Human Micro-Doppler Signature Classification in the Presence of a Selection of Jamming Signals

Dilan Dhulashia & Matthew Ritchie
Department of Electronic and Electrical Engineering
University College London
London, UK
{dilan.dhulashia.15, m.ritchie}@ucl.ac.uk

Shelly Vishwakarma & Kevin Chetty
Department of Security and Crime Science
University College London
London, UK
{s.vishwakarma, k.chetty}@ucl.ac.uk

Abstract—**This work investigates the degradation effects of four distinct jamming signal styles on human micro-Doppler signatures by examining the ability of a linear discriminant classifier to accurately distinguish signatures collected using a simulated frequency modulated continuous wave (FMCW) radar which have been injected with jamming. Misclassification dependence on jamming signal power for each jamming style is presented along with the nature of misclassifications.**

Index Terms—**micro-Doppler, synthetic jamming, radar classification, radar machine learning**

I. Introduction

Targets moving with a radial velocity relative to a radar cause a change in the frequency of the returning electromagnetic (EM) signal, enabling direct measurement of the Doppler effect. Individual components within the structure of a target can move at different velocities, causing additional micro-Doppler modulations beyond the main body return [1]. These can allow classification of the behaviour or type of target observed since micro-Doppler components can appear as unique signatures. In this paper, the difficulty in classifying different activities performed by a human due to four different injected jamming signals into sample micro-Doppler signatures is studied.

Within the electronic warfare domain, the use of electronic counter measures (ECM) is well established. These aim to introduce jamming into the EM environment to cause performance degradation in the range-time domain of search radars. Fewer techniques are capable of providing this service within the Doppler-time domain. As such, radars capable of utilising Doppler information can distinguish between false and real targets present in the range-time domain using micro-Doppler information. To produce realistic false targets it is therefore necessary to also provide deception in the Doppler domain, as shown in [2]. To effectively disrupt classification abilities without using false targets and deception, it is necessary to target jamming such that the Doppler-time spectrogram belonging to a target's return is degraded to an extent where micro-Doppler modulations are unrecognisable by making the signal to interference and noise ratio (SINR) sufficiently low [3].

The aim of the work presented is to investigate the effectiveness of four jamming signals to cause degradation in the Doppler-time domain by examining the ability of a linear discriminant classifier to classify simulated micro-Doppler signatures which have been injected with synthetic jamming data. The relations between the classifiability of interference effected micro-Doppler signatures and the intensity of jamming patterns in the Doppler-time domain due to different jamming signal types has not yet been characterised. Within the work presented, simulated signatures corresponding to recorded motion capture (MoCap) data are generated using *SimHumalator* [4], available at https://uwsl.co.uk. MoCap data has previously been used to successfully construct human models for micro-Doppler signature generation [5][6]. The classification in this work is based on a selection of 16 empirically extracted and singular value decomposition (SVD) based features. In the wider context, micro-Doppler signatures which may be desirable to hide may belong to military vehicles, though initial investigation based on human micro-Doppler signatures allows for more readily available and collectable data to be used. Understanding the effectiveness of different jamming types within the Doppler-time domain is likely to be highly transferable regardless of the nature of the underlying signatures.

The rest of this paper is organised as follows: Section II introduces the jamming signals chosen and provides a motivation for their selection, Section III presents the methodology used for the investigations, Section IV presents the obtained results and provides a brief discussion about the findings, and Section V concludes the work presented and highlights areas for future research.

II. Jamming Signal Theory

A. Matched Filtering

The use of matched filtering as a stage within radar operation provides an element of intrinsic resilience to certain jamming signal types. A matched filter can be achieved by correlating a copy of the transmitted waveform with the received return signal [7]. This effectively searches for a copy of the transmitted waveform within the return

signal, thereby distinguishing between a reflected return and noise/interference. In the case of FMCW radar, the instantaneous frequency difference between the transmission chirp and the returned echo chirp is measured. This is known as the beat frequency and is comprised of frequency differences due to target range and Doppler. Jamming waveforms require characteristics chosen such that they can appear within the radar receiver bandwidth in order to be effective [8].

B. Jamming Techniques

A key advantage the jamming system has over a victim radar is that jamming signals only travel half the distance of the radar signal. To achieve comparable powers at the radar receiver, a jamming signal can have a power proportional to the victim radar's transmitting power divided by the square of the radar to target range [9]. Jamming systems will generally be at a disadvantage in most other aspects.

Greater knowledge of the characteristics of a victim radar can allow for the design of a more effective jamming signal for use against the radar system. In cases where minimal knowledge is available, inefficient styles of jamming, such as barrage jamming, may be used. In such a technique, practical limitations necessitate that the available power at each transmitted frequency is relatively low. Improvements can be made as the amount of situational information increases. Concentration of jamming to a narrower bandwidth can allow higher levels of energy in appropriate sections of the frequency spectrum to be delivered [10]. Sophisticated systems may use digital radio frequency memory (DRFM) technology which can facilitate the recording, manipulation, and re-transmission of the victim radar waveform. This creates a jamming signal which can be correlated with high fidelity at the radar receiver and will register as a return by the victim radar.

Four distinct jamming techniques were designed for investigation in this paper. They represent different levels of jamming complexity and include: tone jamming, deception jamming, frequency streak jamming, and time streak jamming. The intended effects of each type on a sample micro-Doppler signature can be seen in Fig. 1.

1) Jamming type 1 - Deception:
Incoming radar signal is recorded, interacted with the model scatterers, manipulated by phase terms to allow velocity and range deception, and re-transmitted towards the victim radar. A general formulation for such a signal can be described as,

$$s(t) = \sqrt{|P|} \sum_{n=1}^{N} \frac{\sigma_n}{d_n(t)^2} e^{j4\pi \left[\frac{-d_n(t)}{\lambda} + \frac{2d_n(t)}{T_m c} \right]} \quad (1)$$

where: $s(t)$ is the jamming signal, P is the jamming signal power, N is the number of scatterers, d_n is the distance
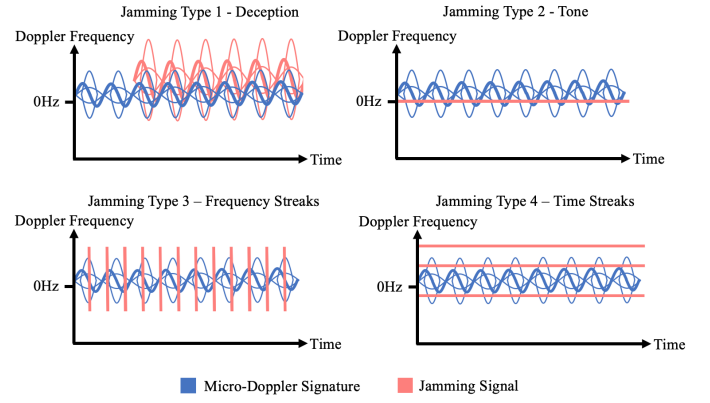

Fig. 1. Theoretical intended effects of each of the four jamming signal types on a generic micro-Doppler signature in the Doppler-time domain.

between scatterer 'n' and victim radar, λ is the signal wavelength, T_m is the victim radar chirp period, c is the speed of light in a vacuum, and σ_n is the radar cross-section (RCS) of scatterer 'n'. The humanoid model is made up of 20 ellipsoid scatterers [4]. In a situation where a deception jamming platform is located separately from the target it is aiming to conceal, the jamming platform will receive two waveforms: the direct waveform arriving from the victim radar, and a waveform from the victim radar which has been reflected from the target in the direction of the jammer. In such a scenario, the jamming system would need to distinguish between these waveforms and construction of the deception waveform would be more elaborate. In the case where the jamming system is co-located with the target, only direct waveforms from the victim radar need to be accounted for.

2) Jamming type 2 - Tone:
Uses a tonal signal with a frequency equal to the carrier frequency of the victim radar

$$s(t) = \sqrt{|P|} e^{j2\pi f_c t} \quad (2)$$

where: $s(t)$ is the jamming signal, P is the jamming signal power, and f_c is the victim radar carrier frequency

3) Jamming type 3 - Frequency Streaks:
Introduces periodic streaks across all Doppler frequencies at certain slow-time intervals.

$$s(t) = \begin{cases} |P|, & t \leq T_m \\ 0, & T_m \leq t \leq T_J \\ s(t - T_J), & \text{In general} \end{cases} \quad (3)$$

where: $s(t)$ is the jamming signal, P is the jamming signal power, T_m is the victim radar chirp period, and T_J is the jamming signal pulse repetition interval

4) Jamming type 4 - Time Streaks:
Introduces streaks at particular Doppler frequencies which extend throughout sample time. Practical implementation can
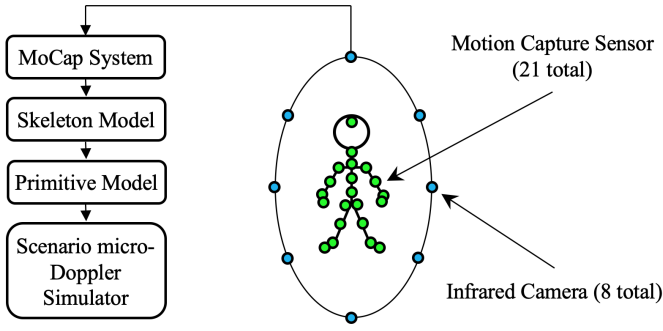
Fig. 2. Depiction of motion capture process used to collect spatial data to create humanoid model. Sensors and infrared cameras are used to obtain the data which is used by the simulation application.

Parameter	Value
PRF	2kHz
Chirp Bandwidth	400MHz
Carrier Frequency	10GHz
Transmit Power	3dBm
Transmit Gain	10dBi
Coherent Processing Interval (CPI)	0.25s
STFT Window Length	200 samples
Overlap Factor	0.9
Pad Factor	4

be achieved by considering and modelling the streaks as returns from point scatterers. The number of scatterers used depends on the number of streaks desired. In this investigation, $N = 3$, since three separate streaks are used, as shown in the corresponding plot in Fig. 1.

III. METHODOLOGY

The micro-Doppler signature samples used are all of a duration of five seconds and were generated using a human micro-Doppler simulation application. MoCap data pertaining to the locations of 21 points on the body of a person performing a particular activity are collected over the activity sample time. A depiction for this capture process and the locations of motion capture points on the body is provided in Fig. 2.

The application creates a model humanoid which performs the activity motion in correspondence to locations recorded in the MoCap data. The RCS of the model ellipsoids are considered over the evolution of the activity time, and returned signal data is generated in accordance with a chosen situational geometry. A monostatic X-band FMCW radar transmitting linearly frequency modulated 'down-chirps', is used in the simulations. The radar parameters are shown in Table. I. Clean micro-Doppler signatures are generated by performing a short time Fourier transform (STFT) on the range-time samples generated by the simulator. These are used for classifier training. For test data sets, jamming signal data is added to the generated range-time samples from the micro-Doppler simulator before the STFT is performed. The parameters used in order to generate the spectrograms are also listed in Table. I.

The signature is then passed to the classifier. In each jamming test, the minimum injected jamming power at which incorrect classification occurs is recorded, as well as the nature of the misclassification (i.e. the incorrect classification activity label). The five possible activity classes are: walking, kicking, punching, grabbing, and body rotating. A block diagram depicting the main stages involved in carrying out a single trial can be seen in Fig. 3.

A Monte Carlo simulation method is used such that repetitive trials using randomly selected training and test data files are carried out. The power of the jamming signal refers to the average jamming signal power level at the receiver of the radar (i.e. the point of injection).

A linear discriminant classifier trained using collections of 16 features extracted from each micro-Doppler sample is used in the classification problem. The feature collections are comprised of both SVD and statistically evaluated empirical features. If the Doppler-time data of a given sample is represented by matrix $\mathbf{A}$, its SVD decomposition can be given by (4), where: $\boldsymbol{\Sigma}$ is a diagonal matrix containing the singular values of $\mathbf{A}$, and $\mathbf{V}$ and $\mathbf{U}$ are the matrices whose columns are the right and left singular vectors of $\mathbf{A}$.

$$\mathbf{A} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^{T} \qquad (4)$$

In each trial, the classifier model undergoes supervised training with a random selection of 90% of the available samples. The trained classifier then attempts to classify the remaining samples prior to the addition of jamming. Test samples which are correctly classified in the absence of jamming can then be used for investigation with jamming signals present, for each of the four jamming cases of interest. In a given trial, four investigations are carried out (one for each jamming signal type) and each of these investigations within the same trial use the same underlying test signature sample. Descriptions
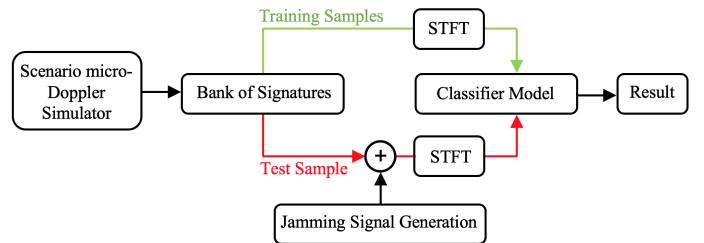

Fig. 3. Block diagram showing the stages involved in a single jamming trial - four investigations occur within each trial, one for each jamming signal type.

Feature	Description
1	Standard deviation (S.D.) of leading diagonal of **U**
2	Mean of leading diagonal of **U**
3	Mean of principle singular vector of **V**
4	Mean of principle singular vector of **U**
5	S.D. of principle singular vector of **V**
6	S.D. of principle singular vector of **U**
7	Sum of all elements in **V**
8	Sum of all elements in **U**
9	S.D. of mean power values from each time sample
10	Mean of mean power values from each time sample
11	S.D. of max. power values from each time sample
12	Mean of max. power values from each time sample
13	S.D. of S.D. values from powers in each time sample
13	Mean of S.D. values from powers in each time sample
15	Max. absolute Doppler frequency of signature return
16	S.D. of sum of powers within a each time sample

of the 16 classification features are provided in Table. II. The effectiveness of the SVD features used have been shown in [11].

IV. RESULTS

A. Jamming Power Results

A total of 550 trial simulations were carried out such that 110 simulations pertaining to each activity were performed. As each trial includes an investigation for each jamming type, a total of 2200 individual investigation runs were made. The primary results from the investigations are presented in a summarised form in Table. III and in the graphs in Fig. 4. Table. III shows the average minimum jamming signal power needed to cause misclassification for each jamming signal type being used on samples of each of the five activity types. Fig. 4 includes plots for each of the five activity types, showing the lowest recorded jamming power from each trial for each of the possible jamming signals at which misclassification occurred. It should be noted that once a single misclassification was recorded, no further increases to the jamming signal power were tested. As the received signal component due to the reflection from the target is identical in each jamming case within a given trial (since each jamming variety is added to a copy of the same underlying clean data), a comparison of the jamming signal power used is equivalent to a comparison of the final SINR for each case.

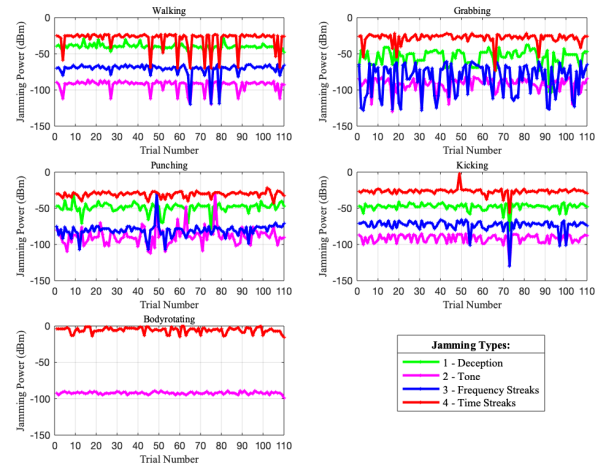| Jamming Type	Walk	Grab	Kick	Punch	Rotate
1 - Deception	-40	-55	-48	-49	Incapable
2 - Tone	-93	-92	-92	-88	-92
3 - Freq. Streaks	-71	-84	-73	-80	Incapable
4 - Time Streaks	-30	-28	-27	-31	-6

Fig. 4. Minimum average jamming signal power found to cause misclassification for each jamming signal type in each trial. This is shown for all five activities

From the results seen in Table. III and Fig. 4, it can be determined that jamming type 2 (tone jamming) tends to require the least power in order to effectively cause misclassification. Jamming type 3 is the second most effective, jamming type 1 is third, and jamming type 4 is the least effective. In instances where the true activity was body rotating, two types of jamming (types 1 and 3) were incapable of causing misclassification. This was verified using a jamming power of 50 dBm and still observing correct classification (These results are not shown). 50 dBm was chosen as a verification power since no further visual changes in the Doppler-time spectrograms were observed at jamming powers above this. The observed phenomena motivates the need for classification with an included confidence level in future work, since it is ambiguous whether jamming was truly ineffective, or whether very intense jamming of any nature, regardless of underlying signature, results in a Doppler-time plot which is most similar to a signature representing body rotating compared to the other classes.

An appreciation for the differences in difficulty of separating target return and jamming components from signatures can be gained by visual inspection of examples of jammed signatures, shown in Fig. 5. The underlying signature used in these example plots is of the walking activity.

The work carried out did not aim to optimise other jamming signal parameters beyond the signal power. Such parameters would include the variables noted in the mathematical descriptions of the jamming signals presented in Section II. An example of this may be the number of streaks included when using jamming type 4, or the time spacing between streaks when using jamming type 3. In these investigations, parameters were chosen which were consistent and compatible with the victim radar operating parameters such that jamming
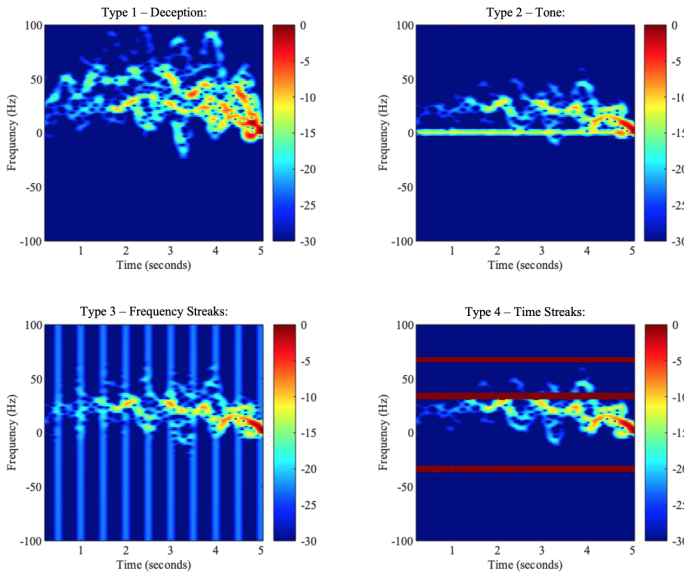
Fig. 5. Real Doppler-time plot examples of a micro-Doppler signature, of the activity of walking, in the presence of each of the four jamming signal types
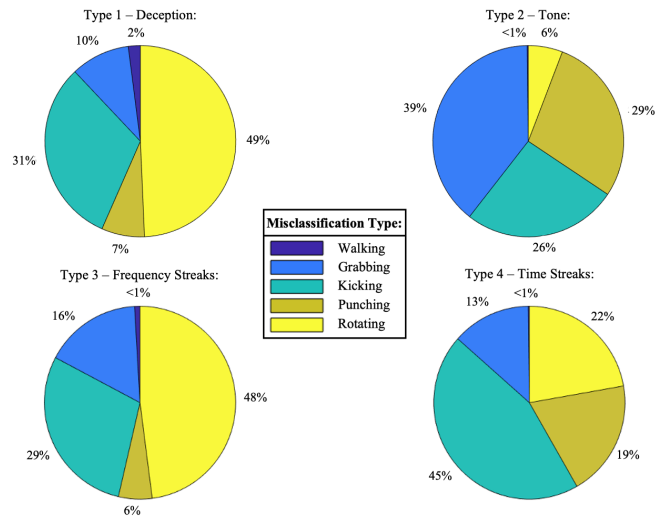

Fig. 6. Pie charts showing the proportion of misclassification occurrences which appeared as each of the possible activity classes, given a particular jamming signal is used

would be permissible and allow for investigation of the jamming signal power. Study into these other variables could show improvements in the jamming capabilities of some of the techniques.

The plots in Fig. 4 show that for a given activity and jamming type, across all trials, the jamming signal power required for misclassification is somewhat constant, with occasional individual simulations giving discrepancies. An exception to this is the grabbing activity with jamming type 3 being used (seen within the top right graph). The results for this combination have a greater variance and, from visual inspection, can be estimated to fall into two jamming signal power level bands.

B. Nature of Misclassifications

Misclassification statistics are provided in Table. IV. These show the proportion of misclassifications which appear as each of the possible activity classes, when data sets belonging to a given true activity class are jammed using a sufficient jamming power.

TABLE IV
PROPORTION OF MISCLASSIFICATION OCCURRENCES WHICH APPEARED AS EACH OF THE POSSIBLE ACTIVITY CLASSES, GIVEN THE UNDERLYING SAMPLE IS A PARTICULAR CLASS

		True Class				
		Walk	Grab	Kick	Punch	Rotate
Misclass	Walk	0%	2.5%	0.9%	0%	0%
	Grab	22.7%	0%	21.1%	48.2%	0%
	Kick	33.0%	58.6%	0%	33.6%	24.1%
	Punch	2.7%	38.6%	5.7%	0%	25.9%
	Rotate	41.6%	0.3%	72.3%	18.2%	50.0%

From Table. IV it can be seen that few misclassifications which register as the walking activity class occur, regardless of the true activity class of the data. The strongest relationship occurs when the true class of the signature is kicking, in which case misclassifications of type body rotating occur in 72.3% of instances.

The plots within Fig. 6 provide an insight into the proportions of misclassifications which appear as each of the possible activity classes, given that a particular jamming signal variant is used. The pie chart for a given jamming signal type shows a proportional breakdown into the five possible activity classes of all misclassifications throughout the investigation caused by that particular jamming type.

It can be determined that jamming types 1 and 3 largely lead to misclassifications of the body rotating activity type, while this only occurs in 6% of misclassifications for type 2 jamming. Type 2 jamming is more likely to cause misclassifications which present as punching, swimming, or kicking, while type 4 jamming primarily leads to micro-Doppler signatures which are misclassified as kicking. All four jamming types cause a very small proportion ($\leq 2\%$) of misclassifications which result in walking misclassifications.

Jamming type 2 (tone jamming), as well as being the most power efficient for causing misclassifications, also appears to cause the most even spread of misclassification types. Type 1 and type 3 jamming both have a dominant misclassification type of body rotating at 49% and 48% respectively, and type 4 jamming has a dominant misclassification type of kicking at 45%. The dominant misclassification type for type 2 jamming is activity type grabbing, and makes up 39% of misclassifications. This is the smallest proportion out of the

dominant misclassification shares belonging to each of the four jamming types, making jamming type 2 more diverse in the way it causes misclassifications.

From both the perspective of jamming signal power efficiency to cause misclassification, and of the ability to cause a more balanced distribution of misclassification types, jamming type 2 has been seen to rank the best out of the four jamming signal types, a seemingly counter-intuitive result. This can be understood by considering that no corrective measures are being taken by the victim radar in the tested scenarios. Tone jamming degrades the SINR from the perspective of the victim radar, by adding a large amount of energy around the 0Hz Doppler frequency. In practice, this could be overcome using a simple filtering stage, thereby making this jamming technique highly ineffective for all real purposes.

The presence of jamming types 3 and 4 (frequency and time streaks, respectively), would be harder for a real radar to identify and remove, though this would still be achievable. These jamming types offer potential for advancement in complexity which would allow them to become harder to deal with. Deception jamming would be the hardest to overcome from the perspective of a victim radar. This work has given an insight into the importance of considering the real life practicalities of radar systems before designing a jamming signal, since the jamming performance of a particular signal is not directly related to the difficulty to remove its effects. That is to say, a jamming signal with very good jamming abilities is not useful if it can easily be dealt with.

V. Conclusions & Future Work

The effects on the ability of a linear discriminant classifier to classify micro-Doppler signatures of five human activities due to a selection of four different jamming signals have been presented. The results from the investigations have shown why, in the approach to ECM jamming, there may be a greater inclination to look to prioritise the use of signals capable of passing through the early processing stages of a victim radar, rather than simply attempting to use the most power efficient jamming method which can cause misclassification of signatures using the lowest signal power. This can be more effectively done when more information regarding the victim radar system operations and characteristics are known.

Future investigations may look to change the approach used for classification, such as the type of classifier used, the features used, or moving to a neural network based system. In future outputs, we will be using experimentally obtained data in conjunction with simulated data, as well as using more conventional ECM jamming signal styles in order to make the work more applicable to real electronic warfare situations.

References

[1] V. C. Chen et al. "Micro-Doppler effect in radar: phenomenon, model, and simulation study". In: *IEEE Transactions on Aerospace and Electronic Systems* 42.1 (2006), pp. 2–21.

[2] X. Shi et al. "Deception jamming method based on micro-Doppler effect for vehicle target". In: *IET Radar, Sonar Navigation* 10.6 (2016), pp. 1071–1079.

[3] Xiaolin Ma et al. "Classification of Human Motions Using Micro-Doppler Radar in the Environments with Micro-Motion Interference". In: *Sensors* 19 (June 2019), p. 2598. DOI: 10.3390/s19112598.

[4] S. Vishwakarma et al. "SimHumalator: An Open Source WiFi Based Passive Radar Human Simulator For Activity Recognition". In: *Preprint at https://uwsl.co.uk/wp-content/uploads/2020/09/Reference-PWR-Simulator.pdf* (Sept. 2020).

[5] B. Erol and S. Z. Gurbuz. "A kinect-based human micro-doppler simulator". In: *IEEE Aerospace and Electronic Systems Magazine* 30.5 (2015), pp. 6–17.

[6] A. D. Singh, S. S. Ram, and S. Vishwakarma. "Simulation of the radar cross-section of dynamic human motions using virtual reality data and ray tracing". In: *2018 IEEE Radar Conference (RadarConf18)*. 2018, pp. 1555–1560.

[7] Mohinder Jankiraman. *Design of Multi-Frequency CW Radars*. 2007. ISBN: 9781891121562. DOI: 10.1049/SBRA004E.

[8] Zhijie Kong et al. "Anti-Sweep Jamming Design and Implementation Using Multi-Channel Harmonic Timing Sequence Detection for Short-Range FMCW Proximity Sensors". In: *Sensors* 17 (Sept. 2017), p. 2042. DOI: 10.3390/s17092042.

[9] J. S. Patel et al. "Fusion of Deep Representations in Multistatic Radar Networks to Counteract the Presence of Synthetic Jamming". In: *IEEE Sensors Journal* 19.15 (2019), pp. 6362–6370.

[10] Leroy B. Van Brunt. *APPLIED ECM*. EW Engineering, Inc. Dunn Loring, VA, 1978. ISBN: 0-931728-00-2.

[11] F. Fioranelli et al. "Feature Diversity for Optimized Human Micro-Doppler Classification Using Multistatic Radar". In: *IEEE Transactions on Aerospace and Electronic Systems* 53.2 (2017), pp. 640–654.