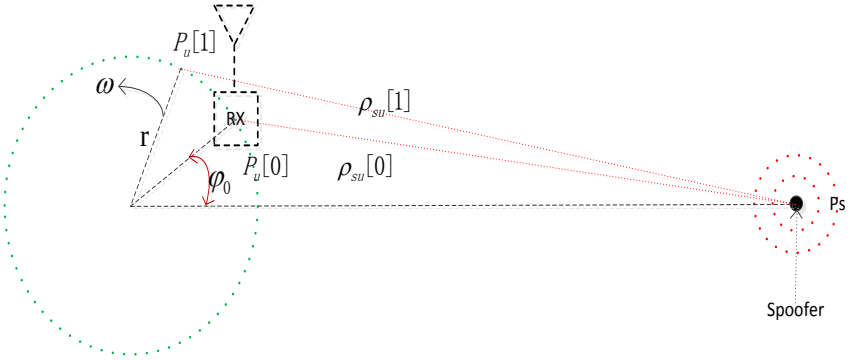

Figure 3. The Receiver is a Circular Motion Scene

Here, the equation (6) can be approximated by the following equation:

$$\Delta\rho_{su}[n] \approx r\cos(\Delta\theta_s)(\cos(\omega_0 n + \varphi_0) - \cos(\varphi_0)) \tag{15}$$

In the formula, this is a $\Delta\theta_s$ deception source relative to the motion plane of the elevation, X and W of the definition of the same type (10), after a certain mathematical simplification, type (8) described the detection mode can be rewritten as follows:

$$H = \begin{bmatrix} \cos(\omega_0) & \sin(\omega_0) & 1 & 1 \\ \cos(2\omega_0) & \sin(2\omega_0) & 1 & 2 \\ M & M & M & M \\ \cos(N\omega_0) & \sin(N\omega_0) & 1 & N \end{bmatrix}, b = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\theta = \begin{bmatrix} r\cos(\Delta\theta_s)\cos(\phi_0) \\ -r\cos(\Delta\theta_s)\sin(\phi_0) \\ c.\tau_u - r\cos(\Delta\theta_s)\cos(\phi_0) \\ c.\dot{\tau}_u \end{bmatrix}, A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \tag{16}$$

The performance characteristics of this scene detection can be described by (13), but here the q=2. In the case of unknown user angular velocity, the test results are estimated with different angular velocity. The detector should select the maximum of the estimate and compare this value with the detection threshold. Thus, the test can be expressed as follows in the literature [10]:

$$\max_{\omega_0} \{T(x;\omega_0)\} > \gamma' \tag{17}$$

The statistical value $T(x;\omega_0)$ of the detection test of the type (11) ω_0 is assumed to be known, γ' for the correction of the detection threshold, and $\max_{\omega_0}\{\cdot\}$ the operator takes the maximum value ω_0 of all different angular velocities. If the velocity of motion ω_0 is [0, π] and the value is not too close to the boundary of the interval. Thus, the assumption of frequency search using the M point fast Fu Liye transform technique, the detector (17) performance can be expressed in the [10]

$$P_D = Q_{\chi_2'^2(\lambda)}(2\ln(\frac{M/2-1}{P_{FA}})) \tag{18}$$

3.4. Random Movement

In this scenario, it is assumed that the receiver uses an unknown random motion pattern, and the detection problem can be expressed as follows:

$$x = H\theta + w\begin{cases} H_0 : w = [\eta[1], \eta[2], \cdots, \eta[N]]^T \\ H_1 : w = [\Delta\rho_{su}[1] + \eta[1], \cdots, \Delta\rho_{su}[N] + \eta[N]]^T \end{cases} \tag{19}$$

X is defined as (10), H and θ defined as follows:

$$H = \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ M & M \\ 1 & N \end{bmatrix}, \theta = \begin{bmatrix} c.\tau_u \\ c.\dot{\tau}_u \end{bmatrix} \tag{20}$$

Therefore, in the detection of the presence of deception signal, it is time to estimate the clock state parameters, it can use (12) to estimate the clock state parameters. Since there is no determined model to describe the motion of the receiver under this scenario, if the following conditions are met, the test will accept the assumption:

$$T(x) = \frac{1}{\sigma^2}(x - H\hat{\theta})^T(x - H\hat{\theta}) > \gamma \tag{21}$$

Here $T(x)$ is the test results, γ is the detection threshold, $T(x)$ H_1 in the assumption and the following tower square distribution, as follows:

$$T(x) \sim \begin{cases} \chi_N^2 & \text{under } H_0 \\ \chi_N'^2(\lambda) & \text{under } H_1 \end{cases} \tag{22}$$

Here χ_N^2 and $\chi_N'^2(\lambda)$ the center of the N degree of freedom and $\lambda = \sum_{n=0}^{N-1} \Delta\rho_{su}^2[n]/\sigma^2$ is the non central tower square distribution. The detection performance of the detector can be described by type (13), and the non central parameter is.

3.5. Linear Motion

In this scenario, the receiver is assumed to move along a linear track, the speed of which is V, and the direction is unknown, as shown in Figure 4:

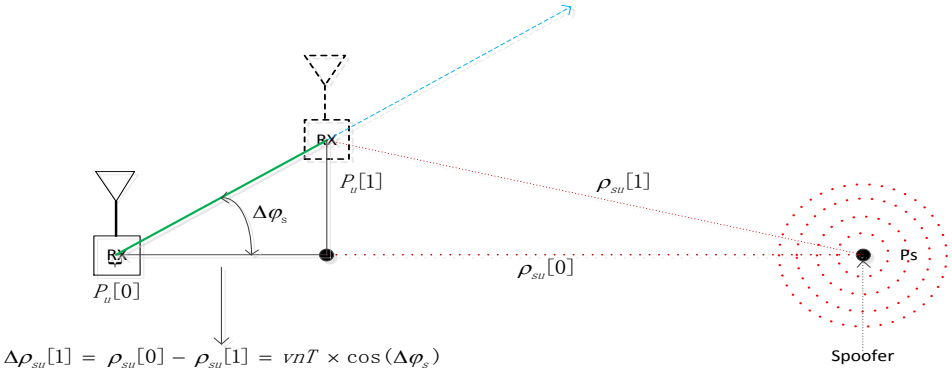

Figure 4. Linear Motion Pattern of the Unknown Direction

Assume that $\Delta\rho_{su} \ll \rho_{su}$ in n=1,2,... , N has, thus, the angle between the receiver motion direction and the incident wave of the deception signal can be guaranteed to be a roughly constant $\Delta\varphi_s$, in this

Equation (6) is as follows:

$$\Delta\rho_{su}[n] = \rho_{su}[0] - \rho_{su}[n] = vnT \times \cos(\Delta\varphi_s) \tag{23}$$

Here the T representation of the time interval is for the continuous sample of the clock state change. This scenario is applied to a moving vehicle along a linear track. For this type of user movement, the distance between the user and the user is the linear function of time. Therefore, it is independent of the user's clock bias. The latter is a linear function of time. Deception detection of this scene can be divided into two steps:

(1) learning phase:

This phase of the receiver is in a static state and the PVT results are calculated. The receiver can estimate the change rate of the clock difference ($\hat{\tau}_{u,0}$) and the difference of the clock ($\hat{\dot{\tau}}_{u,0}$), so as to predict the change of the clock state in the receiver. Here we assume that the receiver using a sufficiently stable crystal, the crystal of the short-term model is a linear function of time.

(2) mobile phase

At this stage, the receiver starts from the initial position, and the clock error of the receiver is constantly monitored, so as to carry out the detection of deception. Considering that the receiver is in a linear motion model, a GLRT detector with a classical linear model can still be applied to the scene to detect deception signals. Here, we define the parameters of the linear model as follows:

$$H = \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ M & M \\ 1 & N \end{bmatrix}, \theta = \begin{bmatrix} c.\tau_u \\ c.\dot{\tau}_u \end{bmatrix}, A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} c.\hat{\tau}_{u,0} \\ c.\hat{\dot{\tau}}_{u,0} \end{bmatrix} \tag{24}$$

The performance of the detector can be calculated using the equation (11), and the performance of the detector can be calculated using the equation (13).

3.6. Unknown Motion

In this scenario, no assumption is made on the receiver motion. Similar to the linear motion pattern, it takes two steps to cheat detection ". The difference between this scenario and the random walk model is that the former does not require the receiver to move at an initial position of 0. The test tests are chosen under the following formula:

$$T(x) = \frac{1}{\sigma^2}(x - \mathrm{H}b)^T(x - \mathrm{H}b) > \gamma \quad (25)$$

The performance of the detector depends on the accuracy of the clock and the model. The clock parameter estimates that even a bit error can result in a decrease in the performance of the detector. Therefore, the performance of the detector to reach the receiver, the crystal quality is very important.

4. Conclusion

In this paper, the method of detecting the clock states of the satellite navigation receiver is used to detect the receiver. The clock state model of the receiver is established in the static and motion mode, and the time variation of the clock state is analyzed. The performance of the detector depends on the accuracy of the clock and the model. The clock parameter estimates that a bit error can result in a decrease in the performance of the detector. Therefore, the performance of the detector to reach the receiver, the crystal quality is very important.

References

[1] Z. Lv, A. Halawani and S. Feng, "Multimodal hand and foot gesture interaction for handheld devices", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 11, no. 1s, **(2014)**, pp. 10.
[2] G. Liu, Y. Geng and K. Pahlavan, "Effects of calibration RFID tags on performance of inertial navigation in indoor environment", 2015 International Conference on Computing, Networking and Communications (ICNC), **(2015)** February.
[3] J. He, Y. Geng, Y. Wan, S. Li and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network", IEEE Sensor Journal, vol. 13, no. 10, **(2013)** October, pp. 3826-3836.
[4] W. Huang and Y. Geng, "Identification Method of Attack Path Based on Immune Intrusion Detection", Journal of Networks, vol. 9, no. 4, **(2014)** January, pp. 964-971.
[5] X. Li, Z. Lv and J. Hu, "XEarth: A 3D GIS Platform for managing massive city information", Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015 IEEE International Conference on IEEE, **(2015)**, pp. 1-6.
[6] J. He, Y. Geng, F. Liu and C. Xu, "CC-KF: Enhanced TOA Performance in Multipath and NLOS Indoor Extreme Environment", IEEE Sensor Journal, vol. 14, no. 11, **(2014)** November, pp. 3766-3774.
[7] N. Lu, C. Lu, Z. Yang and Y. Geng, "Modeling Framework for Mining Lifecycle Management", Journal of Networks, vol. 9, no. 3, **(2014)** January, pp. 719-725.
[8] J. He, Y. Geng and K. Pahlavan, "Toward Accurate Human Tracking: Modeling Time-of-Arrival for Wireless Wearable Sensors in Multipath Environment", IEEE Sensor Journal, vol. 14, no. 11, **(2014)** November, pp. 3996-4006.
[9] Z. Lv, A. Halawani and S. Fen, "Touch-less Interactive Augmented Reality Game on Vision Based Wearable Device", Personal and Ubiquitous Computing, vol. 19, no. 3, **(2015)**, pp. 551-567.
[10] G. Bao, L. Mi, Y. Geng, M. Zhou and K. Pahlavan, "A video-based speed estimation technique for localizing the wireless capsule endoscope inside gastrointestinal tract", 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), **(2014)** August.
[11] D. Zeng and Y. Geng, "Content distribution mechanism in mobile P2P network", Journal of Networks, vol. 9, no. 5, **(2014)** January, pp. 1229-1236.
[12] W. Gu, Z. Lv and M. Hao, "Change detection method for remote sensing images based on an improved Markov random field", Multimedia Tools and Applications, **(2015)**, pp. 1-16.
[13] D. Jiang, Z. Xu and Z. Lv, "A multicast delivery approach with minimum energy consumption for wireless multi-hop networks", Telecommunication Systems, **(2015)**, pp. 1-12.
[14] C. Fu, P. Zhang and J. Jiang, "A Bayesian approach for sleep and wake classification based on dynamic time warping method", Multimedia Tools and Applications, **(2015)**, pp. 1-20.

[15] Z. Lv, "Wearable smartphone: Wearable hybrid framework for hand and foot gesture interaction on smartphone", Computer Vision Workshops (ICCVW), 2013 IEEE International Conference on. IEEE, **(2013)**, pp. 436-443.
[16] Y. Lin, J. Yang and Z. Lv, "A Self-Assessment Stereo Capture Model Applicable to the Internet of Things", Sensors, vol. 15, no. 8, **(2015)**, pp. 20925-20944.

Author

Liu You-ming, enrolled in Naval Aeronautical University, in communications and information engineering research, participated in a number of major national projects and Natural Science Foundation research projects, scientific research on communication has a great interest has published many articles in communication.

