Detection of Power Increasing Jammers: Operational Considerations

Dario Benvenuti
R&D Department
Elettronica S.p.A.
Rome, Italy
dario.benvenuti@elt.it

Pia Addabbo
Università degli Studi
"Giustino Fortunato"
Benevento, Italy
p.addabbo@unifortunato.eu

Gaetano Giunta
Industrial, Electronic, and
Mechanical Engineering Department
Università degli Studi ROMA TRE
Rome, Italy
gaetano.giunta@uniroma3.it

Goffredo Foglia
R&D Department
Elettronica S.p.A.
Rome, Italy
goffredo.foglia@elt.it

Danilo Orlando
Dipartimento di Ingegneria dell'Informazione
Università di Pisa
Pisa, Italy
danilo.orlando@unipi.it

***Abstract*—In a recent paper, the authors proposed an optimum detection algorithm for noise like smart jammers that increase the transmitted power over the time. Remarkably, this kind of jammers can bypass conventional electronic counter-countermeasures, since classical methods are based on the detection of a noise power discontinuity in the observation window. On the other hand, the aforementioned detection algorithm can detect these smart jammers overcoming the conventional approach. While in the mentioned paper the theory of the detector has been presented, in this paper we further investigate the behavior of this detector, especially for what concerns operative application. Specifically, the detector is supposed to use a temporal sliding window and, once a "linear" jammer is detected the cancellation must be performed. In what follows, the conventional and the new detector are analyzed from an operating point of view.**

***Index Terms*—Detection, electronic countermeasures, electronic counter-countermeasures, generalized likelihood ratio test, jammer optimal detection, power increasing jammer, radar.**

I. Introduction

In recent years, multichannel systems are widely used in many application fields. The main advantage of these systems can be summarized as the opportunity of exploiting high number of degrees of freedom that can lead to an improved estimation and/or detection performance. This is due to the fact that multiple channels collect data from different perspectives (diversity) and, hence, the carried information is somehow more complete than single channel systems. It is clear that this superiority can be attained provided that suitable processing algorithms are used [1], [2]. Tangible examples are given by modern radar and new-generation communication systems such as 5G/6G, which create a strict synergy between sensing and communication functions [3]–[6]. As a matter of fact, modern radars are able to communicate and exploit 5G/6G communication infrastructures to offer more reliable services. This is made possible by the miniaturization of technologies and digital architectures.

However, these capabilities can also be used by malicious agents to perpetrate effective electronic countermeasures (ECM) such as smart jammers [7]–[9]. Electronic attack techniques can be classified into two main categories. The first category includes methods to mask the platform to be protected, while the second category includes techniques to create false targets that saturate radar resources or cause it to lose track of the target.

The first category of electronic attacks is known as noise-like jammer (NLJ) and uses unstructured signals that blend into the thermal noise of the radar receiver leading two main effects. The first effect occurs when the radar detection algorithms are not adaptive to the disturbance power, and generates a significant increase of false alarms. The second effect is related to the adaptive threshold that increases hence impairing the radar sensitivity. One of the widely used techniques against NLJ is the Side Lobe Canceler (SLC) [10] that places nulls in the antenna beam towards the NLJ direction.

The second category is called deception jamming and can also be used for self-protection, for example through techniques such as range-gate pull off or range-gate pull in, in which the jammer creates false targets to distract the radar from the real target. Well-known electronic counter-countermeasure (ECCM) techniques against deception are the Side Lobe Blanker (SLB) [10]–[12] and selective (possibly multi-stage) detectors [13]–[19, and references therein].

With the advent of digital architectures, the above ECCM techniques can be realized by means of digital beamforming. Moreover, to save computational resources, early detection stages are required to state that an attack is in progress before triggering ECCM. Focusing on ECCM against NLJs, conventional detection methods are usually based on an abrupt variation of the noise power observed in a dedicated channel [9, and references therein]. However, this approach might be ineffective when sophisticated NLJ techniques, known as "smart" techniques, are used. These NLJ techniques can control the transmitted power to maximize the effectiveness of the attack [20], [21]. Specifically, the NLJ can transmit power to slowly achieve radar receiver saturation, preventing its detection and the activation of effective counter-countermeasures. To cope with this kind of smart jammers, in [22] two architectures that differ in the NLJ power variation model have been proposed. The first architecture is obtained under a linear model for the power variation, whereas the second one is derived by neglecting any constraint on the transmitted power. It is evident that the first approach is more specific than the second one because it utilizes a priori information related to the variation rule. In [22], the performance analysis, conducted using synthetic data, is preliminary and is conducted in terms of probability of detection (P_d) against the "extent" of the power variation (see [22] for further details). In this paper, the performance of detectors proposed in [22] is assessed from an operating point of view. Specifically, the analysis considers the operating mode of such algorithms that, in a real system, work by processing data from a temporal sliding window. Thus, it becomes of primary importance the time at which the smart NLJ presence is declared. In fact, as soon as this information is available, suitable counter-countermeasures can be adopted in order to mitigate the deleterious effects of the NLJ action. For this reason, the analysis is aimed at quantifying what we define below as the "detection time" for each considered decision scheme. For comparison purposes, we also consider a conventional detector grounded on the assumption that a power discontinuity occurs in the data window under test.

In the next section, we briefly summarize the detection problem and the detection architectures (for the complete derivations see [22]), while in section III we present the new numerical results that investigate some important aspects not considered in [22]. In section IV, we draw some conclusions.

Notation: in the sequel, vectors and matrices are denoted by boldface lower-case and upper-case letters, respectively. Symbols $\det(\cdot), \mathrm{tr}(\cdot), (\cdot)^T$, and $(\cdot)^\dagger$ denote the determinant, trace, transpose, and conjugate transpose, respectively. $\mathbb{C}^{N\times M}$ is the Euclidean space of $(N \times M)-$dimensional complex matrices (or vectors if $M = 1$). I stands for the identity matrix vector or matrix of proper size. Finally, we write $\mathbf{x} \sim \mathcal{CN}_N(\boldsymbol{\mu}, \mathbf{M})$ if $\mathbf{x}$ is a complex circular $N-$dimensional normal vector with mean $\boldsymbol{\mu}$ and positive definite covariance matrix $\mathbf{M}$.

II. Smart Jamming Signal Models and Detection Architectures

The system at hand transmits and receives signals by means of N spatial channels. This system also uses an additional listening window where signal and clutter returns are negligible in order to estimate the thermal noise component and possible NLJ signals. Collected samples are organized into $N-$dimensional vectors denoted by $\mathbf{z}_k \in \mathbb{C}^{N\times 1}$ $k = 1, \ldots K$. The detection problem under consideration can be formulated as follows [22]

$$\begin{cases} H_0 : \boldsymbol{z}_k \sim \mathcal{CN}_N(\mathbf{0}, \sigma_n^2 \boldsymbol{I}), & k = 1, \ldots, K, \\ H_1 : \begin{cases} \boldsymbol{z}_k \sim \mathcal{CN}_N(\mathbf{0}, \sigma_n^2 \boldsymbol{I}), & k = 1, \ldots, K_1, \\ \boldsymbol{z}_k \sim \mathcal{CN}_N(\mathbf{0}, \sigma_n^2 \boldsymbol{I} + \boldsymbol{J}(k)), & k = K_1+1, \ldots, K, \end{cases} \end{cases} \tag{1}$$

where $\sigma_n^2 \mathbf{I}$ is the unknown thermal noise component with $\sigma_n^2 > 0$ the thermal noise power and $\boldsymbol{J}(k)$ is the NLJ contribution. Two cases are considered: the NLJ power is assumed to be linearly increasing, namely $\boldsymbol{J}_1(k) = \left[\gamma_0^2 + \gamma^2 (k + K_1)\right] \boldsymbol{v}\boldsymbol{v}^\dagger,\ k = K_1 + 1, \ldots,\ K$ where $\gamma_0^2 > 0$, $\gamma^2 > 0$, and $\boldsymbol{v} \in \mathbb{C}^{N\times 1}$ is the NLJ steering vector; the other case assumes that the NLJ power is unconstrained, i.e., $\boldsymbol{J}_2(k) = \gamma_k^2 \boldsymbol{v}\boldsymbol{v}^\dagger,\ k = K_1 + 1, \ldots,\ K$ where $\gamma_k^2 > 0,\ k = K_1 + 1, \ldots,\ K$.

Defining

$$\Gamma_1 = \left\{\gamma_0^2, \gamma^2\right\}, \Gamma_2 = \left\{\gamma_{K_1+1}^2, \ldots,\ \gamma_K^2, \boldsymbol{v}\right\},$$

the sets of unknown parameters for the two models, $\boldsymbol{Z} = [\boldsymbol{z}_1, \ldots, \boldsymbol{z}_K] \in \mathbb{C}^{N\times K}$, and $\boldsymbol{Z}_1 = [\boldsymbol{z}_1, \ldots,\ \boldsymbol{z}_{K_1}] \in \mathbb{C}^{N\times K_1}$, the PDF of $\boldsymbol{Z}$ under H_0 is

$$f_0(\boldsymbol{Z}; \sigma_n^2) = \frac{1}{\pi^{KN} (\sigma_n^2)^{KN}} \exp\left\{-\mathrm{tr}\left[\frac{1}{\sigma_n^2} \boldsymbol{Z}\boldsymbol{Z}^\dagger\right]\right\}, \tag{2}$$

while that under H_1 has the following expression

$$f_1(\boldsymbol{Z}; \sigma_n^2, \Gamma_i) = \frac{1}{\pi^{KN} (\sigma_n^2)^{K_1 N}} \exp\left\{-\mathrm{tr}\left[\frac{1}{\sigma_n^2} \boldsymbol{Z}_1\boldsymbol{Z}_1^\dagger\right]\right\} \times \prod_{k=K_1+1}^{K} \frac{\exp\left\{-\mathrm{tr}\left[\left(\sigma_n^2 \boldsymbol{I} + \boldsymbol{J}_i(k)\right)^{-1} \boldsymbol{z}_k\boldsymbol{z}_k^\dagger\right]\right\}}{\det\left(\sigma_n^2 \boldsymbol{I} + \boldsymbol{J}_i(k)\right)}, \tag{3}$$

$i = 1, 2$.

Finally, the detection architectures have the following general expression

$$\max_{\sigma_n^2} \max_{\Gamma_i} \mathcal{L}_{1,i}(\sigma_n^2, \Gamma_i; \boldsymbol{Z}) - \max_{\sigma_n^2} \mathcal{L}_0(\sigma_n^2; \boldsymbol{Z}) \underset{H_0}{\overset{H_1}{\gtrless}} \eta,\ i = 1, 2, \tag{4}$$

where $\mathcal{L}_0(\sigma_n^2; \boldsymbol{Z})$ and $\mathcal{L}_{1,i}(\sigma_n^2, \Gamma_i; \boldsymbol{Z})$, $i = 1, 2$, are the log-likelihood functions under H_0 and H_1, respectively. The maximization under H_0 is well known, whereas under H_1 suitable numerical optimizations are used [22]. For brevity, we refer the reader to [22] for the derivation details and the final expressions of the (quasi) compressed log-likelihoods. The decision scheme for $i = 1$ that forces a linear variation of the NLJ power is referred to in the following as linearly-constrained (LC) detector, while the solution corresponding to $i = 2$ is called unconstrained (UN) detector.

III. Operative Performance Analysis and Discussion

Unlike [22], where the preliminary analysis is conducted in terms of detection capabilities with respect to the NLJ strength, in this section the performance of LC and UN detectors is investigated from a different perspective that is complementary

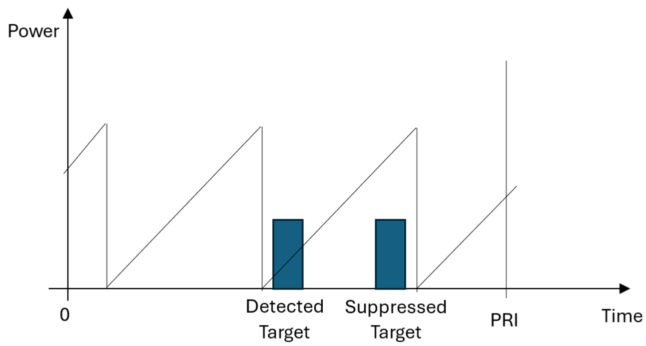

Fig. 1. Power Increasing Jammer Non Synchronized with Radar PRI

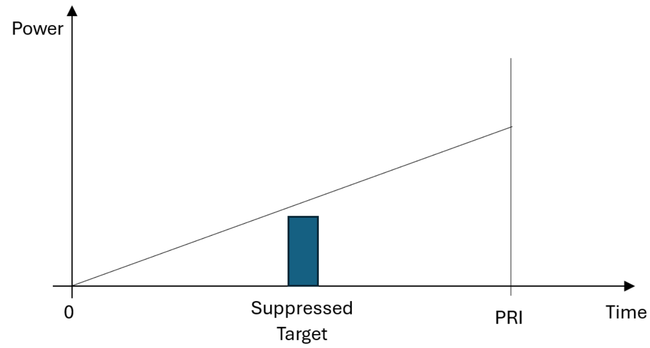

Fig. 2. Power Increasing Jammer Synchronized with Radar PRI

to that in [22]. More importantly, such an analysis would represent a guideline for the entire system design, since it provides an estimate of the responsiveness of such algorithms to the NLJ action and, hence, allows the system engineer to quantify the system latency when is under attack. The ensuing illustrative examples also include the so-called power jump (PJ) detector [22] as a competitor.

Before providing a quantitative analysis of the detection capabilities over the time, important remarks are in order. In real operations, the effectiveness of the considered kind of jammer is optimized if there exists a suitable synchronization between the jammer ramp and the radar time frame. Specifically, if the jammer does not have any side information related to the radar pulse repetition interval (PRI), the transmitted power can follow a sawtooth pattern that is asynchronous with the radar PRI as shown in Figure 1. In such a case, possible targets (under protection by the jammer) might fall in a low power region and, hence, they can be detected by the radar. On the other hand, when an electronic support measure system estimates the parameters of the radar that somehow drive the jammer action, the latter can be synchronized with the time frame of the victim radar. As a consequence, the jammer can start its transmission so that it is concurrent with the beginning of the radar PRI, also considering that there exist blind regions for the radar. In this situation, the jammer smoothly raises the power in order to mask the region of interest in each sweep as shown in Figure 2, where possible targets within the region of interest are always covered by the jamming signals.

The detection algorithms proposed in [22] process data from a temporal sliding window and once jammer action is detected, the cancellation by means of beamforming techniques [10], [23] is performed. Thus, the jammer can be effectively attenuated and the target echo is again visible (see Figure 3).

With the above remarks in mind, it is clear that, from an operating standpoint, the effectiveness of the considered detectors relies on the capability to discover the "jammer ramp" early or later within the PRI. The "detection time" can be defined as the instant at which the P_d becomes greater than a selected probability. In the following numerical examples,

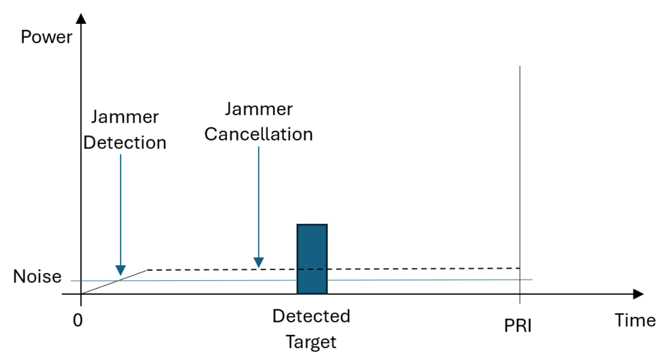

Fig. 3. Jammer detection and cancellation

we set the detection threshold corresponding to $P_{fa} = 10^{-3}$ and $P_d = 80\%$, the P_d curves are estimated through 1000 independent Monte Carlo trials. Moreover, the detectors are applied in scenarios where the jammer ramp has different slopes ($\gamma^2 = 0.01, 0.02, 0.05$) and use a window of length K that moves with a step equal to $K/2$. The reference time instant, t_k say, is given by the center of the sliding window. Thus, each t_k represents a window position and the corresponding P_d values are associated to t_k.

The results are shown in Figure 4, where the number of sensors is $N = 8$ and $K = 16$, as well as in Figure 5 where $N = 16$ and $K = 32$. The LC detector is able to discover the beginning of the jammer ramp at the initial time instants at least for the steepest slope ($\gamma^2 = 0.05$). Nevertheless, for the smoothest slope ($\gamma^2 = 0.01$), it is still capable of detecting the jammer within a short time. On the contrary the other detectors discover the jammer with a certain delay, especially the PJ detector, which is the conventional detector. This situation can lead to the detection of a false target or a region of low radar sensitivity. As a matter of fact, focusing on the case $\gamma^2 = 0.05$ of Figure 5, the conventional PJ architecture only detects the jammer when its power is about 13 dB over the noise. Finally, it is also important to highlight that this analysis emphasizes that the slope of the jammer ramp plays an important role in the detection performance and this aspect is not evident from numerical examples in [22].

IV. Conclusions

In this paper, we have assessed the performance of recent detection architectures for NLJs that cleverly control the transmitted power from an operating perspective. This analysis has revealed further important aspects related to the capabilities of countering this kind of jammers. Specifically, the emphasis has been on the "detection time" that provides an estimate of the system latency between the beginning of the jamming action and its mitigation. In fact, a smooth increase in the transmitted power can deceive conventional solutions based on the detection of a noise power discontinuity in the observation window. In a real scenario, these algorithms use a temporal sliding window and the time instant at which the first detection is declared becomes a significant key performance indicator. The results of this new analysis have proved that detection architectures proposed in [22] can declare the presence of a jammer in shorter time intervals than the conventional approach, whose delay can yield a decrease in sensitivity or a false alarm increase.

References

[1] Tsuban Chen, "The past, present, and future of image and multidimensional signal processing," *IEEE Signal Processing Magazine*, vol. 15, no. 2, pp. 21–58, 1998.

[2] M. Martorella, *Multidimensional Radar Imaging, Volume 1*, Electromagnetics and Radar. Institution of Engineering and Technology, 2019.

[3] M. A. Richards, J. A. Scheer, and W. A. Holm, *Principles of Modern Radar: Basic Principles*, Scitech Publishing, Raleigh, NC, 2010.

[4] W. Tong and P. Zhu, *6G: The Next Horizon: From Connected People and Things to Connected Intelligence*, Cambridge University Press, 2021.

[5] Dingzhu Wen, Yong Zhou, Xiaoyang Li, Yuanming Shi, Kaibin Huang, and Khaled B. Letaief, "A Survey on Integrated Sensing, Communication, and Computation," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024.

[6] "3GPP, Feasibility study on integrated sensing and communication," Tech. Rep. 22.837 version 19.4.0, 3rd Generation Partnership Project, June 2024.

[7] Pia Addabbo, Olivier Besson, Danilo Orlando, and Giuseppe Ricci, "Adaptive Detection of Coherent Radar Targets in the Presence of Noise Jamming," *IEEE Transactions on Signal Processing*, vol. 67, no. 24, pp. 6498–6510, 2019.

[8] D. Adamy, *EW101: A First Course in Electronic Warfare*, Artech House, Norwood, MA, 2001.

[9] D. Orlando, I. Palamà, S. Bartoletti, G. Bianchi, and N. Blefari Melazzi, "Design and Experimental Assessment of Detection Schemes for Air Interface Attacks in Adverse Scenarios," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1989–1993, 2021.

[10] A. Farina, *Antenna-Based Signal Processing Techniques for Radar Systems*, Artech House, Boston, MA, 1992.

[11] A. Farina, "Eccm techniques," in *Radar Handbook*, M. I. Skolnik, Ed., chapter 24. McGraw-Hill, 2008.

[12] A. Farina, L. Timmoneri, and R. Tosini, "Cascading SLB and SLC devices," *Signal Processing*, vol. 45, no. 2, pp. 261–266, 1995.

[13] F. Bandiera, D. Orlando, and G. Ricci, *Advanced Radar Detection Schemes Under Mismatched Signal Models*, Synthesis Lectures on Signal Processing No. 8, Morgan & Claypool Publishers, San Rafael, US, 2009.

[14] Linjie Yan, Pia Addabbo, Chengpeng Hao, Danilo Orlando, and Alfonso Farina, "New ECCM Techniques Against Noiselike and/or Coherent Interferers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 2, pp. 1172–1188, 2020.

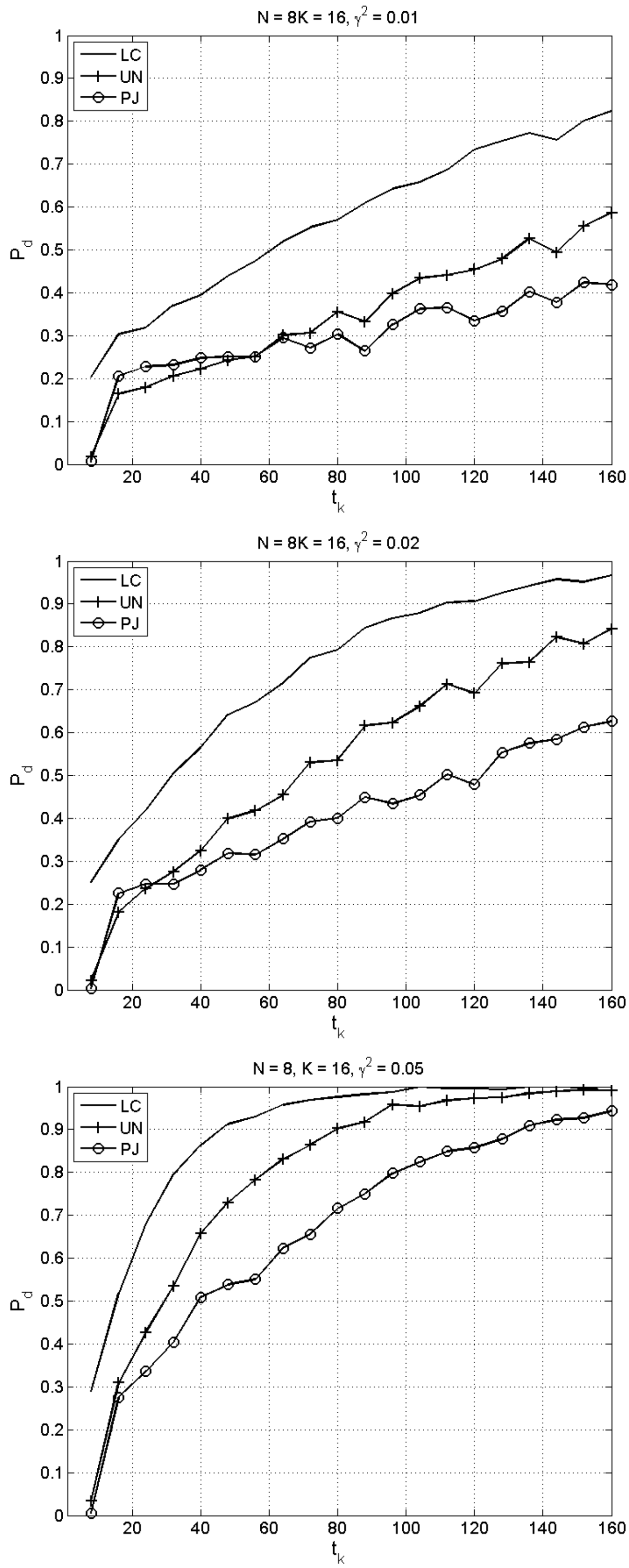

Fig. 4. Detection performance during time, $N = 8, K = 16$

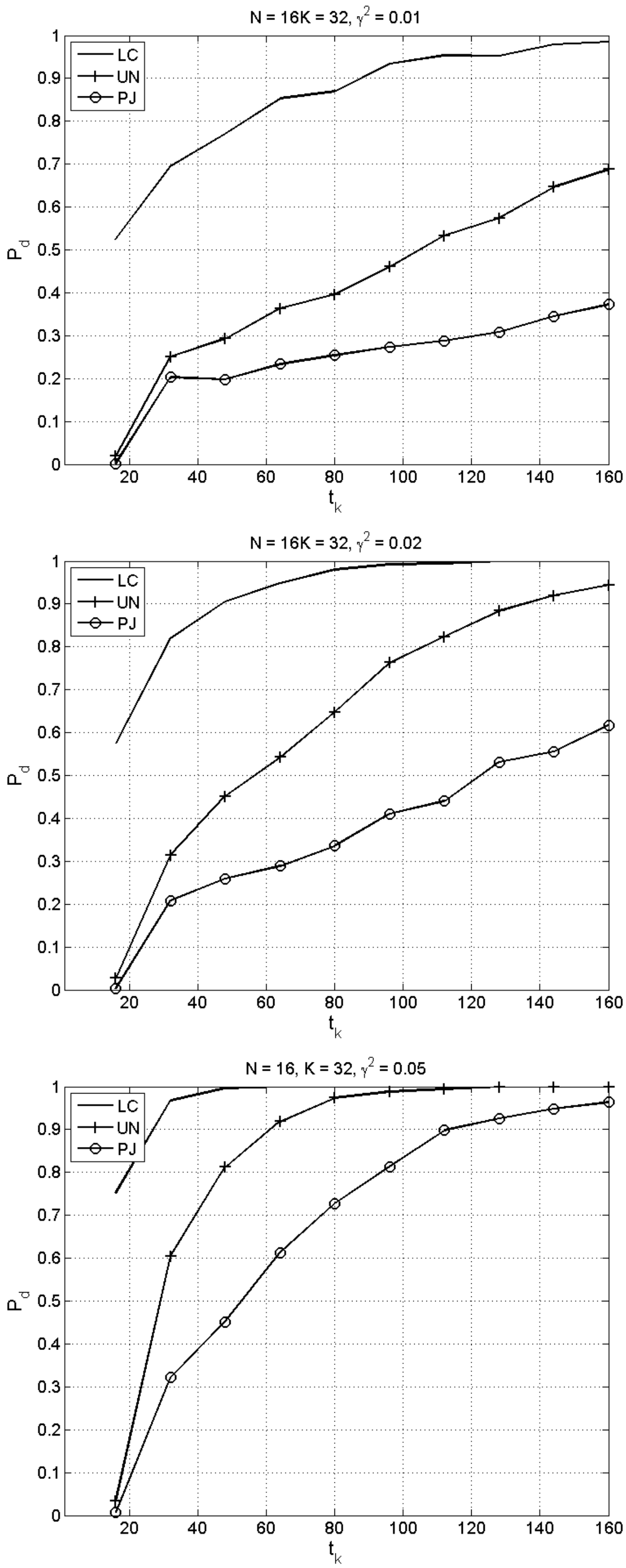

Fig. 5. Detection performance during time, $N = 16, K = 32$

[15] Linjie Yan, Pia Addabbo, Yuxuan Zhang, Chengpeng Hao, Jun Liu, Jian Li, and Danilo Orlando, "A Sparse Learning Approach to the Detection of Multiple Noise-Like Jammers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 6, pp. 4367–4383, 2020.

[16] Francesco Bandiera, Alfonso Farina, Danilo Orlando, and Giuseppe Ricci, "Detection Algorithms to Discriminate Between Radar Targets and ECM Signals," *IEEE Transactions on Signal Processing*, vol. 58, no. 12, pp. 5984–5993, 2010.

[17] Da Xu, Chengpeng Hao, and Chaohuan Hou, "A two-stage tunable detector with enhanced rejection capabilities," *The Journal of Engineering*, vol. 2021, no. 6, pp. 301–305, 2021.

[18] J. Liu, W. Liu, B. Chen, H. Liu, H. Li, and C. Hao, "Modified rao test for multichannel adaptive signal detection," *IEEE Transactions on Signal Processing*, vol. 64, no. 3, pp. 714–725, 2016.

[19] Yufeng Cui, Weijian Liu, Qinglei Du, Jun Liu, and Yong-Liang Wang, "A tunable detector for distributed targets when signal mismatch occurs," *Electronics Letters*, vol. 57, no. 15, pp. 594–596, 2021.

[20] Dejun Yang, Jin Zhang, Xi Fang, Andrea Richa, and Guoliang Xue, "Optimal transmission power control in the presence of a smart jammer," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 5506–5511.

[21] Yujie Zhang, Weibo Huo, Cui Zhang, Jifang Pei, Yin Zhang, and Yulin Huang, "Smart Noise Jamming Power Adjustment Using Exploratory Deep Deterministic Policy Gradient," in *2023 IEEE Radar Conference (RadarConf23)*, 2023, pp. 1–6.

[22] Dario Benvenuti, Pia Addabbo, Gaetano Giunta, Goffredo Foglia, and Danilo Orlando, "ECCM Strategies for Radar Systems Against Smart Noise-Like Jammers," *IEEE Transactions on Signal Processing*, vol. 72, pp. 3912–3926, 2024.

[23] W. L. Melvin and J. A. Scheer, *Principles of Modern Radar: Advanced Techniques*, Scitech Publishing, Edison, NJ, 2013.