A General Security Approach for Soft-information Decoding against Smart Bursty Jammers

Furkan Ercan[†], Kevin Galligan[*], Ken R. Duffy[*], Muriel Médard[§], David Starobinski[†], Rabia Tugce Yazicigil[†]
[†]Department of Electrical and Computer Engineering, Boston University, Boston, MA, USA
[§]Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA, USA
[*]Hamilton Institute, Maynooth University, Ireland

2022 IEEE Globecom Workshops (GC Wkshps) | 978-1-6654-5975-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/GCWkshps56602.2022.10008541

***Abstract*—Malicious attacks such as jamming can cause significant disruption or complete denial of service (DoS) to wireless communication protocols. Moreover, jamming devices are getting smarter, making them difficult to detect. Forward error correction, which adds redundancy to data, is commonly deployed to protect communications against the deleterious effects of channel noise. Soft-information error correction decoders obtain reliability information from the receiver to inform their decoding, but in the presence of a jammer such information is misleading and results in degraded error correction performance. As decoders assume noise occurs independently to each bit, a bursty jammer will lead to greater degradation in performance than a non-bursty one. Here we establish, however, that such temporal dependencies can aid inferences on which bits have been subjected to jamming, thus enabling counter-measures. In particular, we introduce a pre-decoding processing step that updates log-likelihood ratio (LLR) reliability information to reflect inferences in the presence of a jammer, enabling improved decoding performance for any soft detection decoder. The proposed method requires no alteration to the decoding algorithm. Simulation results show that the method correctly infers a significant proportion of jamming in any received frame. Results with one particular decoding algorithm, the recently introduced ORBGRAND, show that the proposed method reduces the block-error rate (BLER) by an order of magnitude for a selection of codes, and prevents complete DoS at the receiver.**

I. Introduction

Jammers typically aim to cause a denial of service (DoS) or reduction of quality (RoQ) at the receiver [1] without getting detected. They exploit the wireless transmission by mixing their signals with legitimate communication. As a result, the received frame becomes undecodable, which causes anomalies such as increased repeat requests, reduced throughput, prolonged delays, or a complete breakdown [2]. Powerful jammers that blast channels with unrestrained amounts of energy can be detected easily by the receiver. More subtle jammers, on the other hand, might seek to inject short bursts or lower levels of energy to disrupt communication while circumventing their detection, causing a DoS. In general, jammers must demonstrate high energy efficiency, low detection probability, high levels of DoS, and resistance against physical layer (PHY) anti-jamming techniques.

From an information-theoretic perspective, uniform jammers are the most effective for reducing the channel capacity and the code rate [3]. However, emerging techniques such as rate-adaptation algorithms propose efficient countermeasures for such jammer attacks [4]. On the other hand, bursty jammers [5] can be an effective approach for increasing the block-error rate (BLER), where an adversary jams a burst of bits in a transmitted frame. Bursty jammers become more effective in increasing the BLER when their burst patterns are unpredictable to the receiver. With increased BLER, the receiver must compensate by reducing the code rate, which sacrifices information throughput. Therefore it is essential to study countermeasures to such jammer attacks.

Most traditional security approaches for wireless technologies are applied to upper layers in the protocol stack [6]. However, with the rapid growth in use cases and network density, maintaining security for 5G-and-beyond technologies has become a challenge [7]. PHY-layer security is an emerging solution to threats that arise with evolving adversaries [8]. Under such adversarial behavior, machine learning-based approaches [9], [10] and spectrum sensing-based approaches [11] have been proposed to counter jamming. Our paper specifically focuses on jamming attacks on soft-information decoders, a topic that has received scant attention in the literature. Our anti-jamming approach applies to general coding schemes and can be effortlessly supported on the physical layer with minimal computational overhead.

In this work, we consider a smart, reactive jammer that is bursty and only active during a fraction of the transmission. It is assumed that transmission parameters, such as the modulation and the subcarrier frequency, are known to the adversary. To counter such an attack, we propose a modified log-likelihood ratio (LLR) computation that takes the conditional probability of jamming into account for each index of the received frame. The computation of this posterior probability is performed in two steps. First, an initial value is calculated based on the received signal strength. Anchor points in the received frame, for which the conditional jamming probability is high, are then used to inform the jamming estimates of neighbouring points, based on Markov state transition probabilities. The proposed method is general to any receiver and carried out before decoding. Simulation results show that the proposed method unveils a significant amount of the attack, and therefore the attacker cannot maintain their deniability. Using the universal ORBGRAND algorithm [12], [13], it is shown that an order of magnitude of BLER performance can be recovered with the proposed method and a complete DoS is prevented, using different codebooks, *i.e.* random linear codes (RLCs) and 5G cyclic redundancy check-aided Polar codes

(CA-Polar).

The rest of the paper is organized as follows. In Section II, preliminaries are detailed. In Section III, the smart bursty jammer model and proposed LLR approach with the conditional jamming probability computation is presented. Section IV explains how to approximate the conditional probability of jamming. Results are presented in Section V, followed by concluding remarks in Section VI.

II. Preliminaries

A. PHY Jammer Models

Protection against an adversary is not possible if the adversary has unlimited resources. Hence, we assume that the adversary must operate under a set of constraints. A fully modeled adversary must have assumptions, goals, and capabilities [14]. Although there are numerous categorizations of jammers in the literature, the PHY jammer models can be summarized in the following two categories [2], [15].

1) Constant jammers: As their name suggests, constant jammers continuously emit disruptive signals over the communication medium. Constant jammers are primitive and often can be detected through the radio signal strength indicator (RSSI) component of the receiver. Simple measures such as frequency hopping can be taken as a precaution against these types of jammers [16]. Moreover, constant jammers are power inefficient, which limits their ability to be mobile.

2) Reactive jammers: As a power-efficient and more intelligent alternative, reactive jammers emit signals only when it senses a legitimate transmission taking place. This type of jammer causes a signal collision at the receiver that disrupts either part of or all of the frame. Prevention techniques for these types of jammers include interference and RSS sampling [17]. Carefully engineered, smart, reactive jammers are the most challenging type of jammer [18].

Usually, the error correction algorithms embedded in the PHY can be considered as a first response against such undesired attacks. However, as the error-correcting codes (ECCs) are standardized, their error correction capability is known to the adversary. Therefore, a jammer can corrupt just enough amount of transmission to cause the decoding to fail, eventually causing a DoS.

B. Channel model

Every soft-information decoder requires LLR as an input which determines the hard output value of each received signal, and also acts as a measure of *reliability* for those signals. In regular conditions, a larger LLR magnitude indicates more confidence in the received signal.

Let b^n, a binary channel input of length n, be modulated using binary phase-shift keying (BPSK) with the mapping

$$b^n \in \{0,1\}^n \rightarrow x^n \in \{+1,-1\}^n,$$

where x^n is the modulated channel input variable sequence. Assuming equiprobable symbols and IID noise, given a realization of the received signal, $y^n = (y_0, y_1, \cdots, y_{n-1})$, the LLRs can be calculated per-bit as

$$L(y_i|A) = \frac{2y_i}{\sigma_A^2}, \text{ for each } i \in \{1, \ldots, n\}, \tag{1}$$

where i indicates the bit index of the received frame, the conditioning on A indicates it is an AWGN channel without jamming, and σ_A is the standard deviation of the channel noise.

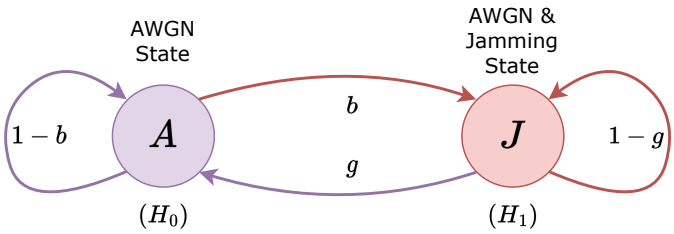

Fig. 1. Two-state Markov chain model for the reactive jammer model, with transition probabilities b and g. The state of the chain for bit i is denoted S_i.

III. Evaluating LLRs Under Jamming

A. Threat Model

The adversary is modeled as a jammer which disguises itself by injecting zero-mean Gaussian noise into the system. It is assumed that the smart jammer can retrieve the modulation and subcarrier frequency of operation and therefore injects jammer signals at the legitimate transmission frequency. In order not to alert RSSI of the transmission system, the jammer interferes only a fraction of the time and does so randomly in a bursty fashion. The occurrence of jamming is modeled as a Markov chain at the level of transmitted bits.

Fig. 1 depicts the two-state Markov chain for the jammed channel model. The state A is AWGN only with zero mean and variance σ_A^2. The J state denotes that jamming is present in the channel, with total variance σ_J^2:

$$\sigma_J^2 = \sigma_V^2 + \sigma_A^2. \tag{2}$$

Here, σ_V^2 is the variance of the signal introduced by the jammer, which is an independent Gaussian random variable. The state transitions are modeled to occur per-bit. The state transition parameters b and g denote the probabilities of passing from the AWGN state to the jamming state and vice versa, respectively. The parameters b, g, σ_J^2, and σ_A^2 can be estimated, and so are assumed known to the receiver.

B. LLR Calculation Under Jamming

Given that a received signal y_i is certainly affected by jamming, then its noise is independent from that impacting other bits and the LLR would be

$$L(y_i|J) = \frac{2y_i}{\sigma_J^2} \tag{3}$$

instead of (1), where σ_J^2 is obtained using (2). In practice, however, the receiver does not have certainty on whether a signal has been impacted by jamming and that induces hidden Markov dependencies in the calculation of the LLRs.

Regardless, the decoder will treat the LLR of each bit as being an independent random variable and so the objective is to provide the best marginal estimate of the LLR of each bit given the jamming uncertainty.

Let $\{S_i\}$ denote the Markov state process, with S_i taking values of A for the AWGN state and J for the jamming state. Then, the conditional probability of the transmitted binary variable B_i at index i being a 0 can be computed as

$$\begin{aligned} p_{B_i|Y^n}(0|y^n) &= \sum_{s^n \in \{A,J\}^n} p_{B_i,S^n|Y^n}(0, s^n|y^n) \\ &= \sum_{s^n \in \{A,J\}^n} p_{B_i|S^n,Y^n}(0|s^n, y^n) p_{S^n|Y^n}(s^n|y^n) \end{aligned} \tag{4}$$

taking the entire received signal into account and accordingly, its marginal LLR would be

$$L(y_i) = \ln \frac{p_{B_i|Y^n}(0|y^n)}{p_{B_i|Y^n}(1|y^n)} \tag{5}$$

which can be expanded to incorporate the jamming uncertainty using equation (4).

Given the received signal sequence y^n, the conditional probability of a jamming sequence $s^n \in \{A, J\}^n$ can be computed as

$$p_{S^n|Y^n}(s^n|y^n) = \frac{f_{Y^n|S^n}(y^n|s^n) p_{S^n}(s^n)}{f_{Y^n}(y^n)}. \tag{6}$$

where f is the probability density function (PDF). As the noise is independent of the channel states, we have that

$$f_{Y^n|S^n}(y^n|s^n) = \prod_{i=1}^{n} f_{Y|S}(y_i|s_i). \tag{7}$$

Incorporating (7) into (6), we get

$$p_{S^n|Y^n}(s^n|y^n) = \frac{\prod_{i=1}^{n} f_{Y|S}(y_i|s_i) p_{S^n}(s^n)}{f_{Y^n}(y^n)}, \tag{8}$$

where s^n ranges over 2^n possible jamming sequences. The probability of a received signal at an arbitrary index i being in the J state can be evaluated from (6) as

$$p_{S_i|Y^n}(J|y^n) = \sum_{s^n \in \{A,J\}^n : s_i = J} p_{S^n|Y^n}(s^n|y^n). \tag{9}$$

The brute force evaluation in (9) requires a burdensome 2^{n-1} computations, so in the following section we propose an efficient estimation technique for the marginal probability of jamming. Moreover, for reduced computation, we employ a linear approximation to the full LLR computation unconditioned on jamming state:

$$\hat{L}(y_i) = L(y_i|A) p_{S_i|Y^n}(A|y^n) + L(y_i|J) p_{S_i|Y^n}(J|y^n). \tag{10}$$

IV. Approximating the Conditional Probability of Jamming

A. The Impact of False Positives/Negatives on BLER

The collected statistical data, which is the received signal in our case, may lead to incorrect conclusions in terms of misidentifying the A and J states. Therefore, it is essential to assess the impact of false positives and false negatives on the BLER performance.

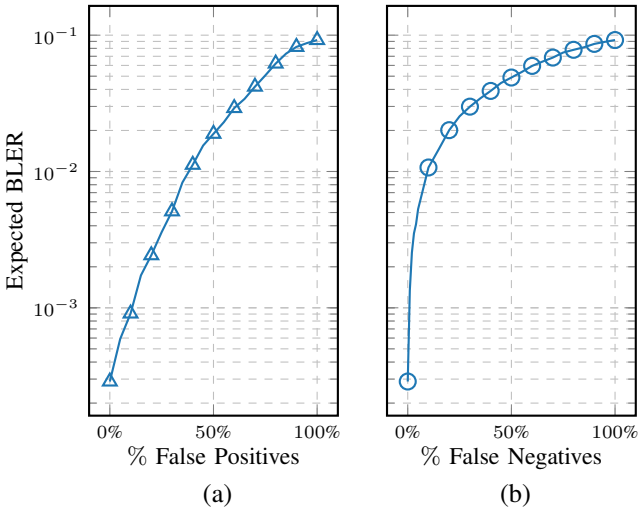

Fig. 2. The quantified impact of (a) false positives and (b) false negatives on the BLER performance, using RLC$[128, 105]$ with the ORBGRAND algorithm.

False positives occur when a non-jammed index is mistaken for being jammed. In this scenario, $L(y_i|J)$ in equation (3) is used instead of $L(y_i|A)$ in equation (1) for the mistaken index i. False negatives occur when a jammed index is mistaken for being non-jammed and $L(y_i|A)$ is used instead of $L(y_i|J)$ for the mistaken index i.

To understand and quantify the impact of mistaking the events on the BLER performance, a set of genie-aided simulations is carried out. A random linear code RLC$[n, k]$ = RLC$[128, 105]$ is used as an example where n denotes the code length and k denotes the code dimension, and the universal ORBGRAND algorithm is used to derive the BLER performance. The state information for each received bit is provided to the genie-aided decoder, therefore, $L(y_i|A)$ is used for indices belonging to state A, and $L(y_i|J)$ is used otherwise. To quantify the impact of false positives, BLER is measured when $L(y_i|J)$ is used for a proportion of indices that belong to state A. Similarly, to quantify the impact of false negatives, BLER is measured when $L(y_i|A)$ is used for a proportion of indices that belong to state J.

Fig. 2 presents the simulated BLER performance for the percentage of false positives (a) and false negatives (b). The SNRs for the AWGN channel and the jammer are selected as $\text{SNR}_A = 12$ and $\text{SNR}_J = 0$ dB, respectively. In both performance assessments, it can be observed that the BLER performance degrades as the number of errors increases. However, the degradation with false negatives is far more severe than the degradation with false positives. For instance, 5% of false negatives has the same amount of impact on BLER performance as about 40% of false positives. This means that the correct identification of jammed indices is far more important than the incorrect identification of the non-jammed indices, and our algorithm should prioritize identifying jammed indices

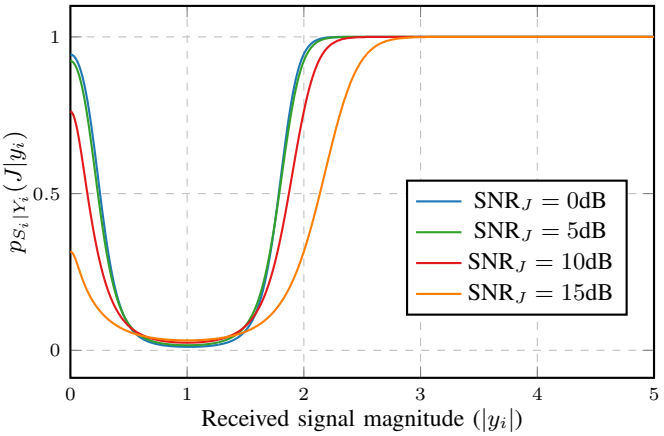

Fig. 3. $p_{S_i|Y_i}(J|y_i)$ as a function of received signal magnitude, $|y_i|$, based on (12). The SNR of the AWGN channel is fixed at SNR$_A$ = 12 dB, and several probabilities are depicted based on various jamming SNRs.

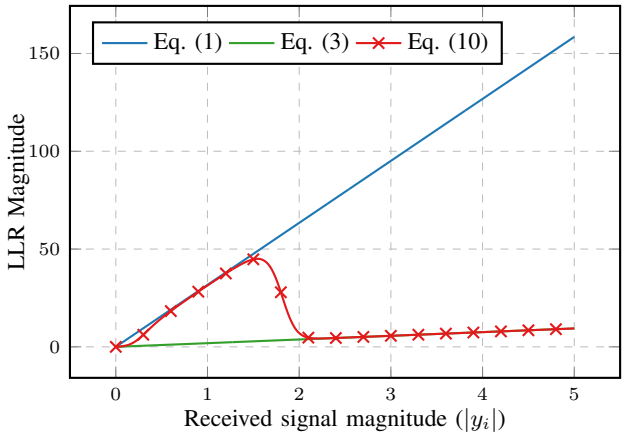

Fig. 4. LLR magnitudes based on AWGN only (1), jamming only (3), and proposed approach (10) using the first approximation to marginal conditional jamming probabilities. The SNRs of the AWGN channel and the jamming channel are fixed at 12 dB and 0 dB, respectively.

correctly.

B. Calculating the Jamming Probability

The estimation of probability of jamming is performed in two steps. In the first step, an initial estimate of the probability that the i-th bit experienced jamming, $p_{S_i|Y^n}(J|y^n)$, is derived based on the marginal distribution given y_i alone $p_{S_i|Y_i}(J|y_i)$. Then, using the Markov state transition probabilities, the probability of jamming for specific indices neighboring those with high jamming likelihoods are recomputed to improve the estimates of their probabilities.

The sign of a received signal y_i does not have an impact on $p_{S_i|Y_i}(J|y_i)$. Hence, we consider a new random variable, $|Y|$, that is based on the magnitude of Y. In this case, the new random variable is a folded Gaussian distribution with PDF, $f_{|Y|}(|y_i|)$, equal to

$$\frac{1}{\sigma\sqrt{2\pi}}\left(\exp\left(\frac{-(|y_i|-1)^2}{2\sigma^2}\right)+\exp\left(\frac{-(|y_i|+1)^2}{2\sigma^2}\right)\right) \quad (11)$$

for $0 \leq i < n$. In the first step, our estimate of $p_{S_i|Y^n}(J|y^n)$ is

$$p_{S_i|Y_i}(J|y_i) = \frac{f_{|Y||S_i}(|y_i||J)p_{S_i}(J)}{f_{|Y|}(|y_i|)}. \quad (12)$$

The conditional PDF expression in (12) can be obtained by substituting the jamming variance in the expression in (11). Using the law of total probability, the PDF at the denominator in (12) is expanded as

$$f_{|Y|}(|y_i|) = \sum_{s_i\in\{A,J\}} f_{|Y||S_i}(|y_i||s_i)p_{S_i}(s_i). \quad (13)$$

Substituting (11) and (13) into (12), the first approximation for the conditional probability of bit i having experienced jamming can be calculated.

Fig. 3 presents $p_{S_i|Y_i}(J|y_i)$ as a function of the received signal magnitude $|y_i|$. It is minimized at the absolute value of the BPSK constellation point, 1, and is maximized as the received signal magnitude drifts away from the constellation. Note that the $p_{S_i|Y_i}(J|y_i)$ takes the stationary probability of jamming at the constellation point since there is always a chance that the received signal could be a result of jamming.

Fig. 4 depicts LLR magnitude trend lines based on AWGN and jamming conditions, as well as the proposed LLR computation (10) when the first approximation $p_{S_i|Y_i}(J|y_i)$ (12) is incorporated. With increasing signal magnitude, the proposed method switches from the AWGN LLR trend line toward the jamming LLR trend line. This behavior reduces the strength of the LLRs at higher magnitudes as a result of the suspicion of jamming, which is then evaluated at soft-information decoders as a less reliable bit index. Consequently, such indices are naturally prioritized for correction, in attempts to identify the transmitted codeword.

When the jammer yields signal magnitude that is great enough to come under suspicion $p_{S_i|Y_i}(J|y_i)$ is a good estimate of $p_{S_i|Y^n}(J|y^n)$, as demonstrated in Fig. 3 and Fig. 4. On the other hand, solely relying on the signal magnitudes would not allow us to detect a substantial portion of the jammed indices as indices with signal magnitudes close to the constellation point would mostly be inferred to be as non-jammed, which is a major limiting factor on the performance improvement.

To tackle this issue, we take advantage of the burstiness of the two-state Markov chain. If an index i has a low initial $p_{S_i|Y_i}(J|y_i)$ value, but is neighboring an index $i \mp 1$ that has sufficiently high value, as governed by a threshold, then our estimate of $p_{S_i|Y_i}(J|y_i)$ is increased using a heuristic. This is illustrated in Fig. 5 for a sequence of signals. On the top, the sequence S^n represents the Markov state of a series of indices and is hidden from the receiver. The receiver calculates $p_{S_i|Y_i}(J|y_i)$, from which it determines a subset of indices that have a relatively high values. The indices at which $p_{S_i|Y_i}(J|y_i)$ yields a significantly high value are called *anchor indices*. Using the Markov chain state transition

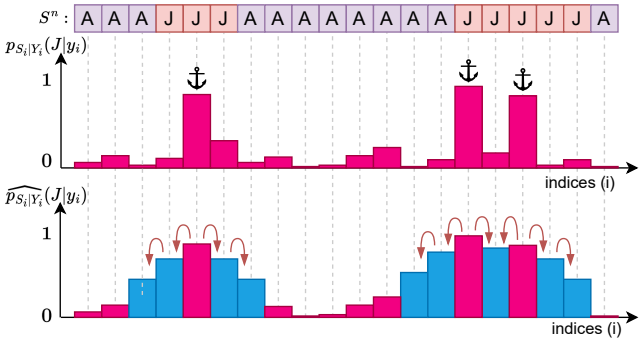

Fig. 5. Example state transition probability and their associated $p_{S_i|Y_i}(J|y_i)$. Indices with high $p_{S_i|Y_i}(J|y_i)$ values are designated as anchor indices (represented with the anchor symbol) and Markov chain state transition probabilities are used to recalculate $p_{S_i|Y_i}(J|y_i)$ for the neighboring indices resulting in a better estimate, $\widehat{p_{S_i|Y^n}}(J|y^n)$.

probabilities, the $p_{S_i|Y_i}(J|y_i)$ for the indices adjacent to these anchor indices can be recalculated recursively. As a result, we derive a new, improved set of jamming probability estimations, $\widehat{p_{S_i|Y^n}}(J|y^n)$ for $i \in \{0, \ldots, n-1\}$.

In order to reconsider the jamming probability of an index, it must either be neighboring to an anchor index or be sandwiched between two distinct anchor indices. Otherwise, the initial $p_{S_i|Y_i}(J|y_i)$ is used.

1) Index Neighboring to a Single Anchor Index: In the first case, the index of interest neighbors an anchor index on one side and a non-anchor index on the other. For simplicity, let us consider the subject index i and the anchor index $i-1$. Using the Markov property, we create an updated $\widehat{p_{S_i|Y^n}}(J|y^n)$ from its anchoring neighbour. Assuming the anchor is in the $i-1$ position, using the Markov property we set

$$\widehat{p_{S_i|Y^n}}(J|y^n) = bp_{S_{i-1}|Y_{i-1}}(A|y_{i-1}) + (1-g)p_{S_{i-1}|Y_{i-1}}(J|y_{i-1}). \quad (14)$$

2) Index Neighboring to Two Anchor Indices: Similar to (14), we derive the updated jamming probability for an index that is in between two anchor indices. For the subject index located at i, the anchor indices are at $i-1$ and $i+1$. Unlike the previous case, the new probability is conditioned on two different states. Based on the values of $p_{S_{i-1}|Y_{i-1}}(J|y_{i-1})$, $p_{S_{i+1}|Y_{i+1}}(J|y_{i+1})$, b and g values, again using the Markov property $\widehat{p_{S_i|Y^n}}(J|y^n)$ is expressed as:

$$\begin{aligned}\widehat{p_{S_i|Y^n}}(J|y^n) = \\ &\frac{(1-g)(1-g)}{(1-g)(1-g)+bg} p_{S_{i-1}|Y_{i-1}}(J|y_{i-1})\ p_{S_{i+1}|Y_{i+1}}(J|y_{i+1}) + \\ &\frac{(1-g)}{(1-g)+(1-b)} p_{S_{i-1}|Y_{i-1}}(A|y_{i-1}) p_{S_{i+1}|Y_{i+1}}(J|y_{i+1}) + \\ &\frac{(1-g)}{(1-g)+(1-b)} p_{S_{i-1}|Y_{i-1}}(J|y_{i-1}) p_{S_{i+1}|Y_{i+1}}(A|y_{i+1}) + \\ &\frac{bg}{bg+(1-b)(1-b)} p_{S_{i-1}|Y_{i-1}}(A|y_{i-1}) p_{S_{i+1}|Y_{i+1}}(A|y_{i+1}).\end{aligned} \quad (15)$$

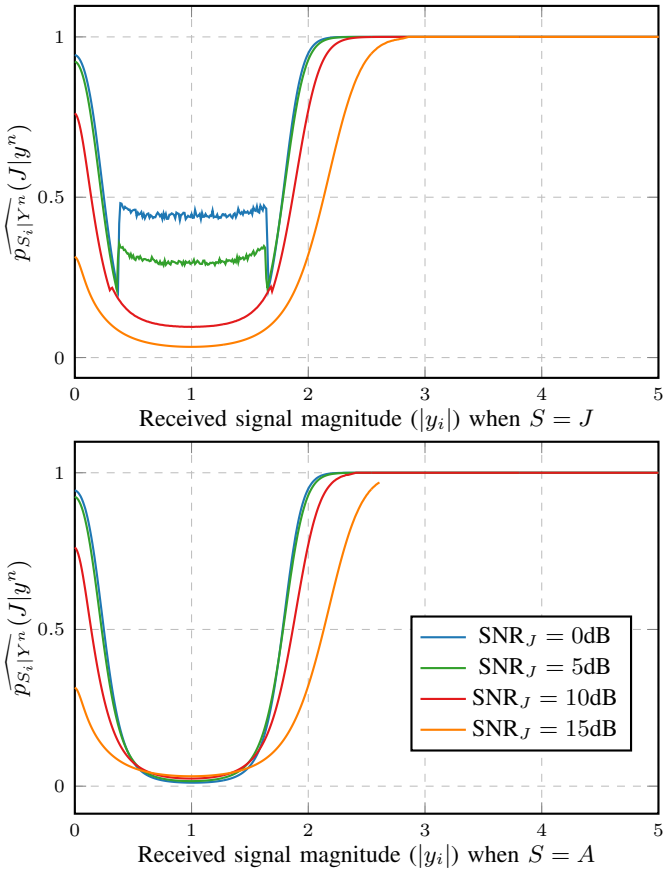

Fig. 6. Simulated $\widehat{p_{S_i|Y^n}}(J|y^n)$ based on the received signal magnitude, when $S = J$ (top) and $S = A$ (bottom). The SNR of the AWGN channel is fixed at SNR$_A$ = 12 dB. All parameters are kept the same as in Fig. 3.

One possible drawback of estimating $p_{S_i|Y^n}(J|y^n)$ from $(p_{S_1|Y_1}(J|y_1), \ldots, p_{S_n|Y_n}(J|y_n))$ based on temporal correlation is the risk of increasing the number of false negatives, especially at non-jammed indices neighboring jammed indices. These false negatives could potentially have a negative impact on performance. However, as discussed in Section IV-A and as presented in Section V, their impact on BLER performance is negligible.

V. Simulation Results

The proposed jamming-aware LLR calculation using $\widehat{p_{S_i|Y^n}}(J|y^n)$ is evaluated. The state transition probabilities are set to $b = 0.01$ and $g = 0.25$, referring to an overall stationary jamming probability of $\frac{b}{b+g} = 3.84\%$. The SNR for the AWGN state is set as SNR$_A$ = 12 dB. An empirical threshold probability of 0.2 is used to derive the anchor indices, and the neighboring indices are re-evaluated recursively, *i.e.* until the estimates $\widehat{p_{S_i|Y^n}}(J|y^n)$ of $p_{S_i|Y^n}(J|y^n)$ of the neighboring index fall below the threshold.

Fig. 6 visualizes $\widehat{p_{S_i|Y^n}}(J|y^n)$ when the ground truth is $S = J$ (top) and $S = A$ (bottom) with respect to the received signal magnitude of an arbitrary index i. Distinct than Fig. 3, the statistics from states A and J states are kept separate to demonstrate the impact of Markov state transitions. All

other parameters are kept the same as in Fig. 3. Compared to Fig. 3, the estimate of $p_{S_i|Y^n}(J|y^n)$ near the constellation point has increased significantly for all considered SNR_J values when $S = J$. This means that the amount of false negatives that originally arise with using (12) solely has decreased significantly. In return, the estimate of $p_{S_i|Y^n}(J|y^n)$ when $S = A$ has not changed significantly compared to the first approximation in Fig. 3. Therefore, false positives due to leveraging temporal correlation with the neighboring indices is negligible.

Fig. 7 presents the BLER performance comparison using RLC$[128, 105]$ and 5G NR CA-Polar$[128, 105]$. The ORB-GRAND algorithm [12], [13] is selected to evaluate the performance of selected codes, since it is a universal soft-information decoder that allows to evaluate distinct codebooks. Moreover, despite its recent introduction to the literature, several works report the practicality of its algorithm family with demonstrated circuit implementations [19]–[21]. The jammer SINR represents the legitimate transmission power to the jammer interference power ratio, *i.e.* low SINR indicates a powerful jammer. For both comparison scenarios, the performance using the regular LLR approach (1) is the baseline BLER. The red curves represent the proposed approach using $\widehat{p_{S_i|Y^n}}(J|y^n)$. The BLER performance for $p_{S_i|Y_i}(J|y_i)$ without using Markov chain state transitions in (14)-(15) is also shown as a reference. The baseline performance shows that a strong jammer yields a BLER close to 1, *i.e.* almost no packets can be decoded, therefore causing a DoS. The proposed LLR computation (10) using $\widehat{p_{S_i|Y^n}}(J|y^n)$ is shown to improve the baseline BLER performance by an order of magnitude at the DoS region, *i.e.* about 9 out of 10 packets can be decoded correctly despite the strong jammer interference. The proposed approach demonstrates 2.7 dB SINR gain at a BLER of 10^{-2} and 0.75 dB gain at a BLER of 10^{-6} for both codes. Note that the high SINR values indicate weak jammers which are not typical since they can only degrade the performance marginally and cannot cause a DoS. Nonetheless, the proposed approach is shown to outperform the baseline even in the high SINR region.

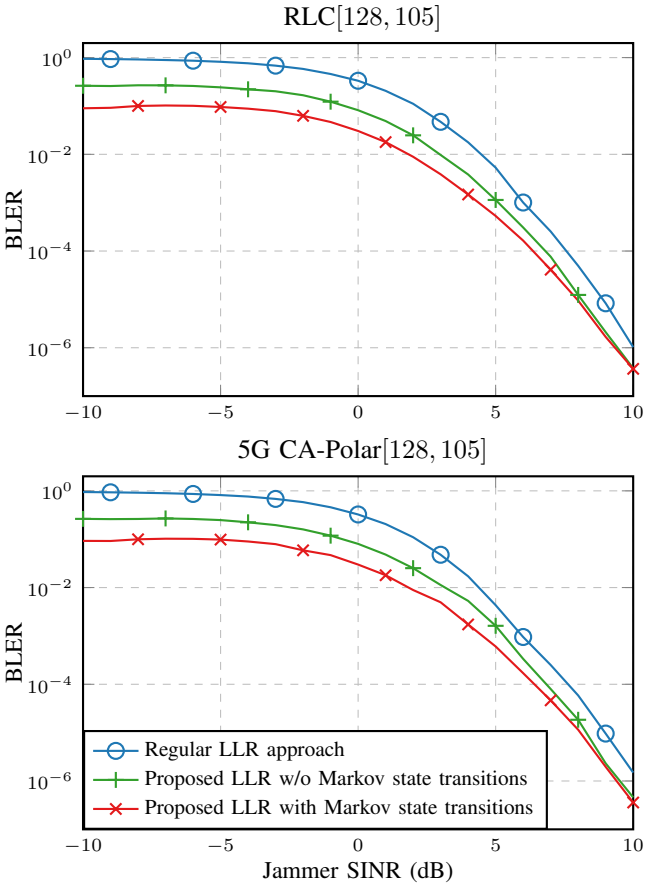

Fig. 7. BLER comparison of the proposed approach against conventional LLR, with respect to jammer SINR, using RLC$[128, 105]$ (top) and 5G CA-Polar$[128, 105]$ (bottom) codes. The SNR of the AWGN channel is fixed at $\text{SNR}_A = 12$ dB.

VI. Conclusion

In this work, a novel and general physical layer security approach against a smart bursty jammer is developed. First, the adversary is modeled as disguised in the channel as a Gaussian variable with zero mean. In addition, the overall active duration for the jammer is determined by a two-state Markov chain with low interference time to avoid RSSI detection. To tackle this challenging model, we proposed a new approach based on LLR calculation under adversarial constraints, to improve the BLER performance. The new LLR calculation is based on a conditional probability of jamming, calculated using the received signal and the Markov chain state transition probabilities. The proposed approach is implemented prior to decoding and works with any soft-information decoder. Simulation results with the universal ORBGRAND algorithm using RLC$[128, 105]$ and 5G CA-Polar$[128, 105]$ codes show that the proposed solution can substantially improves the reliability estimates for the received signals, preventing denial of service, and yields a substantial SNR gain of up to 2.7 dB. Future work includes further improvement of jamming detection accuracy, and comparing with other available soft-information decoders.

Acknowledgements

This work was partially supported by Defense Advanced Research Projects Agency Contract number HR00112120008 and by National Science Foundation ECCS Award numbers 2128517 and 2128555. The content of the information does not necessarily reflect the position or the policy of the US Government, and no official endorsement should be inferred. This publication has emanated from research supported in part by a grant from Science Foundation Ireland under grant number 18/CRT/6049. The opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Science Foundation Ireland.

REFERENCES

[1] C. Orakcal and D. Starobinski, "Jamming-resistant rate adaptation in Wi-Fi networks," *Perf. Eval.*, vol. 75, pp. 50–68, 2014.

[2] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surv. Tutor.*, vol. 13, no. 2, pp. 245–257, 2011.

[3] F. M. Turner, E. Ottoboni, and A. Imada, "Noise quality optimizes jammer performance," *Electronic Warfare Magazine*, vol. 9, no. 6, pp. 117–119, 1977.

[4] M. A. Gawas and R. Tambi, "Data rate adaptation algorithms survey for IEEE 802.11 networks," in *CTCEEC*, 2017, pp. 926–932.

[5] C. Orakcal and D. Starobinski, "Jamming-resistant rate control in Wi-Fi networks," in *IEEE GLOBECOM*, 2012, pp. 1048–1053.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] H. Chen and Y. Ghasempour, "Malicious mmWave reconfigurable surface: Eavesdropping through harmonic steering," in *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*, 2022, p. 54–60.

[8] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[9] Y. Shi, X. Lu, Y. Niu, and Y. Li, "Efficient jamming identification in wireless communication: Using small sample data driven naive bayes classifier," *IEEE Wireless Communications Letters*, vol. 10, no. 7, pp. 1375–1379, 2021.

[10] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine learning-based jamming detection in wireless IoT networks," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, 2019, pp. 1–5.

[11] B. Upadhyaya, S. Sun, and B. Sikdar, "Multihypothesis sequential testing for illegitimate access and collision-based attack detection in wireless IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11 705–11 716, 2021.

[12] K. R. Duffy, "Ordered reliability bits guessing random additive noise decoding," in *IEEE ICASSP*, 2021, pp. 8268–8272.

[13] K. R. Duffy, W. An, and M. Médard, "Ordered reliability bits guessing random additive noise decoding," *arXiv:2202.13951*, 2022.

[14] Q. Do, B. Martini, and K.-K. R. Choo, "The role of the adversary model in applied security research," *Comput. Secur.*, vol. 81, pp. 156–181, 2019.

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *ACM MobiHoc*, 2005, pp. 46–57.

[16] R. T. Yazicigil, P. Nadeau, D. Richman, C. Juvekar, K. Vaidya, and A. P. Chandrakasan, "Ultra-fast bit-level frequency-hopping transmitter for securing low-power wireless devices," in *IEEE RFIC*, 2018, pp. 176–179.

[17] M. Strasser, B. Danev, and S. Čapkun, "Detection of reactive jamming in sensor networks," *ACM Trans. Sens. Netw.*, vol. 7, no. 2, pp. 1–29, 2010.

[18] N. V. Huynh, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, and M. Mueck, "Defeating smart and reactive jammers with unlimited power," in *IEEE WCNC*, 2020, pp. 1–6.

[19] A. Riaz, V. Bansal, A. Solomon, W. An, Q. Liu, K. Galligan, K. R. Duffy, M. Médard, and R. T. Yazicigil, "Multi-code multi-rate universal maximum likelihood decoder using GRAND," in *IEEE ESSCIRC*, 2021, pp. 239–246.

[20] S. M. Abbas, T. Tonnellier, F. Ercan, M. Jalaleddine, and W. J. Gross, "High-throughput and energy-efficient VLSI architecture for ordered reliability bits GRAND," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 6, pp. 681–693, 2022.

[21] C. Condo, "A fixed latency ORBGRAND decoder architecture with LUT-aided error-pattern scheduling," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 69, no. 5, pp. 2203–2211, 2022.