JAMMING DETECTION BASED ON DOPPLER SHIFT ESTIMATION IN VEHICULAR COMMUNICATIONS SYSTEMS

Javad Afshar Jahanshahi

Universidad Católica Los Ángeles de Chimbote,
Instituto de Investigación, Chimbote, Perú

ABSTRACT

Since Doppler shift is one of the most important parameters in wireless propagation, the evaluation of the Doppler shift at the base station (BTS) in vehicular communications improves BTS in many aspects such as channel varying rate, jamming detection, and handover operations. Therefore, in this study, we propose a novel method at a base station based on the received user signal to estimate the channel Doppler shift seen by BTS. Utilizing the inherent information existed in common receivers, a level crossing rate (LCR) based Doppler shift estimation algorithm is developed without any excessive hardware. Moreover, a jamming detection algorithm is improved based on the proposed Doppler shift estimation scheme. The performance of the proposed scheme is evaluated in a Terrestrial Trunked Radio (TETRA) network, and comprehensive experimental results have shown superior performance in a wide range of velocities, signal to noise ratios and jammers.

KEYWORDS

Jamming Detection, Vehicular Communications, Level Crossing Rate, Mobile Communication, TETRA (Terrestrial Trunked Radio).

1. INTRODUCTION

In the vehicular communications, radio frequencies are interfered by inaccurate frequency planning, bandwidth allocation errors, or lack of ideal filters in transceivers. Unlike radio frequency interference, jamming signals are transmitted to occupy (i.e. destroy) the radio channels. They interfere with wireless communication channels by intentionally preventing the transmitter to access the right link, excluding the receiver from obtaining accurate information and/or disrupting the transmitted information over the wireless channel. Hence, they cause a lack of security in the communications network and degrade the quality of service experienced by the users [1].

To improve the performance of the wireless vehicular system, it is important to estimate the speed of a mobile terminal in wireless communication links. Knowing the speed of the mobile user enables the receiver to efficiently evaluate channel estimation. Similarly, in adaptive transmission, it helps the transmitter to adjust a suitable modulation/coding scheme according to the channel condition. Especially, speed information can also be used in anti-jamming techniques, when the receiver tries to differentiate between signal attenuations caused by jamming and channel effects [1-2]. Meanwhile, speed estimation by additional sensors like gyroscopes or accelerometers, and systems like GPS (Global Positioning System), increases the complexity and overall costs of user terminals, and furthermore, reduces the handset battery lifetime. Therefore, several techniques have been proposed in the literature for mobile terminal

DOI: 10.5121/ijcnc.2020.12502

speed estimation based on channel Doppler shift measurement, and some of them have been implemented in existing mobile communication systems. Covariance estimation schemes estimate Doppler frequency shift by computing covariance value between training received samples [3-12]. Other schemes for Doppler frequency shift estimation have used spectral analysis and variance [13-14], estimation of channel envelope and angle [15-16], statistical information of channel phase variations [17-18], Eigen based spectral estimation [19-20], spectrum estimation method based on channel power spectrum density [21-22], multi-vector test by using maximum likelihood approaches [23-24], wavelet analysis by tracking changes in the temporal scale [25-26] and channel auto-correlation [27-28]. In [29], the authors proposed an LCR based algorithm that estimates terminal's Doppler shift over each Doppler shift estimation window, and consequent windows do not overlap each other. They also used a single threshold for signal power comparisons. However, the proposed algorithm in [29] cannot follow the mobile terminal's variation in low SNR conditions. In this paper, the Doppler shift estimation algorithm is improved by utilizing a Doppler shift estimation window that slides over bursts with overlaps and by introducing two different low and high thresholds for power level comparisons. These thresholds are updated for each Doppler shift estimation window's movement in order to better track the Doppler shift variations even in low SNR conditions. This algorithm uses only inherent cellular system information, which means there is no need for any hardware modification of the user terminal, as well as cellular network signalling structure.

In order to reduce the implementation complexity, improve the performance and enhance the efficiency of the jamming detection algorithms proposed in the mentioned references, several improvements have been made. In the proposed algorithm, in addition to compromising and modifications in the Doppler shift estimation process, the modulation detection process is done only for the bursts which have been destroyed. Also, by using a new proposed Doppler shift estimation algorithm, the scaling factor value is estimated with higher accuracy. In addition, the high and low thresholds are set based on several experimental trials. Simulation results show that the proper value of these parameters has a considerable impact on algorithm performance. The proposed algorithm is modelled in a TETRA base station receiver.

The rest of this paper is organized as follows. In section 2, the latest related works are reviewed. Then we present the system model in detail in section 3. The proposed jamming detection algorithm is presented in section 4. In section 5, simulation results of the proposed algorithms, both shift Doppler estimation algorithm and jamming detection method, are reported. Finally, in section 6, we provide our concluding remarks.

2. RELATED WORKS

Utilizing different encoding, modulation, and decoding methods, one of the most important problems of current cellular systems (GSM, TETRA, CDMA, LTE, 5G, and 6G) is that they are not primarily designed to work in the jamming environments. Therefore, the best method for jamming detection in these systems is one that will have the most efficient detection performance, lowest cost and minimum complexity and maximum hardware and software compatibility with available hardware [30].In [31], a certain test signal is transmitted to any mobile users in the coverage area. Then the uplink is monitored to receive the response signal form end-users. In case the respond is not received, the interference in the channel is measured. If the interference level is higher than a threshold, the existence of jammer is announced. Their proposed algorithm is very complicated, and it causes an additional cost and is not beneficial to be used in common systems [32]. The proposed jamming detection algorithm presented in [33] measures channel power between the base station and mobile user to compare with a maximum noise power level. This algorithm also needs a modification in common hardware structures of BTS [34]. In [35], the proposed scheme firstly measures the synchronization peak and

synchronization average of each burst and secondly the synchronization average is weighted based on the channel status. If the weighted average is more than a predefined threshold, the received burst signal is modulated. Otherwise, it has been ignored. And all the received bursts are considered as a jammer signal. If the number of ignored is more than a high threshold, the jamming status is distinguished. In [18], the computational complexity of the proposed algorithm is very complicated mainly because of the modulation detection process [36]. Although the scaling factor, which is used by the algorithm, has a significant effect, but in [35] only a very simple method has been used to estimate it, due to its simplicity and complexity reduction. However, this method has a low performance level in poor channel conditions (such as low SNR and high Doppler shift). In the proposed method in [37] for jamming detection, the channel power between the base station and the mobile station is measured and compared with the maximum noise power level. If it is more than maximum noise power level, the temporary mobile subscriber identity, which is recognizable to the both base station and mobile station, is checked. If the temporary mobile subscriber identity is not understood, the number of jammed channel increases. In this algorithm, the hardware structure of the mobile station should change.

To distinguish anomaly traffic, an Entropy-based jamming detection system evaluates the different kinds of entropy of traffic descriptions obtained by randomly distributed data structures [38]. At first, Shannon-based entropy measurement and its variances utilized to a distinct boundary between normal and anomalous behaviour of data flows. The authors in [38] proposed parameterized entropy and supervised learning methods to improve the accurate detection of small or low attacks in IP networks. Authors in [39] presented that Shanon entropy-based approach has a limited descriptive capability and a proper tuning parameter needed. The authors in [40] proposed a novel jamming detection based entropy method that uses different measures of entropy to detect anomalous behaviours such as Shanon entropy, Tsallis entropy, Renyi entropy [41]. The above studies also show differences in measurement methods and approximate characteristics of entropy-based jamming detection methods. Based on the statistical method, the authors in [42] proposed a jamming detection algorithm that investigates the spatial and temporal correlations of data in wireless networks. However, this method leads to a larger amount of computations. To deal with resource constraints, fuzzy logic-based anomaly detection has been used to estimate feature traffic in the statistical model. In [43], fuzzy logic is used to identify if the anomaly is presented in a time interval. It delivers a threshold to observe forthcoming data traffic. The authors in [44] proposed a jamming detection method that uses fuzzy logic to create a single threshold over multiple metrics.

In fact, the main inspiration for our work is that the existing Doppler estimation based jamming detection schemes in the literature fail to meet the real-time monitoring and detection requirements for low complexity, accurate detection, and optimized speed. Therefore, an efficient method that can accurately detect jamming signals is essential for vehicular communications systems.

3. SYSTEM MODEL

In wireless telecommunication networks, the base station is a network element providing an air interface between radio units of mobile subscribers and the network infrastructure (referred to as Switching and Management Infrastructure). The base station is responsible for radio transmission and reception to and from wireless subscriber stations over the air interface. An example of a basic architecture of a base station receiver along with the jamming detection block is shown in Figure 1

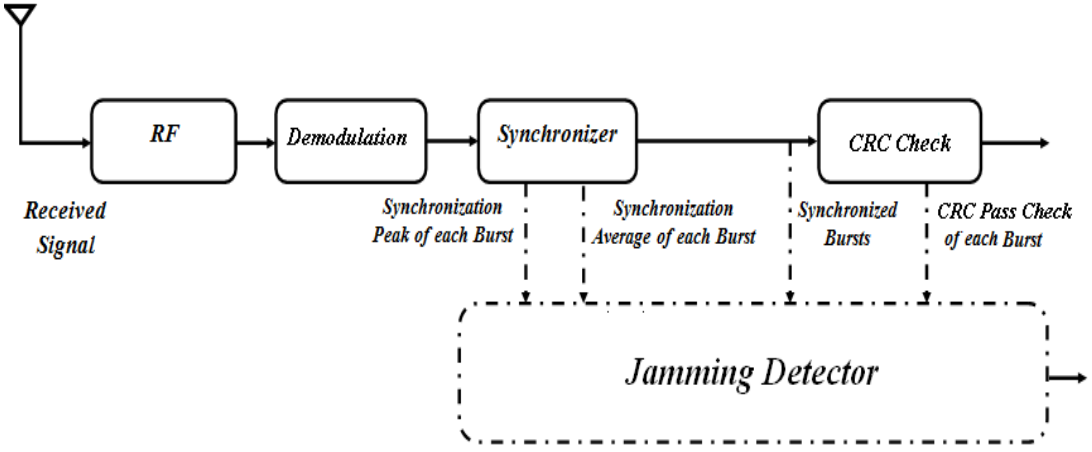

Figure 1 basic architecture of a base station receiver along with the jamming detection block

RF part amplify radio frequency (RF) signals received from an antenna, which provide selectivity and mix the received carrier to a lower intermediate frequency (IF). Then the received signals delivered to the baseband sections, such as the demodulation block, synchronization block, diversity combining and the Cyclic Redundancy Check (CRC) block. The diversity reception is optional, if it is employed, the baseband signals can be combined in the diversity-combined block. This improves the bit error rate considerably. In the present work, this block has not been employed.

In Time Division Multiple Access (TDMA) systems, the physical channel is a time slot. There can be a present number of time slots, i.e. physical channel, on the same carrier frequency. A burst is a period of an RF carrier which is modulated by a data stream. A burst thus presents the physical content of the timeslot or a subplot. The burst, i.e. the modulated data stream in the time slot, also contains a training sequence in the center of the time slot.

The received bursts after transmission to the baseband frequency are demodulated. Then they delivered to the synchronization block. In the synchronization block, in order to synchronize the received bursts in the synchronization block, a cross correlation function is calculated between the selected training sequence reference signal, which exists in the base station receiver, and training sequence samples of the incoming signal data. Then an average value $E(R_{RxTx})$ of the cross-correlation vector is calculated in order to define the average amplitude of the vector. Next, a peak value $P(R_{RxTx})$ is searched from the correlation vector, the peak is assumed to be in the center of the training sequence. Then, the synchronized bursts are delivered to the CRC block. The CRC check is a method for detecting errors in the transmission of data by using a polynomial code and cyclic check character. In the CRC block, cyclic redundancies of the bursts are analyzed. If the burst has been extremely damaged by the external factors (such as channel Doppler shift, environmental noise, or the jamming signals) and is not recyclable, the CRC pass flag is considered to be zero. Otherwise, it set to 1.

As is observed in Figure1, the synchronized bursts are delivered to the CRC block and the jamming detection block as well. As we will see in the following sections, the jamming detection block includes Doppler shift estimation block and modulation block. The Doppler shift estimation is performed by the synchronized burst. The average and the peak values of each burst are used to make decision in the modulation detection block.

4. THE PROPOSED JAMMING DETECTION ALGORITHM

The proposed algorithm uses three parameters of each burst along with the synchronized bursts. These three parameters are as follows: the average synchronization, the peak synchronization, and the CRC flag. The incoming parameters to the jamming detection block have been shown in Figure2.

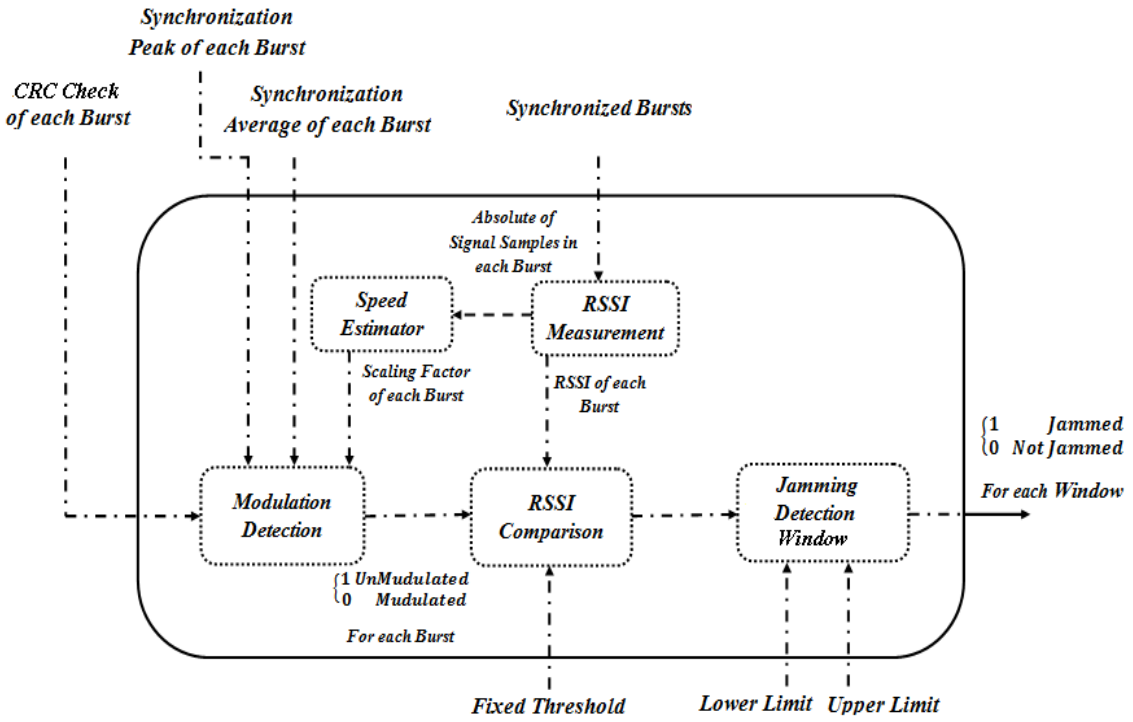

Figure 2 the jamming detection block

At first, power amplitude of the incoming synchronized bursts is measured. Then, the power amplitude of each burst is used in both Doppler shift estimation and Received Signal Strength Indicator (RSSI) comparison processes. In the Doppler shift estimation process, the Doppler shift that bursts experienced through the channel is estimated. Then, based on the estimated Doppler shift, the value of the scaling factor is identified. In the next section, we will describe how to identify this factor.

The jamming detection block also includes modulation detection that is used for detecting whether or not the synchronized bursts are modulated according to the modulation method used in the specific radio system. In order to reduce the computational complexity, only the modulation detection's accuracy of the damaged bursts will be examined. The estimated Doppler shift, the average, and the peak values of each burst are used to make decisions in the modulation detection block. The status bits 0 and 1 represents a modulated burst and an un-modulated burst, respectively, in the received burst flow.

Then, the jamming detection also checks the RSSI level of each burst, in order to ensure a sufficient quality for the signal. If the power of the received burst is too low (below a certain predetermined limit like fixed threshold), the last burst is considered to be a modulated burst regardless of the decision of the modulation detection. This feature prevents unnecessary alarms if the channel is not good enough to ensure a sufficient signal quality for the modulation

detection. However, the jamming detection algorithm is never capable to detect a jamming signal with extremely low power. This is not a serious problem, since a low power level jamming signal would not usually affect the performance of a receiver. In a certain signal to noise ration level, the number of un-modulated bursts in the time window may oscillate at the critical level of the threshold value. This causes the jamming detection to switch between the ON and OFF states. In order to keep from happening unexpected alarms, a transition interval is employed. The transition interval sets two limits, an upper and a lower one. Figure 3 shows the flowchart of the proposed jamming detection algorithm.

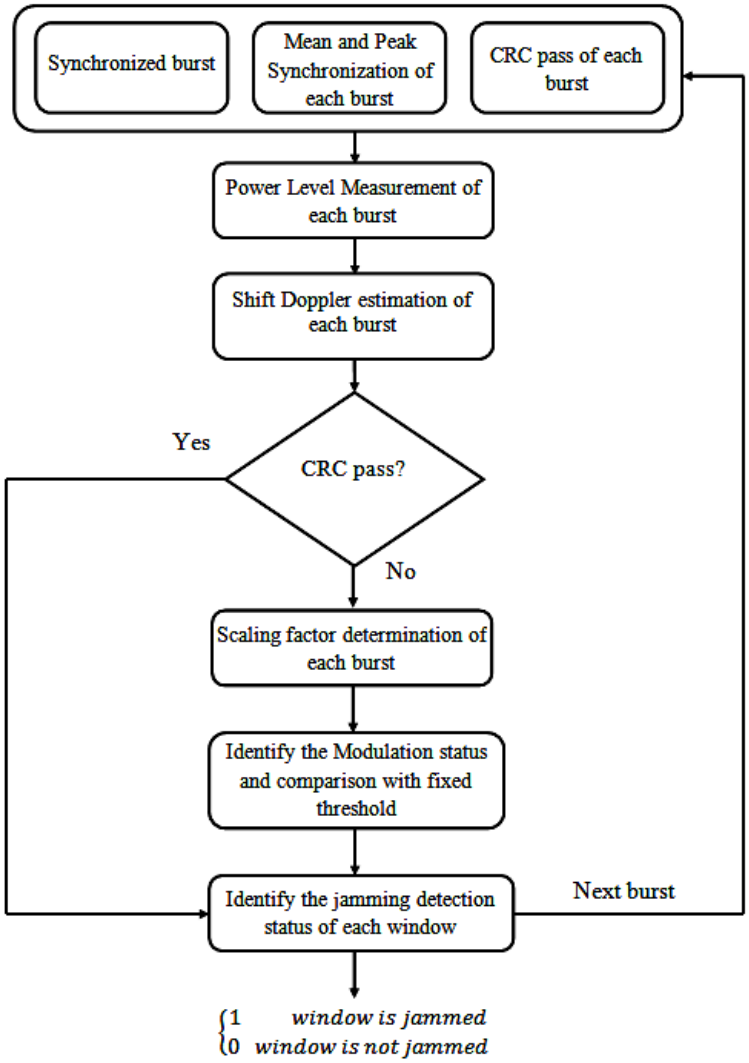

Figure 3 flowchart of the proposed jamming detection algorithm

4.1. The Modulation Detection Block

The base station receiver includes modulation detection that is used for detecting whether or not the received burst is modulated, according to the modulation method used in the specific radio system. The decision in the modulation detection is carried out by comparing the weighted synchronization average value with the synchronization peak value, which is calculated in the synchronization block, earlier. The modulation detection equation is given by [35-36]:

$$T = P(R_{RxTx}) - \zeta \times E(R_{RxTx}) \quad (1)$$

Where $P(R_{RxTx})$ denotes the synchronization peak and $E(R_{RxTx})$ denotes the synchronization average which are provided by calculating the cross-correlation function between training sequence samples of the incoming signal data (Tx) and the selected training sequence reference signal (Rx), which exists in the base station receiver. Z represents the scaling factor which depends on the channel Doppler shift. If the value of T is higher than or equal to zero, the burst is considered to be modulated and the modulation status bit is set to 1. Otherwise, the burst is unmodulated and the modulation status is set to 0.

$$\begin{cases} T \geq 0 & \text{Modulated} \\ T < 0 & \text{Unmodulated} \end{cases} \quad (2)$$

Then, the power level of the unmodulated burst is compared with a certain predetermined limit (fixed threshold). If it is lower than the fixed threshold, regardless of the decision of the modulation detection, the burst considered to be modulated. This means that the jamming detection algorithm recognizes only the jammer with the power more than the fixed threshold. The modulation detection algorithm is shown in Figure 4.

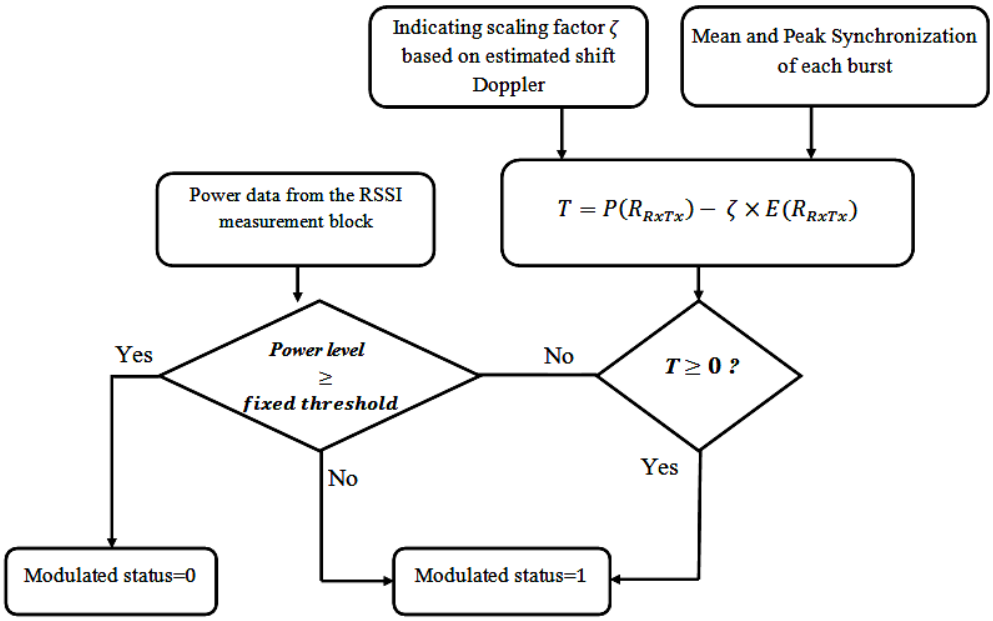

Figure 4 the modulation detection algorithm

4.2. The Proposed Channel Doppler Shift Algorithm

Figure 5 shows the structure of the received complex samples over one Doppler shift estimation window (i.e. 0.5 or 1 second). This window slides over samples of the received signal. Each window divided into N groups of samples:

$$N = [\frac{WL}{M}] \quad (3)$$

where [.] is the rounding down operator, WL is the number of samples within a Doppler shift estimation window and *M* is the segmentation factor. The segmentation factor will be updated for each received burst.

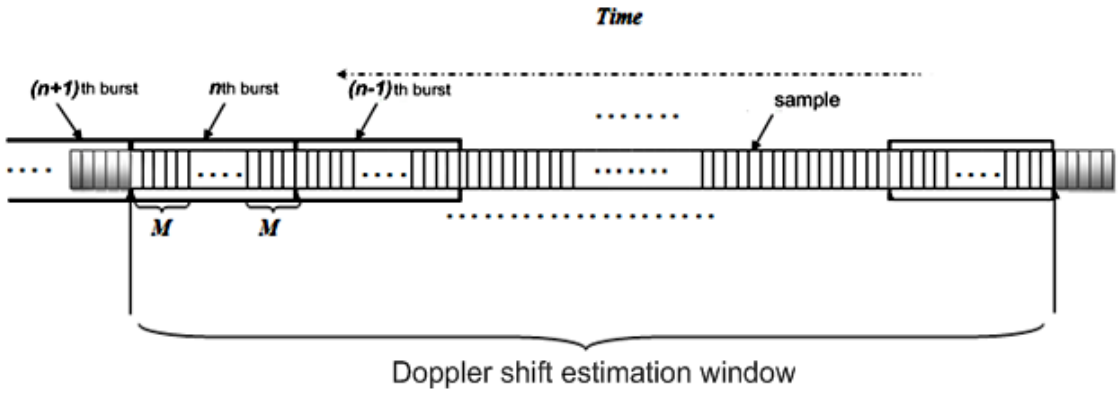

Figure 5 structure of Doppler shift estimation window.

The flowchart of the proposed Doppler shift estimation algorithm is illustrated in Figure 6. At the first stage, the power of the received signal is calculated. This power is measured within a fixed size Doppler shift estimation window. Then, the power meter computes group powers

$$S_D(i), \quad i = \{1, 2, 3, ..., \frac{WL}{M}\}$$

$$S_D(i) = \frac{1}{M(n)} . \sum_{z=(i-1)*M+1}^{i*M} |s(z)|^2 \tag{4}$$

where $S_D(i)$ is the power of samples over the i^{th} group**.** In the third stage, *RMS* meter computes the root mean square of group powers during Doppler shift estimation window as:

$$RMS = \sqrt{\frac{1}{\frac{WL}{M}} . \sum_{i=1}^{\frac{WL}{M}} |S_D(i)|^2} \tag{5}$$

The calculated *RMS* is then used to determine low and high thresholds for level crossing calculations. Then, high and low level crossing thresholds T_H and T_L are calculated. These thresholds should be fractions of the *RMS* value calculated in previous stage:

$$\begin{aligned} T_H &= y.RMS \\ T_L &= x.RMS \\ \forall \quad & o < x < y < 1 \end{aligned} \tag{6}$$

In the fourth stage, level crossing counter counts level crossing frequency L_R, which indicates how many times group powers $S_D(i)$ cross thresholds T_H and T_L in positive slope.

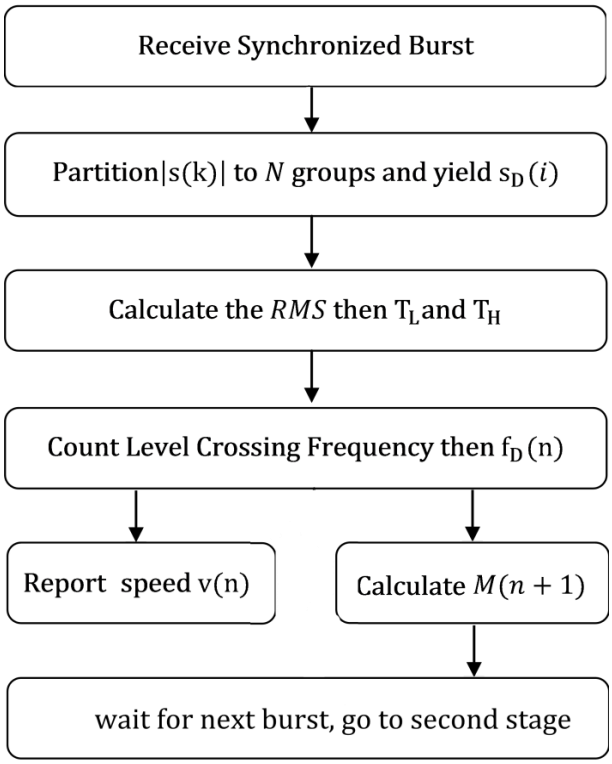

Figure 6 Signal Flow of the Proposed Algorithm.

In Rayleigh fading channel with 2-dimensional isotropic scattering, the Doppler shift is given by [45-46]:

$$f_D = \frac{L_R e^{\rho^2}}{\rho.\sqrt{2\pi}}$$
$$\rho = \frac{T_H + T_L}{RMS} \quad (7)$$

where f_D denotes the Doppler shift, and e is Euler's number. The Doppler shift of each received burst is given by its angle of arrival θ_n, the carrier frequency f_c, the propagation speed C (which is the speed of light), and the mobile terminal speed v. It can be calculated as:

$$f_D = v.\frac{f_c}{C}.\cos(\theta_n) \quad (8)$$

For the maximum value of the Doppler shift, the mobile terminal speed is given by

$$v = f_{D_{\max}}.\frac{C}{f_c} \quad (9)$$

For example, when signaling is done with $f_c = 396MHz$ in a typical value for a TETRA system, 100 km/h terminal speed results in maximum Doppler shift of $f_{D_{\max}} = 37Hz$. The estimated

speed is reported in the fifth stage. In the last stage, segmentation factor for the next incoming burst is updated as:

$$M = [\frac{f_s}{external\ factor * f_{D_{\max}}}] \tag{10}$$

where[.] is again a rounding down operator, f_s is sampling frequency, $f_{D_{\max}}$ is maximum Doppler frequency and "external factor" which depends on the channel type. In rapidly changing channels, since the amplitude of the signal varies more rapidly during a burst, the limits of external factor cannot be set as high as what it is in static channels. A rapidly changing channel may appear in some situations, i.e. where the speed of the user terminal is high. The algorithm interrupts until it receives new bursts. Algorithm started again (go to stage two) by using this new value of M when a new burst arrives.

4.3. How to Calculate the Scaling Factor

By increasing user's speed, channel Doppler shift and thus the channel power change rapidly. Since it increases the value of the synchronization average, $E(R_{RxTx})$, this makes the decision of the modulation detection uncertain. By decreasing the amount of the scaling factor, the performance of the modulation detection is improved. In other words, the sensitivity of modulation detection is reduced, which means that the tendency to classify bursts as unmodulated in difficult channel conditions is decreased. On the other hand, in static channels (channels that have low power changes), the scaling factor should be increased such that the modulation detection is more sensitive and it has a higher tendency to neglect bursts.

The scaling factor ζ is set based on the channel conditions and the amount of the channel Doppler shift expresses the status of the channel. Therefore, the scaling factor should be set so that in a certain Doppler shift and for all possible signals to jamming ratios (SJRs) has the best performance. To obtain the relation between the scaling factor and the amount of the channel Doppler shift, a realistic physical layer simulator of TETRA system including transmitter, channel, and receiver has been used. First, it is necessary that the Doppler shift's effect is determined, without considering the effect of the environmental noise on the received data at the receiver (e.g. a high signal to noise ratio: SNR = 30dB). For this purpose, the mobile station transmitted data have been passed through a Rayleigh fading channel with different Doppler shifts. The percentage of extremely damaged bursts versus SJR in different channel Doppler shift values has been shown in Figure 7. The horizontal axis includes SJR values from 0 to 15 dB and the vertical axis shows the percentage of the damaged bursts which are not recyclable by the CRC block (total number of bursts have considered to be 1000). The jammer signal has been considered a fixed amplitude sinusoid wave with 1 kHz frequency and has been applied to all the transmitted bursts over the channel

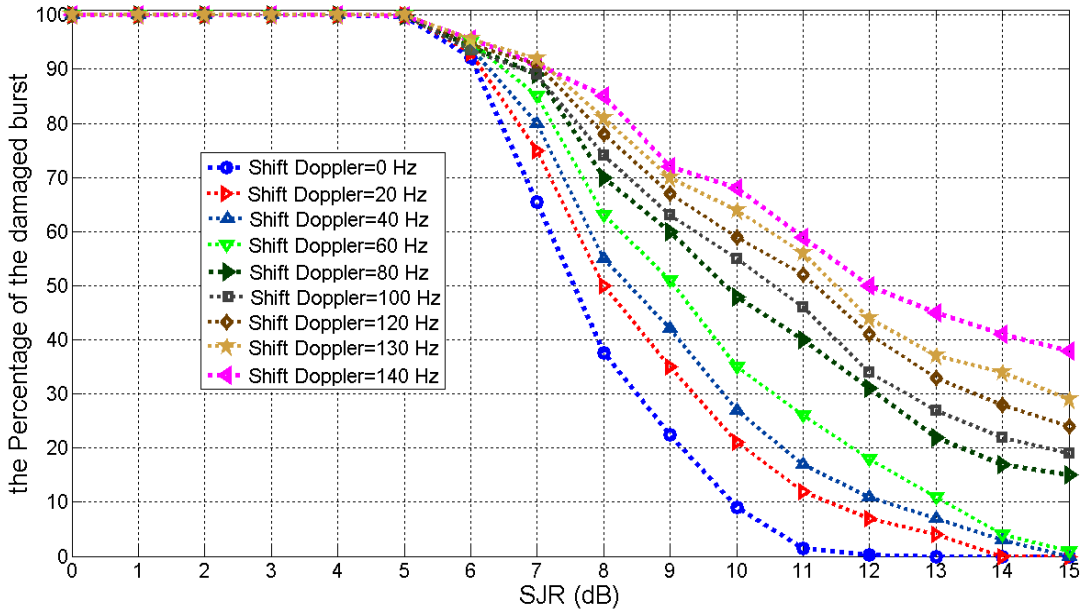

Figure 7 the percentage of the damaged bursts which are not recyclable

As can be inferred from Figure 7, by increasing the Doppler shifts in a certain SJR, the percentage of the damaged bursts increases as well. Consider a high value of SJR (e.g. SJR=15), where the jammer obviously does not affect the received data, considerably. It can be seen that by increasing the channel Doppler shift, the percentage of the unrecyclable bursts increases. Therefore, the scaling factor should be adjusted so that the jammer detection algorithm distinguishes between such damages and the damages caused by Jammer and do not consider these damaged bursts to be the jammed bursts. In order to obtain the scaling factor ζ range based on the different Doppler shifts, decision criteria, δ, is defined as follows.

$$\delta = \sum_{i=1}^{N} |CRC.Pass(i) - Mod.Flag(i)| \qquad (11)$$

Where $|.|$ is absolute value, $\mathrm{Mod.Flag}(i)$ is the modulation status of ith burst, $\mathrm{CRC.Pass}(i)$ is the CRC status of the i^{th} burst and N is the total number of the transmitted bursts. If the modulation status of the i^{th} burst is 0, then the burst considered to be modulated. Otherwise, the modulation status is set to 1 and it considered to beunmodulated. If the received burst is retrieved correctly, the status bit of the $\mathrm{CRC.Pass}(i)$ is 0 and when it is recycled incorrectly, the $\mathrm{CRC.Pass}(i)$ is set to 1. Theδ changes versus a range of the scaling factor ζ values for a given channel Doppler shift (e.g. $140Hz$) and for different values of SJR is shown in Figure 8. In order to focus on the jammer, these results are driven with the assumption of negligible environmental noise (e.g. SNR=15).

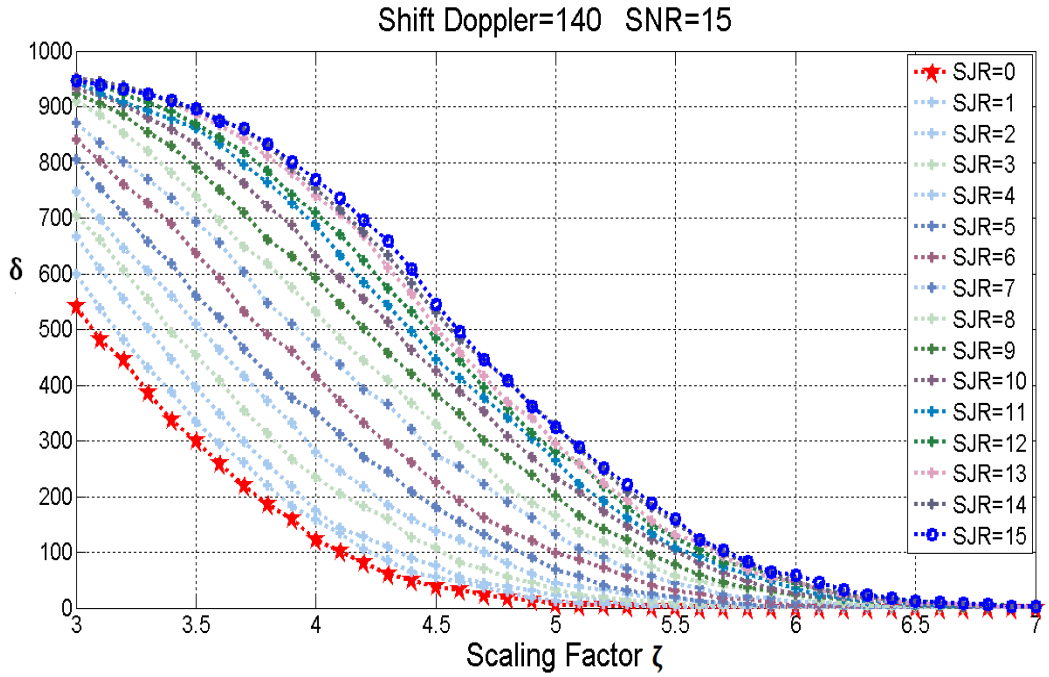

Figure 8 theδchanges versus a range of the scaling factor ζ in Doppler shift $140Hz$

By looking at the definition of δ, we can find that in ideal situation, δ should have its minimum value at low SJRs (here, $SJR_{min} = 0$) and its maximum value at high SJRs (here, $SJR_{max} = 15$) Therefore, the best scaling factor, ζ_{opt}, should be chosen so that the value of δ in the SJR_{min} has the highest difference with the value of δ in SJR_{max}.:

$$\zeta_{opt} = \text{argmax}_{\zeta}\left(\delta_{SJR_{max}} - \delta_{SJR_{min}} \right) \quad (12)$$

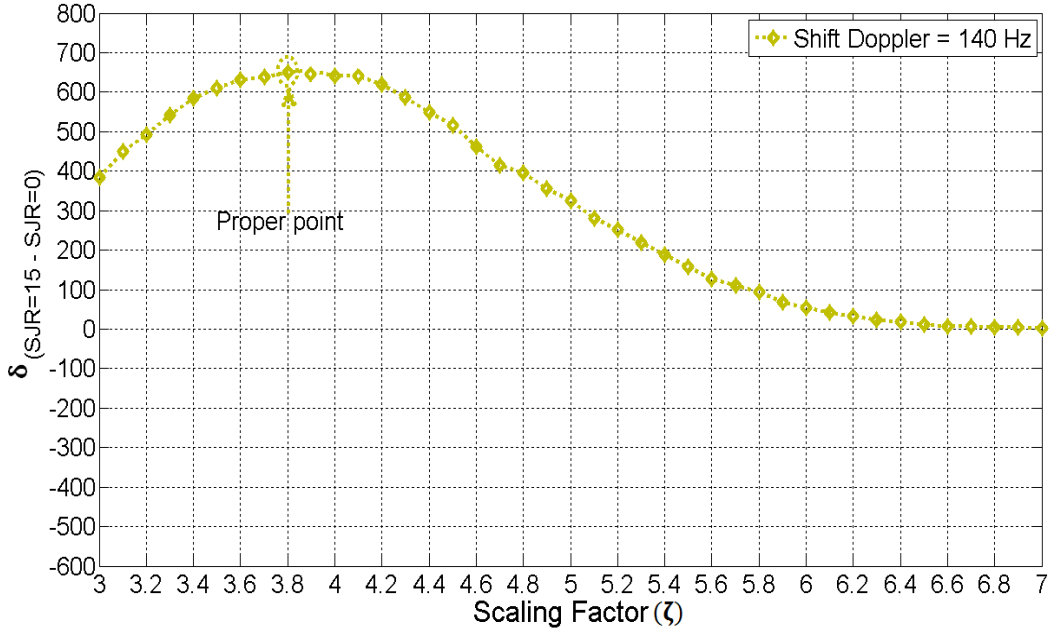

Figure 9 variation of $\left(\delta_{SJR=15} - \delta_{SJR=0} \right)$ versus the range of the scaling factor ζ in Doppler shift $140Hz$.

In Figure 9 variation of the equation (12) versus the range of the scaling factor ζ in the channel Doppler shift of $140Hz$ is shown. The optimum value of the scaling factor for other Doppler shifts say 30 -120 Hz, has been deduced in a similar way and shown in Figure 10.

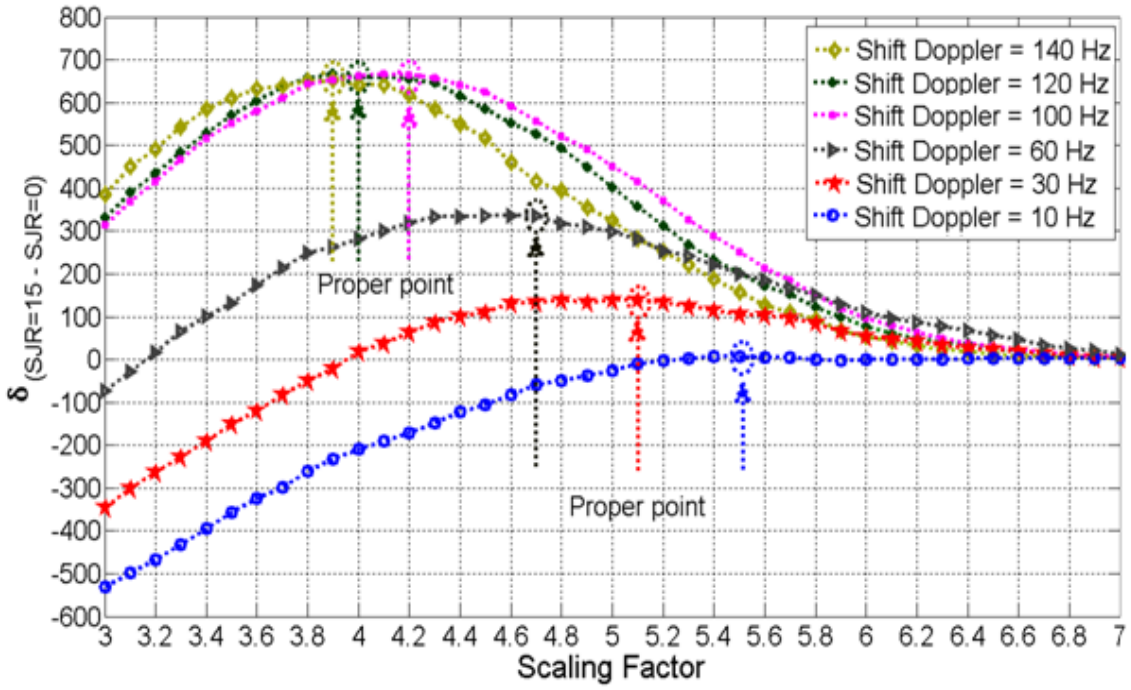

Figure 10 variation of $\left(\delta_{SJR=15} - \delta_{SJR=0}\right)$ versus the range of the scaling factor ζ

4.4. The Jamming Detection window Block

Having determined the modulation status of each received burst by using the concluded scaling factor from the estimated Doppler shift, the synchronization average, and the synchronization peak of each burst, the unmodulated burst's power is compared with the fixed threshold in order to ensure sufficient power for the received burst. Then, the modulation status is changed if the power of the received burst is below the fixed threshold. Afterward, the jamming detection algorithm counts the number of the unmodulated burst within a fixed time window which is called 'jamming detection window'. The jamming detection window slides over the received burst status bits of the modulation detection block. The moving step of the jamming detection window is only one burst and its time is fixed and its length depends on the required accuracy of the system. The jamming detection window is shown in Figure 11.

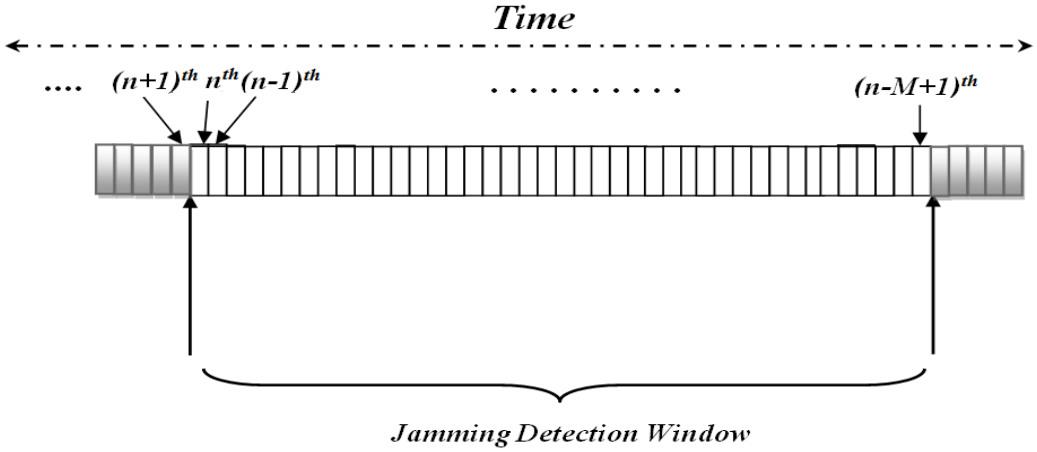

Figure 11 the jamming detection window

The purpose of applying the jamming detection window is to decrease the harmful effects of environmental noise as much as possible. In jamming detection window, the number of unmodulated bursts is counted. In order to avoid an uncertain jamming detection decision in the jamming detection window, especially in low SNRs, a transition interval set as up and a low threshold (which are called $UpTH$ and $DownTH$, respectively). The transition interval reduces the amount of unnecessary alarms in the case of the varying channel. Then, it is checked whether or not the previous burst was jammed. If the last burst was jammed, the number of unmodulated bursts is compared with$DownTH$. Otherwise, the number is compared with $UpTH$. The jamming detection flag bit sets to 1, if the number of unmodulated bursts exceeded the threshold in both states. Consequently, the jamming detection flag bit is up (i.e. bit=1) until the amount of unmodulated bursts drops below the threshold in both states. The jamming detection algorithm is shown in Figure 12. Having indicated the jamming status of the burst, the jamming detection window moves ahead.

5. DISCUSSION AND SIMULATION RESULTS

In order to evaluate the performance of the proposed algorithms for estimating the channel Doppler shift and jamming detection by BTS for the uplink channel, simulations are performed according to conditions reported in Table 1. In the simulation, we used a realistic physical layer simulator for TETRA systems including a Rayleigh fading channel.

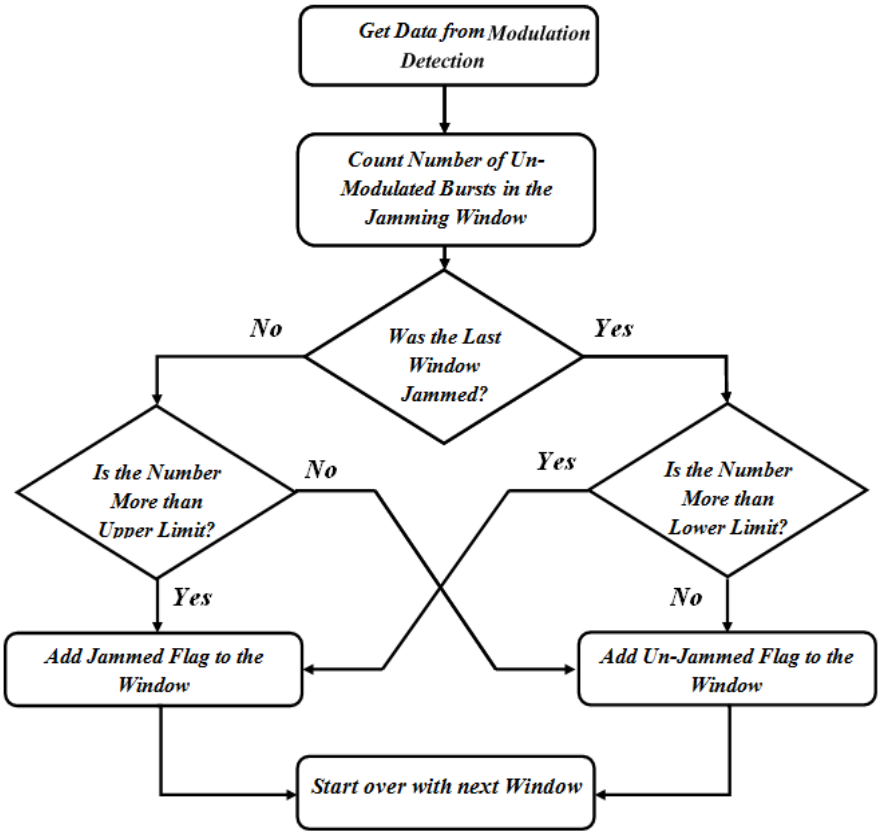

Figure 12 algorithm of the jamming detection

Table 1 Simulation Parameters

Parameters	**Values**
Simulated Receiver	TETRA Receiver
Carrier Frequency	396 MHz
Modulation Mode	$\pi/4$ QPSK
Access Method	TDMA with 4 timeslots per carrier
Channel Model	Rayleigh Fading Channel
Speed of Mobile	0-120 km/h
Length of the Doppler shift Estimation Window	500 msec (34 Bursts), 1 Burst= 14.17 msec
Length of the jamming detection Window	500 msec (34 Bursts), 1 Burst= 14.17 msec
Jammer Signal	Sinusoid Signal with $1kHz$ frequency
Sampling Frequency	8 kHz
Simulation burst length	1000 Bursts
$[SJR_{min}, SJR_{max}]$	$[0\ dB, 15\ dB]$

Figure 13 shows the model of the TETRA system and the Jammer. The transmitted signals are attacked by a jammer, then the jammed signal passes through a Rayleigh fading channel, and at the receiver, the additive white Gaussian noise is added.

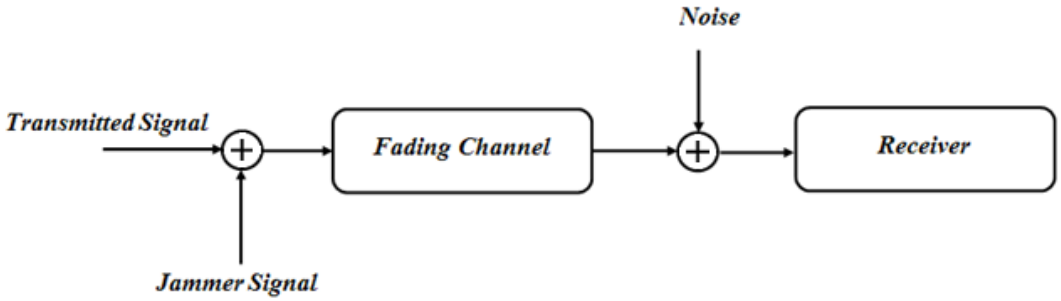

Figure 13 how the jamming signals have been applied to the transmitted signals

The percentage of the extremely damaged bursts at the TETRA receiver in ideal conditions (i.e. $SNR = 30\ dB$ and channel Doppler Shift = 0) is shown in Figure 14. The jammer is a sinusoid wave. These values are the percentage of the unrecyclable bursts, which are not able to be recycled based on the CRC pass block. On the other hand, these values are used as the expected number of destroyed bursts, (Γ) , for different $SJRs$.

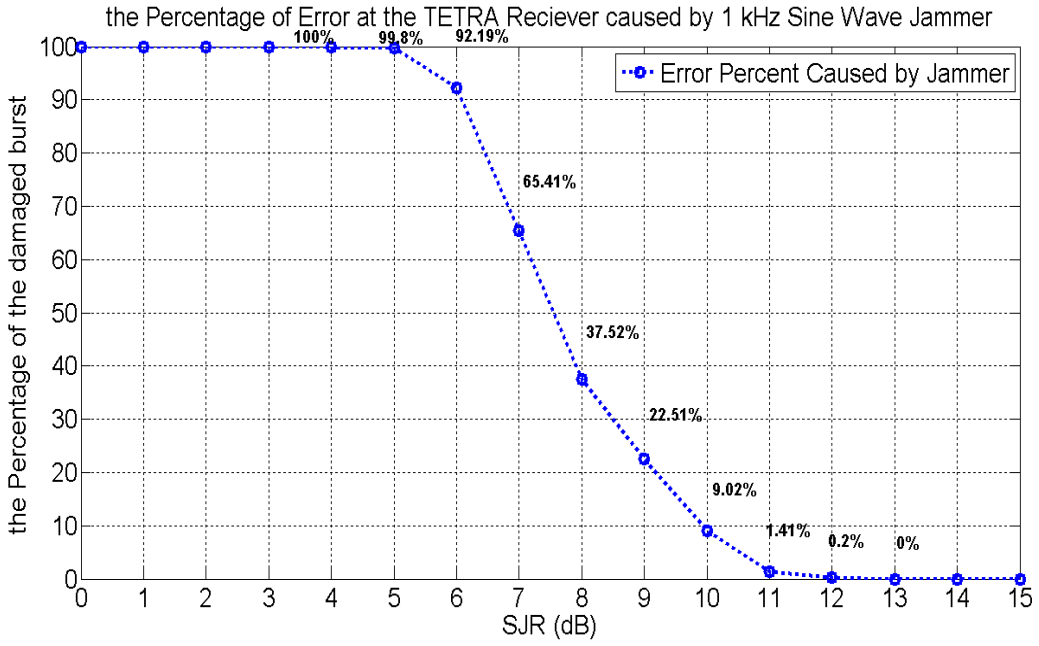

Figure 14 the percentage of the extremely damaged bursts in the TETRA receiver in ideal conditions.

5.1. Performance of the Proposed Channel Doppler Shift Estimation Algorithm

The accuracy of the proposed algorithm in tracking the channel Doppler shift is shown in Figure 15. After receiving 34 bursts (34 burst = 0.5 sec), the proposed algorithm starts, and the initial estimation of user's Doppler shift are performed. Then, the Doppler shift of each incoming burst is estimated. It can be seen that the proposed algorithm outperforms the reference algorithm [29-30] in following the channel Doppler shift, in low SNR conditions.

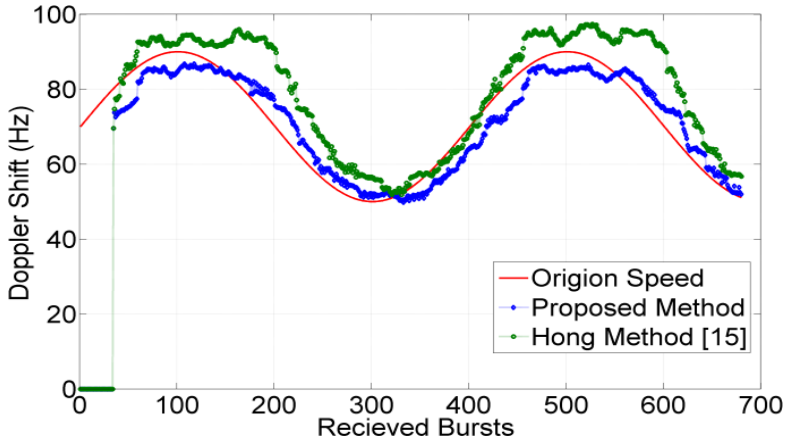

Figure 15 Comparison between the result of Doppler shift estimation in proposed method and Hong method [29].

5.2. Effects of Environmental Noise

In order to assess the effect of environmental noise on the performance of the proposed jamming detection algorithm, the parameter Π is defined as follows:

$$\Pi = \frac{\sum_{i=1}^{N} |\mathrm{JamVec(i)} - \mathrm{Mod.Flag(i)}|}{N} \tag{14}$$

where $|.|$ is the absolute operator, $\mathrm{Mod.Flag}(i)$ is the modulation status of the i^{th} burst, $\mathrm{JamVec}(i)$ is the jamming detection status of the i^{th} burst and N is the number of all received bursts in the TETRA receiver. If the i^{th} received burst is unmodulated, then the$\mathrm{Mod.Flag}(i) = 1$. Otherwise, it is modulated and$\mathrm{Mod.Flag}(i) = 0$. The$\mathrm{JamVec}(i) = 1$, if the i^{th} burst is jammed and $\mathrm{JamVec}(i) = 0$ if it is not jammed.Πis the relative difference between these two flag statuses. Figure 16 shows the parameter Π versus SJR changes in different SNRs. Here, the sinusoid jamming signal with 1kHz is applied on the transmitted signals. Then, the jammed signal has been passed through the Rayleigh fading channel with 0Hz Doppler shift.

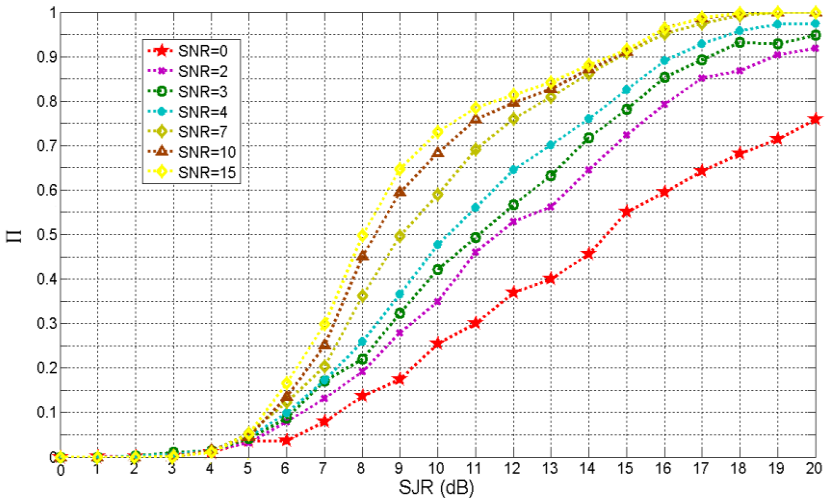

Figure 16 parameterΠ variations versus SJRfor different SNRs.

The higher values of Πshow more correlation between being jammed and being unmodulated. Therefore, in high Πvalues jamming detection only based on modulation status is much reliable. In low Πvalues, more caution in the jamming detection process only based on the modulation detection status should be exercised. This caution is considered by using the jamming detection window, the $UpTH$ and $DownT$ limits.

Since the sinusoid jammer signal has been applied on all sent bursts, the relative difference between the jamming detection statuses $\mathrm{JamVec}(.)$ and the modulation detection statuses $\mathrm{Mod.Flag}(.)$ by reducing the jammer power. This means that, the destroyed bursts by environment noise is considered as the damaged bursts by the jammer. Expected by increasing the SJR, the Π increases and reachs to 1 in SJRs more than $13dB$ (because based on Figure 14, the percentage of the destroyed bursts by the jammer is 0 when SJR is more than $13dB$). However, the environmental noise effects cause the difference between the jamming and modulation detection statuses. By decreasing theSNR, for instance, consider a certain SJR (e.g. $SJR = 20$), the environmental noise effect increases and then the Π value reduces more. The algorithm performance is improved by applying the fixedTH, appropriate $UpTH$ and $DownT$ limits. Then, the differences between the $\mathrm{JamVec}(.)$ and $\mathrm{Mod.Flag}(.)$ statuses reduce.

Compared to Figure 16, this improvement is observed in Figure 17. The values of the fixed TH, UpTH and DownTH are set to -85 dBm, 12 and 9 dB, respectively. The jamming detection in low and high SJRs is easier than detection in middle SJRs (i.e. the SJRs form 5dB to 13dB) because a proportion of the jammed bursts are destroyed. This problem is solved to a great extent by jamming detection window, and UpTH and DownTH limits. Precise determination of the threshold parameters has a great impact on the jamming detection performance and these parameters should be obtained by the extensive experiments.

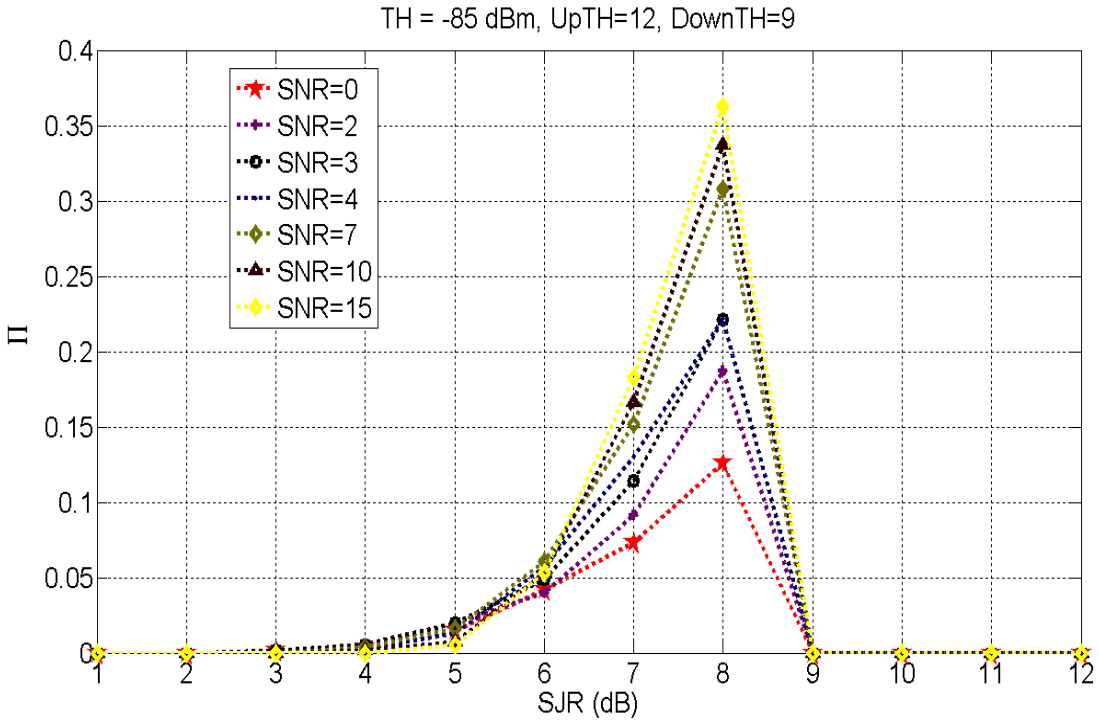

Figure 17 the improved parameter Π versus SJR for different SNRs.

5.3. False Alarm and Missed Detection

In order to evaluate the performance of the proposed algorithm, two criteria of false alarm and missed detection are defined these criteria are calculated as follows.

$$\text{False Alarm}_{\text{SJR}} = \sum_{\text{SNR}:\{\Delta_{\text{SNR}}>\Gamma\}}^{\text{k}} \frac{\Delta_{\text{SNR}} - \Gamma}{\text{k} \times \Gamma}$$
$$\text{Missed Detection}_{\text{SJR}} = \sum_{\text{SNR}:\{\Delta_{\text{SNR}}<\Gamma\}}^{\text{k}'} \frac{\Gamma - \Delta_{\text{SNR}}}{\text{k}' \times \Gamma} \quad (15)$$

Where k and k′ are the number of times that the number of detected jammed bursts are more or less than the real numbers, respectively. $\Delta_{\text{SNR}}$is the number of detected jammed bursts by the proposed jamming detection algorithm in a certain SNR. Γis the number of expected jammed bursts by a certain SJR which are announced by CRC block in the ideal conditions. The amount of the normalized errors is summed together to obtain the number of false alarms and the missed detections at a specific SJR and in a specific range of SNRs.

The achieved number of false alarms and missed detections by applying the proposed jamming detection algorithm as well as a reference algorithm, are shown in Figure 18. The amounts of the fixed TH, UpTH and DownTH are set to -85 dBm, 12 and 9 dB, respectively

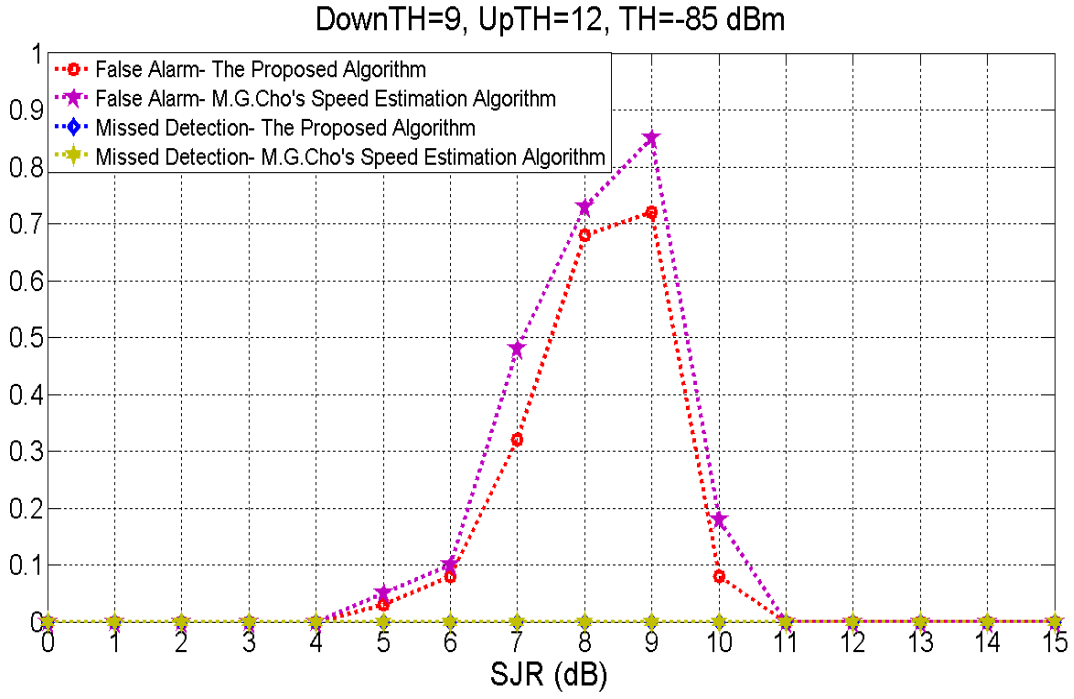

Figure 18 the amount of the false alarm and the missed detection

The proposed algorithm in [29] cannot carefully follow the channel Doppler shift in lowSNR conditions. Overestimating a Doppler shift causes to obtain a lower scaling factor that is needed and the number of bursts that are marked as unmodulated, increases, consequently. Therefore, the number of false alarms increases as well.

As mentioned before, the UpTH and DownTH limits are obtained by experimental tests and have a great influence on the false alarm and the missed detection of the proposed jamming detection algorithm. These limits indicate the sensitivity of the proposed jamming detection algorithm against the attack. By decreasing these parameters, the algorithm sensitivity increases. Therefore, the number of false alarms increases, and the number of missed detections decreases. The optimized values for these thresholds should be obtained by doing experimental tests. The optimized value of these two limits and their impacts on detection performance are shown in Figure 19. The optimized value of the UpTH and DownTH is 18 and 14, respectively.

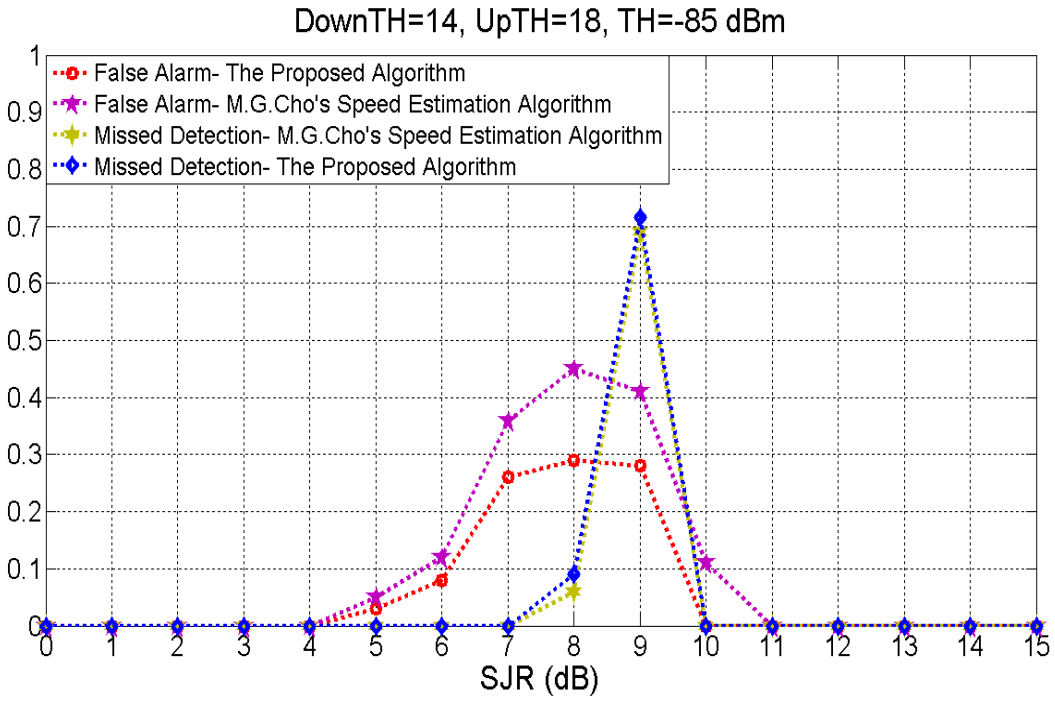

Figure 19 using the optimized value of theUpTH and DownTH

In Figure 20, the performance of the proposed jamming detection algorithm has been compared with kurhila et.al [35] algorithm. The fixed threshold and SJR have been considered TH $=$ -85 dBm and SJR $=$ 7.5 dB, respectively. The percentage of the damaged burst at $SJR = 7.5dB$ in the TETRA simulated receiver is equal to 52%. It can be found that the proposed algorithm outperformed the kurhila et al. algorithm, especially in low$SNRs$. In addition, the impact of the optimized limits can be implied?.

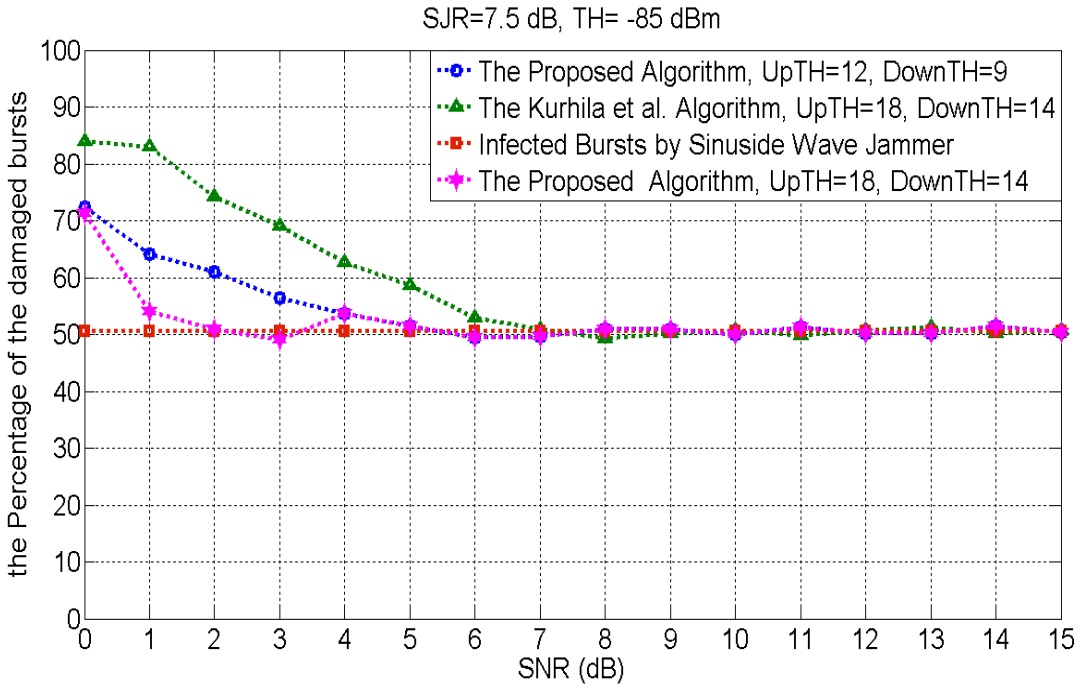

Figure 20 comparison of the performance of the proposed jamming detection algorithm

6. CONCLUSIONS

In this paper, a level crossing based algorithm for Doppler shift estimation is improved and used to enhance the performance of the proposed jamming detection algorithm. The proposed jamming detection algorithm is modelled in a TETRA simulated base station receiver. In order to reduce the implementation complexity, and to improve the performance and enhance the efficiency of the jamming detection algorithm in comparison with reference models [35-36], several improvements are made. In the proposed algorithm, the modulation detection process is only applied to the distorted bursts. Also, by using the proposed Doppler shift estimation algorithm, the scaling factor values with high accuracy is estimated. In addition, the high and low thresholds are calculated by several experiences. It is observed in our simulation results that the proper values of these thresholds have a considerable impact on the performance of the system. It is shown that the performance of the improved Doppler shift estimation algorithm in moderate SNRs (i.e., SNR=5 dB) for TETRA users is in good agreement with other published results. The application of the proposed Doppler shift estimation algorithm is modelled and simulation results exhibit a noticeable improvement in the presence of a wide range of velocities and jammers.

The main limitation of deploying the algorithm is the lack of a real platform for experimental simulations. Then, the next steps to demonstrate the applicability of our proposed framework would be to build it in hardware, so as to be able to investigate its performance and energy efficiency under real-life conditions instead of relying on simulations and assumptions. It would also be interesting to consider neural networks in training BTS in order to achieve considerable performance enhancements in terms of jamming detection and missed detection of the destroyed signals.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Sampath, A., &Holtzman, J. M. (2003, May). Estimation of maximum Doppler frequency for handoff decisions.In IEEE 43rd Vehicular Technology Conference (pp. 859-862).IEEE.

[2] Merwaday, A., &Güvenç, I. (2016). Handover count based velocity estimation and mobility state detection in dense HetNets. *IEEE Transactions on Wireless Communications*, *15*(7), 4673-4688.

[3] Baddour, K. E., & Beaulieu, N. C. (2015). Robust Doppler spread estimation in nonisotropic fading channels. *IEEE Transactions on Wireless Communications*, *4*(6), 2677-2682.

[4] Bellili, F., Selmi, Y., Affes, S., &Ghrayeb, A. (2017). A low-cost and robust maximum likelihood joint estimator for the Doppler spread and CFO parameters over flat-fading Rayleigh channels. *IEEE Transactions on Communications*, *65*(8), 3467-3478.

[5] Anim-Appiah, K. D. (1999). On generalized covariance-based velocity estimation. *IEEE Transactions on Vehicular Technology*, *48*(5), 1546-1557.

[6] Zhang, H., &Abdi, A. (2009). Nonparametric mobile speed estimation in fading channels: Performance analysis and experimental results. *IEEE transactions on wireless communications*, *8*(4), 1683-1692.

[7] Holtzman, J. M., &Sampath, A. (2005). Adaptive averaging methodology for handoffs in cellular systems. *IEEE Transactions on Vehicular Technology*, *44*(1), 59-66.

[8] Zemen, T., &Molisch, A. F. (2012). Adaptive reduced-rank estimation of nonstationary time-variant channels using subspace selection. *IEEE Transactions on Vehicular Technology*, *61*(9), 4042-4056.

[9] Tepedelenlioğlu, C., Abdi, A., Giannakis, G. B., &Kaveh, M. (2011). Estimation of Doppler spread and signal strength in mobile communications with applications to handoff and adaptive transmission. *Wireless Communications and Mobile Computing*, *1*(2), 221-242.

[10] Engdahl, K., &Andersson, L. (2010).Detection of high velocity movement in a telecommunication system.*U.S. Patent No. 7,647,049*. Washington, DC: U.S. Patent and Trademark Office.

[11] Austin, M. D., &Stuber, G. L. (2004). Velocity adaptive handoff algorithms for microcellular systems. *IEEE Transactions on Vehicular Technology*, *43*(3), 549-561.

[12] Klein, T. E., Leung, K. K., &Zheng, H. (2007).Method and apparatus for scheduling transmissions in wireless data networks.*U.S. Patent No. 7,283,814*. Washington, DC: U.S. Patent and Trademark Office.

[13] Mottier, D., &Castelain, D. (2009, September). A Doppler estimation for UMTS-FDD based on channel power statistics. In *Gateway to 21st Century Communications Village.VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324)* (Vol. 5, pp. 3052-3056).IEEE.

[14] Liu, Q. Y., Wang, M., &Zhong, Z. D. (2011). Statistics of capacity analysis in high speed railway communication systems. *Tamkang Journal of Science and Engineering*, *14*(3), 209-215.

[15] Tepedelenlioğlu, C., Abdi, A., Giannakis, G. B., &Kaveh, M. (2011). Estimation of Doppler spread and signal strength in mobile communications with applications to handoff and adaptive transmission. *Wireless Communications and Mobile Computing*, *1*(2), 221-242.

[16] Zhang, C., Fan, P., Dong, Y., &Xiong, K. (2015). Service-based high-speed railway base station arrangement. *Wireless Communications and Mobile Computing*, *15*(13), 1681-1694.

[17] Jingyu, H., Xiaohu, Y., Bin, S., & Kim, Y. H. (2014, May). A Scheme for the Doppler shift estimation despite the Power control in Mobile Communication Systems. In *2004 IEEE 59th Vehicular Technology Conference.VTC 2004-Spring (IEEE Cat.No. 04CH37514)* (Vol. 1, pp. 284-288).IEEE.

[18] Shu, M. L., Hua, J. Y., Li, F., Xu, Z. J., & Wang, D. M. (2014, November). Doppler shift estimation exploiting iterative processing in mobile communications. In *2014 International Workshop on High Mobility Wireless Communications* (pp. 53-56). IEEE.

[19] Austin, M. D., &Stuber, G. L. (2004). Eigen-based Doppler estimation for differentially coherent CPM. *IEEE transactions on Vehicular Technology*, *43*(3), 781-785.

[20] Choi, Y. S., &Alamouti, S. (2010).Doppler frequency determination for mobile wireless devices.*U.S. Patent No. 7,801,084*. Washington, DC: U.S. Patent and Trademark Office.

[21] Jinyu, H., Han, H., Qingmin, M., &Xiaohu, Y. (2014, September). A scheme for the SNR estimation and its application in Doppler shift estimation of mobile communication systems.In *IEEE 60th Vehicular Technology Conference, 2004.VTC2004-Fall.2004* (Vol. 1, pp. 24-27).IEEE.

[22] Ke, X. Q., Yuan, F., Gao, C. X., & Cheng, E. (2018, December). A robust and efficient digital FM underwater acoustic voice communication system based on SNR estimation.In *Proceedings of the Thirteenth ACM International Conference on Underwater Networks & Systems* (pp. 1-5).

[23] Krasny, L., Arslan, H., Koilpillai, D., &Chennakeshu, S. (2011). Doppler spread estimation in mobile radio systems. *IEEE communications letters*, *5*(5), 197-199.

[24] Veluppillai, M., Sangary, N. T., Simmons, S. B., &Jarmuszewski, P. (2013).Method, device and system for detecting the mobility of a mobile device.*U.S. Patent No. 8,442,447*. Washington, DC: U.S. Patent and Trademark Office.

[25] Narasimhan, R., & Cox, D. C. (2009). Speed estimation in wireless systems using wavelets. *IEEE Transactions on Communications*, *47*(9), 1357-1364.

[26] Rezende, C., Boukerche, A., Pazzi, R. W., Rocha, B. P., &Loureiro, A. A. (2011). The impact of mobility on mobile ad hoc networks through the perspective of complex networks. *Journal of Parallel and Distributed Computing*, *71*(9), 1189-1200.

[27] Sha, Y., Yao, N., &Xu, X. (2008, October). Improvement and Performance Analysis of A Scheme for the Maximum Doppler Frequency Estimation. In *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-4).IEEE.

[28] Nanda, S., Rezaiifar, R., &Yavuz, M. (2014).Method and apparatus for interference management, *U.S. Patent No. 8,923,212*. Washington, DC: U.S. Patent and Trademark Office.

[29] Cho, M. G., & Hong, D. (2016).Velocity Estimation Apparatus and Method Using Level Crossing Rate.*U.S. Patent No. 7,120,440*. Washington, DC: U.S. Patent and Trademark Office.

[30] Forenza, A., & Perlman, S. G. (2017).System and method for managing inter-cluster handoff of clients which traverse multiple DIDO clusters, *U.S. Patent No. 9,826,537*. Washington, DC: U.S. Patent and Trademark Office.

[31] Mark, S., Rafael, C., & Salomon, S. (2013). Transceivers and method for use in radio communications. *European Patent Application, EP*, *1*(304), 895.

[32] Gorokhov, A., Khandekar, A., Tingfang, J. I., &Bhushan, N. (2015).System and method to enable resource partitioning in wireless networks.*U.S. Patent No. 9,179,469*. Washington, DC: U.S. Patent and Trademark Office.

[33] Moscovitz, Y., Deperini, F., &Locatelli, M. (2010).Method and User Equipment for Jamming Detection and Signaling in a Mobile Telecommunications Network,*U.S. Patent No. 7,680,450*. Washington, DC: U.S. Patent and Trademark Office.

[34] Breuer, V., &Wehmeier, L. (2019). Method of detecting a jamming transmitter affecting a communication user equipment. *U.S. Patent No. 10,263,726*. Washington, DC: U.S. Patent and Trademark Office.

[35] Kurhila, M., &Torvinen, M. (2014). Base station. *United State Patent*, *203423*, A1.

[36] Shepard, C., Yu, H., Anand, N., Li, E., Marzetta, T., Yang, R., &Zhong, L. (2012, August). Argos: Practical many-antenna base stations. In *Proceedings of the 18th annual international conference on Mobile computing and networking* (pp. 53-64).

[37] Jover, R. P., &Murynets, I. (2016). U.S. Patent No. 9,295,028. Washington, DC: *U.S. Patent and Trademark Office*.

[38] Bereziński, P., Szpyrka, M., Jasiul, B., & Mazur, M. (2016, September). Network anomaly detection using parameterized entropy.*In IFIP International Conference on Computer Information Systems and Industrial Management* (pp. 465-478).Springer, Berlin, Heidelberg.

[39] Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using novel information theory metrics. *Computer Networks*, 116, 96-110.

[40] Waskita, A. A., Suhartanto, H., &Handoko, L. T. (2016, October). A performance study of anomaly detection using entropy method.*In 2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA)* (pp. 137-140). IEEE.

[41] Spuhler, M., Giustiniano, D., Lenders, V., Wilhelm, M., & Schmitt, J. B. (2014). Detection of reactive jamming in DSSS-based wireless communications. *IEEE Transactions on Wireless Communications*, 13(3), 1593-1603.

[42] Vijayakumar, K. P., Ganeshkumar, P., Anandaraj, M., Selvaraj, K., &Sivakumar, P. (2018). Fuzzy logic–based jamming detection algorithm for cluster-based wireless sensor network. *International Journal of Communication Systems*, 31(10), e3567.

[43] Hamamoto, A. H., Carvalho, L. F., Sampaio, L. D. H., Abrão, T., &ProençaJr, M. L. (2018). Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications*, 92, 390-402.

[44] Khan, M. A., Khan, S., Shams, B., &Lloret, J. (2016). Distributed flood attack detection mechanism using artificial neural network in wireless mesh networks. *Security and Communication Networks*, 9(15), 2715-2729.

[45] Rappaport, T. S. (2006). *Wireless communications: principles and practice* (Vol. 2). New Jersey: prentice hall PTR.

[46] Lin, L., So, H. C., & Chan, Y. T. (2013). Accurate and simple source localization using differential received signal strength. *Digital Signal Processing*, *23*(3), 736-743.