An Overview of Methods of Reducing the Effect of Jamming Attacks at the Physical Layer of Wireless Networks

Dimitriya Mihaylova(✉)

Faculty of Telecommunications, Technical University of Sofia,
8 Kl. Ohridski Blvd, 1000 Sofia, Bulgaria
dam@tu-sofia.bg

Abstract. Jamming as a form of denial-of-service is a commonly-used attack initiated against security at the physical layer of a wireless system. This paper starts with an overview of various types of jamming and measures for its detection. Then, a number of methods for jamming mitigation that can be used at the physical layer are discussed and compared according to their main advantages and drawbacks.

Keywords: Jamming · Denial-of-Service · Physical layer security

1 Introduction

Interference is a major issue in modern-day wireless networks. As a consequence of their easily accessible air interface, wireless systems are impacted by interference emanating from a number of sources. Intra-cell interference, coming from other legitimate users (LUs) in the cell, is usually avoided by using orthogonal frequency division multiple access (OFDMA), meaning that the resources allocated to the users in the cell are orthogonal to one another. On the other hand, frequency reuse in neighbouring cells results in inter-cell interference, which is a big challenge in multi-cell systems. The amount of inter-cell interference depends on numerous parameters, namely the suppression and frequency reuse factors, the antenna gain of the receiver, the transmit power of interfering users and the attenuation (which emanates from small-scale fading, shadowing and path loss). The effect of inter-cell interference can be reduced by collaboration and coordination among cells or by an intelligent management system that regulates the transmission rates and powers.

In order to be successfully decoded at the base station (BS), the received signal's power must exceed the overall power of interference plus ambient noise. In other words, the signal-to-interference-plus-noise-ratio (SINR), which is a quantitative limitation of the channel capacity according to the Shannon-Hartley theorem, must exceed zero decibels. For this reason, an effective attack that an adversary can mount against the security of a wireless system involves deliberately increasing the level of interference in the transmission channel. When the source of interference is not a valid user of the network but rather a malicious user intentionally generating interfering signals in order to disrupt legitimate communication, this type of intervention is called jamming.

V. Poulkov (Ed.): FABULOUS 2019, LNICST 283, pp. 271–284, 2019.
https://doi.org/10.1007/978-3-030-23976-3_24

Jamming can be initiated during the transmission of either data or pilot signals, or both. The uplink pilot transmission phase is typical for time division duplex (TDD) systems, whose channel state information (CSI) is obtained at the BS based on the information about the sent and received pilots. Therefore, jamming the pilots' exchange may result in erroneous computation of the channel gain which, similarly to data transmission jamming, destroys the legitimate communication. A special subcase of jamming the pilot phase is the so-called pilot contamination attack, in which the jammer interferes with the same set of pilots which are used for legitimate channel estimation [1].

The intentional interference may have a significant positive effect on the network performance as well. An interesting opportunity employed by the physical layer security (PLS) comprises interference transmissions from legitimate parties, known as artificial noise (AN) [2], aiming to prevent message decoding from attackers that eavesdrop on the information exchange.

Numerous research works have focused on the different aspects of interference. However, in the scope of this paper, only the interference originated from jamming attacks is considered. In [3] the authors examine the downlink data transmission in a massive MIMO system and demonstrate that unless the jamming attack is initiated during the training phase, it does not have significant impact on the system's performance. Several strategies for jamming the MIMO CSI at the data link layer are presented in [4], such as opposite waterfilling, channel inversion and channel rank attacks. Uplink massive MIMO jamming is discussed in [5] together with investigation of the optimal jamming energy allocation for data and training phases when the number of antennae at BS is much larger than the number of users served by the network. Although many other studies are directed to massive MIMO improvements against jamming, many of the emerging wireless networks are not capable of supporting such a large number of antenna elements, due to hardware restrictions and computational and energy limitations. The physical layer security approaches against jamming, which are discussed in this paper, are extremely beneficial to this type of network.

The paper is organized as follows: in Sect. 2, the topic of jamming attacks on the physical layer and different studies related to their mitigation are discussed. Existing methods that can be used on the physical layer to reduce the effect of a jamming attack are described and several of their main features are compared in Sects. 3 and 4, respectively.

2 Related Studies

The open nature of emerging wireless systems exposes them to the risk of different types of malicious intervention. One possible attack that can be launched against the security of a wireless network is the so called DoS (Denial-of-Service) attack. With the DoS underway, the intruder aims to make the system's resources and services unavailable to its legitimate users and thus disable normal system operation. Depending on the functions performed, each layer of the network architecture is vulnerable to certain types of DoS attack. The authors of [6] describe several possible types of DoS attacks at the various layers of WSNs (Wireless Sensor Networks), whose security

enhancement attracts significant scientific interest with the development of CPSs (Cyber-Physical Systems) and IoT (Internet of Things). A schematic representation of DoS attacks on the levels of the TCP/IP stack is given in Fig. 1.

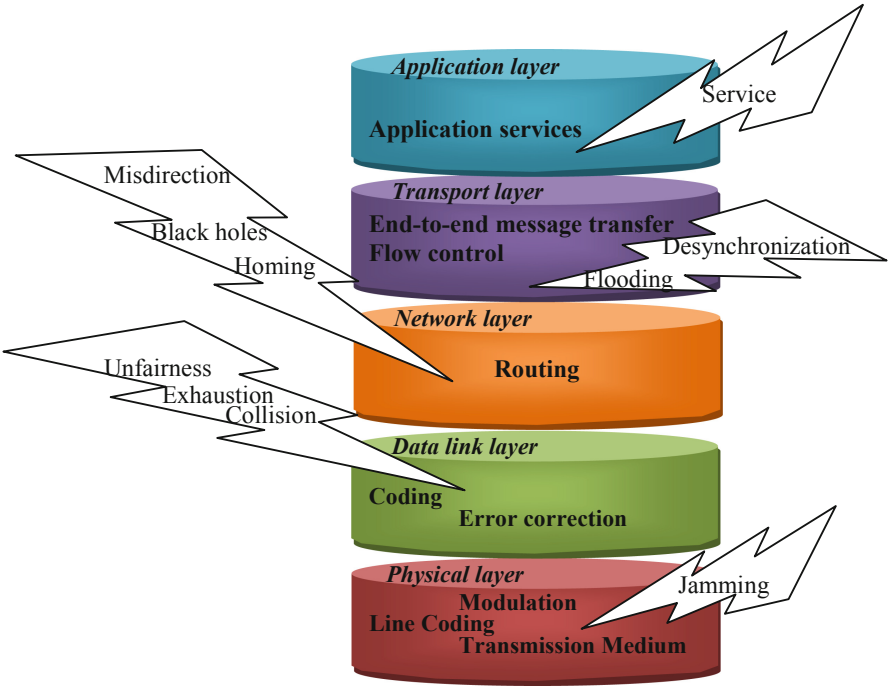

Fig. 1. Possible Denial-of-Service attacks on the TCP/IP layers

Though each level of the protocol stack is vulnerable to specific types of DoS attacks, as illustrated in Fig. 1, the focus of this paper is solely on the physical layer when threatened by a jamming attack.

The jamming attack on the physical layer represents a deliberate generation of radio signals by an adversary with the intent to interfere with the signals transmitted between legitimate parties and thus degrade the quality of legitimate communication. Moreover, as the intruder occupies the resources of the wireless channel, it impedes the users of the network from accessing the channel, leading to DoS at the physical layer. In order to increase their impact on the system's performance, the adversary can undertake various jamming strategies in accordance with his capabilities, the desired effect and the characteristics of the network. Different classifications of jamming are available in the literature but the main types are briefly described here:

1. Wideband jamming – this active attack can be achieved by sending an electromagnetic signal over the entire radio frequency spectrum, resulting in the obstruction of all ongoing transmissions [7].

2. Single-tone jamming – the adversary emits a narrowband signal within the specified bandwidth of the channel being jammed.
3. Multi-tone jamming – as described in [8], the jammer can interfere on multiple frequencies simultaneously, decreasing the SINR of the legitimate receivers. However, the larger the number of frequencies being jammed, the lower the transmit jamming power for each frequency and thus the less the effect on it [9].
4. Single-tone jamming with frequency hopping – with this type of intervention, the attacker jams the entire bandwidth with a high-power narrowband signal with rapidly-changing frequency [9].

Depending on the behaviour of the adversary and, more specifically, the recurrence of his transmissions, the single-frequency jamming can be additionally subdivided into the following six categories [7, 9, 10]:

- Constant jammer – the constant jammer continuously transmits an electromagnetic signal in the form of random bits over the selected channel. Besides interfering with the current communication, the constant emission keeps the wireless channel busy and prevents further access to the channel for subsequent communications. The main disadvantage of constant jamming is its energy inefficiency.
- Deceptive jammer – the deceptive jammer, is identical to the constant, since interference is continuously generated, but they differ in that while the constant jammer transmits random bits, the deceptive one sends regular fames, duping the system into believing that there is no illegitimate presence.
- Random jammer – the random jammer transmits at random during particular time periods and sleeps in others. Its energy efficiency can be regulated by changing the duration of operation and sleep.
- Reactive jammer – this is a jammer which monitors the system and starts interfering only when legitimate information exchange is noticed. Although this type of intrusion surpasses the previous ones in energy efficiency, its effectiveness is reduced as it degrades the SINR of the current transmissions but cannot be used to prevent access to the system resources. As the authors of [10] emphasise, the successful performance of the reactive jammer is closely bound by its capabilities to sense legitimate communication. In certain cases, the adversary can listen for specific activity on the channel, which defines a special subtype of reactive jamming. Examples of this include the node-specific and message-specific jamming attacks in [11] and the IEEE 802.15.4-specific interruption, described in [12].
- Adaptive jammer – the adaptive jammer employs the best jamming strategy in terms of energy efficiency but, as described in [10], represents an unrealistically optimal attack scenario. The adaptability of this intruder consists in adjusting their transmit power in accordance with the CSI of the legitimate channel. When the legitimate users experience good channel conditions, the jammer has to increase its power to deteriorate the communication. Conversely, if the legitimate channel is poor enough to prevent normal information exchange, no jamming is needed and the attacker can stay silent. What makes the use of adaptive jamming impractical is the time-varying fading of the wireless medium which constantly changes the RSS (Received Signal Strength) at the intended receiver. Furthermore, the legitimate channel's CSI is not available to the malicious user.

- Intelligent jammer – the intelligent jammer attacks the system in using the knowledge of certain instabilities of the upper-layers protocols. Several examples of DoS by an intelligent jammer include flooding with TCP/UDP packets, MAC (Medium Access Control) control frames or Smurf attack. As a result, this type of intrusion mostly affects the data link, network, transport and application layer, rather than the physical layer, and is therefore outside the scope of this work.

The authors of [13] discuss different detection techniques that can be used to reveal the presence of the jammer depending on the perceived behaviour. The commonly used approach is based on an analysis of the statistic of the signal received at the legitimate user, expressed by the RSS, CST (Carrier Sensing Time) or PER (Packet Error Rate).

The presence of a constant, deceptive, random and reactive jammer can be revealed through comparison of the RSS of the currently received signal to the one collected during previous transmissions. Since jamming alters the energy of the received signal, a variation in RSS demonstrates the interference's origin.

Monitoring the CST is another way to detect malicious intervention, as the DoS on the physical layer occupies the wireless channel and generates an unusual increase in CST. This could indicate the existence of a constant, deceptive or random jammer. Due to their nature, reactive and adaptive jammers transmit signals only when legitimate communications take place, therefore they do not have the effect of keeping the system busy. For that reason, the CST is not a criterion that can be used to decide whether there is a reactive or adaptive jammer in the network.

An analysis of PER can also indicate the presence of interference induced by jamming as the corruption of legitimate communication significantly enlarges the number of undecodable packets, leading to abnormal values of PER. This method is appropriate for exposing constant, random and reactive jamming, which increase the number of erroneously received packets at the destination. Since the deceptive jammer transmits regular frames, it does not affect the value of PER, hence this statistic is not suitable for detecting this type of jamming.

The unrealistic scenario of the adaptive jamming represents a great challenge from the point of view of detection because its constantly altering power can make the use of RSS or PER statistics inadequate for jamming detection. However, a combination of both the methods is a promising solution [10]. Where both RSS and PER are relatively high, the adaptive jammer can be successfully revealed.

Unlike the physical layer jammers, the intelligent one impacts the upper-layer protocols and analyses of the physical characteristics such as RSS, CST and PER, cannot be used to disclose its presence.

When a jammer is detected, measures to mitigate its influence on the system performance must be considered. Various approaches to counter jamming exist in the literature but most of them rely on complex algorithms and protocols from upper layers, which makes them unsuitable for resource-constrained applications.

A swarm intelligence conception of an ant system is suggested for use against WSN jamming in [8], where the transmission route between source and destination changes depending on parameters such as number of hops, energy and distance, SNR (Signal to Noise Ratio), BER (Bit Error Rate), packet delivery and packet loss, some of which relate to the upper layers of the protocol stack. Another study [14] proposes several

MAC layer mechanisms, including frame masking, packet fragmentation and redundant encoding, for combatting different types of jammers whose capabilities are identical to those of legitimate users. Limiting factors for their implementation are the induced overhead, computational complexity and power consumption. The authors in [15] propose a mapping protocol to inform the network about the location and shape of the jammed range so that routing management can be applied on upper layers to avoid the attacked nodes of the network. In [16] the channel surfing method for jamming avoidance is proposed, which switches to another link layer channel if jamming is detected. Another commonly used strategy to suppress the effect of jamming attacks relies on game theory. A taxonomic survey of the available game theoretic methods to defend against jamming in the literature is given in [17], where the authors draw attention to the growing number of such approaches. Nevertheless, the resource allocation problem in game theory is again solved at the MAC or data link layer, which makes it more complicated than the physical layer security techniques.

3 Jamming Mitigation Techniques Used at the Physical Layer

3.1 Spread Spectrum as a Jamming Defence Mechanism

One conventional method to counteract jamming attacks at the physical layer is by using spread spectrum techniques, which expand the spectrum of the original signal into a wider frequency band. The effect of spread spectrum modulation is twofold: on the one hand, it helps to hide the fact that communication is in progress from unauthorized parties, referred to as low probability of intercept (LPI). On the other hand, spreading the signal over the entire frequency band of the channel makes it more resistant to natural noise and interference as well as jamming and eavesdropping attacks. The various spread spectrum approaches include direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), time hopping spread spectrum (THSS), parallel sequence spread spectrum (PSSS), chirp spread spectrum (CSS), and different hybrids between them. However, the most widely used in wireless communications are DSSS and FHSS, which are outlined in the following two subsections.

Frequency Hopping Spread Spectrum. Frequency hopping (FH) is a modulation technique in which the carrier frequency changes repeatedly in order to prevent narrowband jamming [18, 19]. The algorithm according to which the frequency is shifted over the entire spectrum follows a pseudo-random sequence and must be available at both the transmitter and the receiver but has to be kept secret from non-authorised users. Otherwise, if the jammer gets access to the hopping pattern, he can simply alter the central frequency of the jamming signal following the one used in legitimate transmission, thus making FHSS modulation impractical.

For the demodulation purposes, perfect synchronisation is needed between the spreading sequences of the legitimate parties, which represents a major problem of the FHSS technique. The pseudo-random sequence agreement can be realized by using

cryptography mechanisms on the upper layers of the system model, inducing high system complexity. However, a lightweight PLS key generation algorithm can be implemented instead, by which the hopping pattern can be negotiated using the random radio characteristics of the wireless propagation environment.

Another FHSS drawback concerns the inefficient use of the frequency band. Although narrowband signals, which occupy small parts of the entire spectrum for very short periods of time, are transmitted, the large number of frequencies needed for reliable FH modulation demands the availability of a wideband frequency spectrum.

Direct Sequence Spread Spectrum. Direct sequence spread spectrum is another modulation technique widely used as a measure against interference and jamming [20]. The approach consists in expanding the transmitted signal into a wider frequency band by simple multiplication to a pseudo-noise (PN) sequence, which is again random. The PN represents a sequence of rectangular pulses with values 1 and −1, also called chips. Since the PN frequency is much higher than that of the transmitted signal, the resultant spectrum of the modulated signal is similar to the spectrum of noise. Thus the narrowband jamming signal, whose power is concentrated over a small bandwidth, affects only a negligible part of the frequency spectrum of the transmitted signal. Moreover, spreading the original signal into a wider bandwidth distributes its entire power over a large number of frequency components so that its power spectral density is significantly reduced and may even fall under the white noise level. In this way, secure legitimate transmission can be carried out without being detected by a malicious user trying to intercept the communication, i.e. privacy enhancement is another advantage of DSSS application.

The larger the frequency of the PN sequence, the wider the spectrum occupied and hence the lower the power spectral density and the influence of jamming interference are. Nevertheless, spreading restrictions must be taken into account for bandwidth efficiency purposes.

The DSSS demodulation at the receiver, called de-spreading, again represents multiplication of the received signal by the same pseudo-random noise sequence used in the transmitter for spreading modulation. In order to obtain reliable results, the PN sequences of both the transmitter and receiver must be negotiated in advance, meaning that synchronization is a major challenge in DSSS, as it is in FHSS. The other disadvantage of FHSS, namely the spectrum utilization problem, also concerns DSSS, as wide bandwidth needs to be occupied for each transmission.

3.2 Jamming Filtering at the Receiver

RZF Receive Filter. An approach proposed in [21] aims to reduce the radio jamming induced by an adversary through special construction of the receive filter at the BS. The method employs the idea introduced in [22] to design the filter in a regularization manner, so as to be adjustable and able to obtain optimal results. It can be applied when the jammer attacks both the training and data transmission phases. The algorithm followed to design the receive filter, called regularized zero-forcing (RZF) and explained in Algorithm 1, uses the channel estimates of both legitimate and jamming

channels – $\hat{h}$ and $\hat{g}$, correspondingly. In order to obtain $\hat{g}$, a zero-forcing technique is used. When using RZF for the estimation of jamming channels, it is assumed that at least one pilot sequence exists that is orthogonal to those of LU and remains unused during the pilots' transmission. The jamming channel is estimated by nulling the LU's training sequence through projection of the received signal onto the unused pilot sequence, which is orthogonal to the sequences assigned to LU.

After the process of channel estimation of both legitimate and non-legitimate channels, a linear RZF receive filter is constructed.

Algorithm 1: RZF algorithm

1: Uplink transmission of a training sequence and receiving its corresponding jammed signal at the BS;

2: Obtaining an estimate of the legitimate and jamming channels – $\hat{h}$ and $\hat{g}$, at the BS through zero-forcing;

3: Construction of a regularized linear receive filter, based on both $\hat{h}$ and $\hat{g}$.

The MMSE-type receiver uses conventional MMSE (Minimum Mean Square Error) estimation for filter design. Optimal performance of the MMSE-type receiver is observed when $\hat{h}$ and $\hat{g}$ are calculated with no errors from channel estimation.

The ZF-type receiver aims at eliminating the jamming signal by orthogonal projection of $\hat{h}$ onto $\hat{g}$. It reduces the complexity of the MMSE-type receiver as no matrix inversion is needed for its computations. Moreover, as the numerical results in [21] demonstrate, the ZF-type receive filter improves the rate achieved by the MMSE-type receive filter for the same levels of transmit power used by LU and the jammer. The ZF-type receiver is an RZF filter whose regularization factor converges to zero.

BJM Receive Filter. A promising approach for the mitigation of jamming attacks, that can be used at the physical layer of a MIMO wireless system, is proposed in [23]. The strategy involved consists in the construction of a jamming-resistant receiver based on a blind jamming mitigation (BJM) algorithm. The BJM algorithm can overcome the effect of jamming induced by multiple malicious devices as long as the number of receive antennae at the MIMO receiver exceeds the total number of antennae at the jammer. A main advantage of the BJM receiver is that no channel knowledge is needed to resist an attack, since the receive filter is designed using only the information about the pilot signals sent and received during the training phase. The BJM algorithm is represented in Algorithm 2.

Algorithm 2: BJM algorithm

1: Uplink transmission of a training sequence $\left[\widetilde{X}(1), \widetilde{X}(2), ..., \widetilde{X}(L)\right]$ composed of L number of pilot signals and receiving its jammed values $\left[\widetilde{\mathbf{Y}}(1), \widetilde{\mathbf{Y}}(2), ..., \widetilde{\mathbf{Y}}(L)\right]$ at the BS;

2: Computation of expected values $E\left[\mathbf{Y}\mathbf{Y}^H\right]$ and $E\left[\mathbf{Y}X^H\right]$ at the BS, where X is the uplink signal at the LU, $\mathbf{Y}$ is its corresponding received signal at the BS and $(\cdot)^H$ denotes a Hermitian matrix;

3: Construction of an optimal linear spatial filter P by setting the MSE of the decoded signal at the BS to zero.

The BJM algorithm aims at designing an optimal linear spatial filter **P** using solely the knowledge of the training signals. For that reason, the MSE (Mean Squared Error) of the estimated pilot signals must be minimized by setting its derivative with respect to **P** to be zero.

Digital Filter for IEEE 802.15.4. A method for jamming avoidance in IEEE 802.15.4 communication networks, working in the 2450 MHz frequency band, is proposed in [24]. At the physical layer, the 802.15.4 standard incorporates the DSSS technique for jamming mitigation. After the message is de-spread at the receiver, a MAC layer 2-byte cyclic redundancy check (CRC) is performed. The CRC is computed at both the transmitter and receiver ends and its value is sent together with the payload data. If both the CRC computations differ from one another, the transmission of the packet is not considered successful and it has to be retransmitted. This procedure represents an opportunity for the attacker, since corruption of a symbol per packet results in denial of service. For that reason, although DSSS is applied in the standard, the system is not secure against jamming attacks. As interfering with only one symbol per packet is enough to disrupt the communication, a successful jammer can take advantage and reduce its energy consumption by undertaking random jamming attack.

For counteracting such a type of intervention, initiated at the centre frequency of a legitimate signal, the authors of [24] suggest the use of an additional high-pass digital filter to eliminate the narrowband jamming component. While the low-pass filter conventionally incorporated in 802.15.4 is capable of suppressing the inter-cell interference and noise, it is not able to affect jamming at the baseband. In contrast, as the experimental results in [24] show, jamming mitigation is achieved when an additional high-pass finite impulse response (FIR) filter of low order is added. The operation sequence of 802.15.4 together with the implementation of the proposed filter is summarized in Algorithm 3.

Two major problems with the proposed filtering are emphasized in [24]. The first relates to SNR degradation when no jamming is present in the system. The other weakness of this technique is in the assumption that the centre frequencies of the legitimate and jamming signals coincide, which is not a realistic scenario. To cope with these drawbacks, in [25], algorithms for filter selection in an adaptive manner are proposed. However all the algorithms explore information about the packet delivery ratio (PDR), which is a parameter computed at the MAC layer and takes the approach out of the scope of this paper, where solely physical layer security methods are discussed.

Algorithm 3: 802.15.4 algorithm with high-pass filter implemented

1: Transmission of a signal, spread by DSSS;

2: Signal's de-spreading at the receiver;

3: Filtering of noise and inter-cell interference by low-pass filter and jamming mitigation by high-pass digital filtering;

4: Comparison of the CRC received in the packet with the one calculated at the receiver and raising a flag if they are different.

4 Comparison of the Jamming Mitigation Techniques Discussed

This section comprises a comparison of several essential advantages and drawbacks of the methods discussed which can influence their implementation in different types of networks depending on the infrastructure and resources available. The results of the comparison are summarized in Table 1.

As is shown in the table, all the methods discussed need some additional processing to be conducted at the receiver – in FHSS and DSSS the signal is de-spread at the receiver, while all types of filtering are also performed there. Whereas spreading of the signal in a larger frequency band is realized at the transmitter before the message to be sent, none of the filtering methods rely on processing at the transmitter, which makes them advantageous from the ease of implementation point of view. Two more features that are in the favour of the filters proposed as distinct from the spread spectrum approaches relate to the efficient utilization of the available bandwidth and the lack of necessity for time and frequency synchronization to ensure reliable performance.

Although the digital filter design suggested for IEEE 802.15.4 networks is the easiest to be implemented, as only a simple FIR filter of low order must be additionally applied, its main drawback consists in the increased error rates in non-jamming environments. The reason for this is that the resultant band-stop filter attenuates the legitimate signal at the centre frequency when no attack is initiated.

MMSE receive filter, FHSS and DSSS are the three methods that are inappropriate to be used for networks with memory and power constraints, due to their high computational complexity.

The major disadvantage of the two RZF receive filters – MMSE and ZF, is that channel estimation is needed for them to perform successfully. Moreover, the CSI of not only the legitimate but also of the jamming channel must be obtained. For that reason, a purposely unused pilot sequence and large number of training signals are needed. Though the BJM receive filter also explores the training phase with multiple pilots, its operation does not concern any CSI which makes it more accurate in scenarios when jamming is also present in the training phase.

Summarizing the results of the properties compared in Table 1, it can be observed that the digital filter proposed for IEEE 802.15.4 networks is superior to the others from a computational complexity point of view, since only processing at the receiver, which is much simpler than in the other filtering approaches, needs to be applied. Furthermore, as no CSI is needed for its implementation, this technique is not dependent on the channel training phase and can achieve reliable results for jamming mitigation during the pilots' transmission session. Despite its inefficient performance in the absence of jamming, the aforementioned characteristics of the IEEE 802.15.4 digital filter make it the recommended method, particularly in scenarios of resource-constrained wireless systems, where operations are restricted due to computational and power limitations.

Table 1. Comparison of the jamming mitigation techniques at the physical layer

No	Features compared	Jamming mitigation technique					
		Spread spectrum approaches		Receive filter approaches			
		FHSS	DSSS	MMSE	ZF	BJM	Digital filter for IEEE 802.15.4
1	Additional processing at the receiver	✓	✓	✓	✓	✓	✓
2	Additional processing at the transmitter	✓	✓	✗	✗	✗	✗
3	Synchronization needed	✓	✓	✗	✗	✗	✗
4	Increased bandwidth needed	✓	✓	✗	✗	✗	✗
5	Performance loss in non-attack scenarios	✗	✗	✗	✗	✗	✓
6	High computational complexity	✓	✓	✓	✗	✗	✗
7	CSI needed	✗	✗	✓	✓	✗	✗
8	Large number of pilots needed	✗	✗	✓	✓	✓	✗
9	Purposely unused pilot sequence needed	✗	✗	✓	✓	✗	✗

5 Conclusion

In this paper several physical layer security methods for jamming mitigation are described and analysed based on substantial features for their implementation. Observing the main characteristics of the solutions in the comparison, in summary it could be said that a filter that does not rely on channel estimations and can adaptively change its centre frequency, using only physical layer parameters, will be a promising strategy for jamming mitigation.

A topic worthy of further investigation concerns a review of receive filter approaches that can be used in wireless systems to mitigate the effect of a jamming attack whose frequency is variable in time. Such a novel filtering method with tunable bandwidth and central frequency will be proposed in a future work. In order to be applicable in resource-constrained systems, the filter will be of low order and have low computational complexity and high efficiency. Moreover, the adaptive properties of the filter will avoid degradation of the signal in non-jamming environments and in this way will improve the performance of the digital filter proposed for IEEE 802.15.4. Such an approach is proposed in [26] and will be experimentally evaluated in the presence of jamming attacks in a future study.

Acknowledgment. The paper is published with the support of the project No BG05M2OP001-2.009-0033 "Promotion of Contemporary Research Through Creation of Scientific and Innovative Environment to Encourage Young Researchers in Technical University - Sofia and The National Railway Infrastructure Company in The Field of Engineering Science and Technology Development" within the Intelligent Growth Science and Education Operational Programme co-funded by the European Structural and Investment Funds of the European Union.

References

1. Wu, Y., Schober, R., Ng, D.W.K., Xiao, C., Caire, G.: Secure massive MIMO transmission with an active eavesdropper. IEEE Trans. Inf. Theory **62**(7), 3880–3900 (2016)
2. Bash, B.A., Goeckel, D., Towsley, D., Guha, S.: Hiding information in noise: fundamental limits of covert wireless communication. IEEE Commun. Mag. **53**(12), 26–31 (2015)
3. Basciftci, Y.O., Koksal, C.E., Ashikhmin, A.: Securing massive MIMO at the physical layer. In: 2015 IEEE Conference on Communications and Network Security (CNS), Florence, pp. 272–280 (2015)
4. Miller, R., Trappe, W.: On the vulnerabilities of CSI in MIMO wireless communication systems. IEEE Trans. Mob. Comput. **11**(8), 1386–1398 (2012)
5. Pirzadeh, H., Razavizadeh, S.M., Björnson, E.: Subverting massive MIMO by smart jamming. IEEE Wirel. Commun. Lett. **5**(1), 20–23 (2016)
6. Sinha, P., Jha, Rai, A.K., Bhushan, B.: Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey. In: 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, pp. 288–293 (2017)
7. Amin, Y.M., Abdel-Hamid, A.T.: Classification and analysis of IEEE 802.15.4 PHY layer attacks. In: 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT), Cairo, pp. 1–8 (2016)

8. Muraleedharan, R., Osadciw, L.: Jamming attack detection and countermeasures in wireless sensor network using ant system. In: 2006 SPIE Symposium on Defense and Security, April 2006 (2006)
9. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G.: A survey on jamming attacks and countermeasures in WSNs. IEEE Communications Surveys Tutorials **11**(4), 42–56 (2009). Fourth Quarter
10. Zou, Y., Zhu, J., Wang, X., Hanzo, L.: A survey on wireless security: technical challenges, recent advances, and future trends. Proc. IEEE **104**(9), 1727–1765 (2016)
11. O'Flynn, C.P.: Message denial and alteration on IEEE 802.15.4 low-power radio networks. In: 2011 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, pp. 1–5 (2011)
12. Jokar, P., Nicanfar, H., Leung, V.C.M.: Specification-based Intrusion Detection for home area networks in smart grids. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, pp. 208–213 (2011)
13. Pelechrinis, K., Iliofotou, M., Krishnamurthy, S.V.: Denial of service attacks in wireless networks: the case of jammers. IEEE Commun. Surv. Tutor. **13**(2), 245–257 (2011). Second Quarter
14. Wood, A.D., Stankovic, J.A., Zhou, G.: DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, San Diego, CA, pp. 60–69 (2007)
15. Wood, A.D., Stankovic, J.A., Son, S.H.: JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, RTSS 2003, Cancun, Mexico, pp. 286–297 (2003)
16. Xu, W., Wood, T., Trappe, W., Zhang, Y.: Channel surfing and spatial retreats: defenses against wireless denial of service. In: Proceedings of the 2004 ACM Workshop on Wireless Security (WiSe), NY, USA, pp. 80–89 (2004)
17. Vadlamani, S., Eksioglu, B., Medal, H., Nandi, A.: Jamming attacks on wireless networks: a taxonomic survey. Int. J. Prod. Econ. **172**, 76–94 (2016)
18. Navda, V., Bohra, A., Ganguly, S., Rubenstein, D.: Using channel hopping to increase 802.11 resilience to jamming attacks. In: IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications, Barcelona, pp. 2526–2530 (2007)
19. Bloch, M., Barros, J.: Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, Cambridge (2011)
20. Liu, Y., Ning, P., Dai, H., Liu, A.: Randomized differential DSSS: jamming-resistant wireless broadcast communication. In: IEEE INFOCOM, pp. 1–9 (2010)
21. Do, T.T., Björnson, E., Larsson, E.G.: Jamming resistant receivers for massive MIMO. In: 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, pp. 3619–3623 (2017)
22. Peel, C.B., Hochwald, B.M., Swindlehurst, A.L.: A vector-perturbation technique for near-capacity multiantenna multiuser communication-part I: channel inversion and regularization. IEEE Trans. Commun. **53**(1), 195–202 (2005)
23. Zeng, H., Cao, C., Li, H., Yan, Q.: Enabling jamming-resistant communications in wireless MIMO networks. In: 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, pp. 1–9 (2017)
24. DeBruhl, B., Tague, P.: Digital filter design for jamming mitigation in 802.15.4 communication. In: 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), Maui, HI, pp. 1–6 (2011)

25. DeBruhl, B., Tague, P.: Mitigation of periodic jamming in a spread spectrum system by adaptive filter selection. In: Proceedings of the International Symposium on Photonic and Electromagnetic Crystal Structures, pp. 431–439 (2012)
26. Nikolova, Z., Stoyanov, G., Iliev, G., Poulkov, V.: Complex coefficient IIR digital filters. In: Márquez, F.P.G. (ed.) Digital Filters, Chapter 9, April 2011, pp. 209–239. InTech (2011). ISBN: 978-953-307-190-9