Covert and Reliable Short-Packet Communications against A Proactive Warder

MMahiin\Wangi, Yao Yao[†], Bin Xia[†], Zhiyong Chen[†] and Jiangghou\Wangig[†]

† Dépenanne no o Eletarouic Enginearing, Shanghai Jiao TonggUitic xisity Shibnghgha Chabaina

† Sélichballo Engineering, University of Kent, Claute blum, yUKK.

En Enhalf: {\wangganhilin, sandywao, bxia, zhiyongehen}}@sjtueeducnii; i.wang@Rentacaekuk

Abstract+-Wireless-short-packet communications pose challenges to the security and reliability of the transmissions Besides, the siproactive warder compounds the so challengese who litetects and interferes with the potential transpossional Americas jamming channéhia introduced by the proactive war derecomparéd with the passive one resulting anothe inapplicability of analytical inethids and are sults alimness it in a works; all thus n effective system. design schemes ayetrequiredgloseshort-packet communicationst-against then proactive wardens Tot laddress: this vissue, we consider the analysis and design of covert and reliable transmissions for above systems. Specifically, to investigate 3 he rightable, and covery performänke of the system editection erroth probability dated towarder and decoding terror reprobability detable neceiver are derived, which is affected by dooth the whatsmit above and the flamining powert Eurthermoreketommaximizewhe Effectiventhroughputeianzoptie milization frameworktis proposed under reliability and covertness constraints.bNitmeridal oresults serifys the accultacy of cahalytical results tand atherfeasibilityrofly headptimization draineworkibilitis shown that in deoff detween transmission are liability dand bovertness is changed by the pitoactive warden compared with the plassive one; Besides; it is shown that longerablock lengt Bis always beneficial to improve the khroughput for systems with optimized transmission pates: But when transmission rates are fixed athe Blocklength should becarefully designed since the maginum one isenotroptimal cisigthis casee the maximum one is not optimal in thiIndexe Terms-covert and reliable transmission, short-packet communications, proactive dvarder, leffective throughputt-packet communications, proactive warder, effective throughput

I. Introduction

Time-sensitive and missibh child in the fifth-generation applications baye aroused great attention in the fifth-generation notife communications systems [2]. The user of short packets meats, the stringent low batteney requirements, but an accept this inacoding gain exists with short packets posing challenges do transmission speliabilityse Besidess massive agrifuent exessages are transmission speliabilityse Besidess massive agrifuent exessages are transmission speliabilityse Besidess massive agrifuent exessages are transmission swip last lenguages to transmission as autity of the exposure of atransmission behaviors may be important productions of a transmission behaviors for this bisage my bicki provents the transmission behaviors from being the post of the communication of ferson behaviors from being the post of the communication of the filter and that a communication of the filter and deniably over n channel use. In addition,

This work is supported in part by the National Natural Scient-This Foods distinguished by the National Natural Science Housidation bis China winder Science 62271 309 chando Shanghajor Municipal usudencer and Technikity Majtir Exoject under grant 2021 SHZDZX0102.

coffshdering dag envel two rim finication; with short neekets. [?] three stigated the effective throughput of the system in additive white: Gaussian chiology (AWGN) echablic lso Similar that the basis-Ened dhittachievabilitle:bounds.on: thermaximal channel coding sater at pagivers, blockleveshiga dedrrith profibility over AAMGIN channelsysfamadditionlitt@, whitenvestigated athesethrol@fgout overngelasiSstatilenfadjifg (chandels; drevealing ethe) ifundamental difference in the design betweengthe tease of gives i-static leading chahner and thatabiliaW GNrc Nahitely More going lex adelitions With?multiple:gwarders,eminitisantennao veurces sand atimfanined abriah vehicle vaided goe tworks; swerenconsidered deire (2), [2], [3], delign warderein the aforementioned-sworks fischnagsivbawhe aims the detect AMeCransmission behaviours while contadegrading the liquidity of leonmunication rehannels.c Different rimon rithe pessave valaider, athle-proective kanev behaves sidore diangerous ly, This is because the proactive warder can not only detect the Clasing less detrains this sibre ibentals we de mitrho is en assimtent dre with the detential transmission or inheltaneously of lile In of? then proaktive (warden litas of insiderednin the relationatelor Riffwhere the beliaviors of the tradesmitter and the warder lwere modeled danthermoslycobbisrative egame.tlin padditione f@rdnvestigated thely is suesc to flapowere leon trol ninn their odevlicet-to-keevigeit covere communication in the consisting of aspecative lwarders ly [?] Hbw@era theoantilysisvandercorrespondingredstembdesigns aboutoths, prohetive the ardenia vi(2); [2], t[2] were shasteroused ihfeniteablecklengthrasdelightion, the high isonoplengeves uitable for abortipacket transmissiond Blesidesucher results from the isystem whithi quassive ewarders (2), [2] m(2) m(2) a f(3), care tnoube directly applied torthe system with the proactive warder, since and there jamenting alinky exists abetween stheroward eryand at the desiris abtion irrhaddition (to covanulmidation), and, defection linksed his compounds the challenges of thoth reliability and coverness ismi shibit-packeto dopamberications n i Shereforesi deffective resholts packet bransatissioni tlesigas schenaesl to spriby (de, both Teliability and coverinessy guaranteestard still yopem issues, the proactive waToladdress: this ris the, rinjahis maper liwle considerative analysis and design of teliable and covert transmissions against a proact tivel wlatderti-Sipeliifically[ltis guaranteendhe tsystemaldougeness hequiremental, ithe average veletees ionner for probability out the wardenis. delivedfoBesidffs;ctovfacilitatepsystemtanalysissand detimizationmenteiserappheximationliexphassiondiscalsot pres pased which is tighter than the widely used Kullback-Leibler (KD) didelrgeacehappisaximation his existing works siderovent

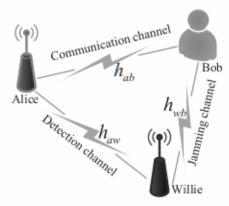


Fig. 1. Covert und deliable benominication by stery against gap noticipe oward en war der.

communications. To guarantee the reliability requirement, the avelugis depotatesiemor brobiability and the vectores rais raissives. Farthernore; cartoprimization Sportlere 4s, formulared tand the SOM MERCANOS TRANSESSORIA DE BIODOS É LOS YMEREMISES INTÉRIEMENTOS umobahibity ortutales vsterde with derivatility anideover fasilitate strainty by strainty adds ignition that transport dower pransimastion rater and blockleheth PNumerical whitelarions before the right neislebt une proposed appreixtmations alicente reas in the proposed in the biobolycycoting zamole framework governmentications. To guarantworathon: reliabilitie megatisomen varthe observer CN (odirig denotes rehabilitaries daussen versimbleron with relear mean and optimization. Problem is dermalated annivant optimizat. to(n) framework isexp (p.4890) to denotes zentho nifection throughput of it be notes the vish reliabilition and cover tress quinstraints devicements designifications de la company de in ission range blocklength. Numerical simulations verify $\psi(x) \equiv \frac{dx}{dx}$ denotes the digamma function while $\psi(x)$ the tightness of the proposed approximations and the denotes its n-th derivative $E(x) = \frac{dx}{dx}$ denotes the feasibility of the proposed optimization framework for the exponential integral function.

Notation: |-| dehocsystem Modilite value operator. A. Signal denotes the models. Gaussian distribution with zero mean and variance σ^2 . $\Pr(\cdot)$ denotes the probability As shown in Fig. 4. a covert wireless communication of an event. $O(x) = \int_{-\infty}^{\infty} \frac{1}{x} \int_{-\infty}^{\infty} \frac{1}{x$

In one transmission round. Alice transmits n covert signals $X_a[i], i \in \{1, \cdots, n\}$ to Bob, while Willie sends n jamming signals how [i] in Fig. [[12-covert]] w Bekide sort will inconficute on received signals be detected to the other transmit Africe (has items smitted signals without sanguait power rote Africa (Boldenote de ascepting a full in plet N ($0 \in M_a$) (Willie) in that N are the financial power of Willie is plenoted in N and N and N are defined as N and N are defined as N and N and N are defined as N and N and N as shown N and N are defined as N and N are defined as N and N are defined as N as shown N and N are defined as N as N and N are defined as N and N are defined

anthenwirelessuchamtelsalfrompAtico to Boha (com (detication ahangamming) Affect to Willie (detection channel, h_{aw}) and Willie dock obeginnising schannel, h_{a} bicarct subject to the quasit station Rayleight fadifity. [2]. Specifically, while Willie, sands h_{a} jamming (statal) and h_{a} jamming (statal) and h_{a} jamming (statal) and h_{a} jamming conclusions trained collifiction resembles collifiction are instructed and are independently and deficically statistic bated (i.i.d. Advisoring different rounds. The line tantaneous whether it is somitation (GSI) draming unavailable for Wallice is indenWillie docs protocol operate with Alice as awarders arise hood Willie the Batistical USI is absented be estimated as a Wadders arise hood Wille the Batistical USI is absented be estimated as some operate with Alice as a Wadders arise hood Willie the Batistical USI is absented be estimated as some operate with a dissipation of the distinct of the dissipation of the distinct of the

B. The wireless channels from Alice to Bob (communication channel, h_{ab}). Alice to Willie (detection channel, h_{aw}) In order to detect the presence of covert communications and Willie to Bob (jamming channel, h_{aw}) are subject to Willie must distinguish between the following two hypotheses the quasi-static Hayleigh fading [1]. Specifically, $h_{ab} \sim 10^{\circ}$ (0, λ_{ab}), $h_{aw} \sim 10^{\circ}$ (0, λ_{aw}) and $h_{wb} \sim 10^{\circ}$ (0, λ_{aw}). The channel coefficients is independently and alignment transmission round, and are independently and alignment transmission round, and are independently and alignment as mission round, and are independently and alignment as not channel state miorimation (CSI) h_{aw} is unavailable for transmitted. H. denotes the alternative hypothesis where Alice has not channel state miorimation (CSI) h_{aw} is unavailable for transmitted. H. denotes the alternative hypothesis where Alice has not channel state miorimation (CSI) h_{aw} is unavailable for transmitted. H. denotes the statistical CSI is a play to be estimated through the statistical CSI is a play to be stimulated through the jamming signal. H. Sesides, the Willie aradiometer [1], Willie makes a binary decision as instantaneous CSI is available for Willie from a worst case perspective for covert communication.

B. Binary Hypothesis Testing at Willie where T is the average power of each received signal at Willie, In order to detect the presence of covert communications. Willie must distinguish between the following two decisions that infer whether Alice transmits or not.

Nypotheses in each transmission found Suppose there is no prior knowledge for Willie about when Alice will transmit, the priori probability of either hypothesis is equal? Mathematically, the detection error probability of his willie is defined as follows [?], [?], [?], [?], [?], [?]

where \mathcal{H}_{ℓ} (denotes (the $|\mathcal{H}_{\ell}|$) hyperthesis \mathcal{H}_{ℓ} here Alice has not transmitted, \mathcal{H}_{ℓ} denotes the attenuative hypothesis where Alice has transmitted. $y_w[i]$ is the received signal where \mathcal{H}_{ℓ} (denotes the elast alam probability and \mathcal{H}_{ℓ}) denotes the missed detection probability. In covert communications, [Willie in altimates goal in appleted the presence of Alice's transmission with the minimum detection error probability ξ^* , which is achieved by using the optimal detection threshold \mathcal{L}_{τ}^* that minimizes ξ . τ . (2)

C. Effective Throughput with Finite Blocklength where T is the average power of each received signal at Bob can be at Willie, τ denotes the detection threshold, D_0 and expressed as D_1 denote the binary decisions that infer whether Alice transmits $\text{ory}_1[b] = h_{ab}x_a[i] + h_{wb}x_w[i] + n_b[i]$. (4)

Suppose the eigenveryignancy leader of an Ville of the where ξ is the where ξ is the particular and ξ is the probability ξ at Willie is defined as follows [2], [2], [2], [2], [2]

$$\xi \delta(\tau) = \Pr \left(\frac{\ln 2 \sqrt{n} (\log_2 (\frac{1}{1} + \widetilde{\mathcal{D}}_0^b) - \overline{\mathcal{H}}_1^R)}{\Gamma(\mathcal{D}_1 + \mathcal{H}_0) + \Pr (\widetilde{\mathcal{D}}_0^b + \overline{\mathcal{H}}_1)} \right),$$

$$= \Pr \left(T > \sqrt{r} |H_0| / n + \Pr (\widetilde{\mathcal{D}}_1^c + \widetilde{\mathcal{H}}_1) \right),$$
(3)

where $\gamma Pr = (DP_{lo} | h H_{lo})^2 / d(eh Pr | h H_{lo}) | l^2 + far_{lo}^2$ denotes the becoived signal to Bois fratide (SNR) the Bois and Restine transmission Face one a ture on the property of the propert te Sibbe phesqueodin lier orthonorabilion (*?) his affeinisauto flating i channels p(a) be and p(a), the caverage iteresting using probability of isotopied to evaluate the reliability performance. And the effective throughput of the system is given by [?] C. Effective Throughput with Finite Blocklength

When Alice transmits, the received signal at Bob can which quantifies the expected number of information bits that can be reliably transmitted from Alice to Bob.

 $y_b[i] = h_{ab}x_a[i] + h_{wb}x_w[i] + n_b[i].$ III. COVERTNESS PERFORMANCE ANALYSIS

Based on the received signal (??) Bob can decode the in this section, to analyze the coveriness performance of the messages. The decoding error cannot be ignored in short-system, the average detection error probability is denved. packet communications, which is given by [?] With detection threshold τ , the detection error probability

is expressed as [?]/ essed as [?] $\delta = \mathcal{Q} \left(\frac{\ln 2\sqrt{n} \left(\log_2 \left(1 + \gamma_b \right) - R \right)}{\gamma \left(n \sqrt{\frac{\pi}{2}} \right) - \left(\gamma_b \sqrt{\frac{n}{2}} \frac{n\tau}{r^2 + P_a |h_a|_c} |^2 \right)}, \gamma_b \right)$ $\xi(\tau) = 1$ (5)

(7)

where $\hat{\sigma}^a = \varphi P_w^a |h_a b_w^2 / \text{for expression simplification.}$ the receismeesiwiniet annoise ration (Sala roundowinied can isolika transmission matermensured by hits neg changel used begunproblem the property of the problem by fading channels h_{ab} and h_{wb} , the average decoding error probablity+5 Rs adopted to evaluate the reliability performance. And the effective throughput of the system is given by [?]

Notably, from the perspective of Alice, only statistical CSI is available. Therefore, the average detection error probability is delived a stiffes covertness to dujout? her of information bits that can be reliably transmitted from Alice to Bob. Theorem 1. The average detection error probability at Willie with optimal detection threshold under Rayleigh fading channels can be derived as

In this section, to analyze the covertness performance of the system, the average detection error probability is $\operatorname{derived} \pi$

 $\frac{\operatorname{rived} \pi}{BRh\lambda \operatorname{defertion}} \int_{n}^{B} \left(n \frac{n \left(\sigma^{2} + \tan \theta_{i}\right)}{n \operatorname{chold} \tanh \theta_{i} \operatorname{defertion}} \ln \left(\frac{\sigma^{2} + \tan \theta_{i}}{\operatorname{con} \operatorname{cr}^{2} \operatorname{or}} \operatorname{probabilities} \right) \right)$ bility is expressed as [?]

$$-\gamma \left(n, \frac{n\sigma^2}{\tan \theta_i} \ln \left(\frac{\sigma^2_w + \tan \theta_i}{\gamma \left(n, \frac{\sigma^2_w}{\sigma^2}\right)} + \right)\right) \left(\frac{e^{-\frac{R_w}{P_u \lambda_{uw}}} \sqrt{\theta_i \left(\frac{\pi}{2} - \theta_i\right)}}{\Gamma(n)}, \frac{R_w}{\Gamma(n)}\right), \quad (5)$$

where B is the parameter of Gaussian-Chebyshev Quadrature, where $e^2 = (\Phi P_w \cos \frac{2i + 1}{4})^{\frac{1}{2}}$ expression simplification.

Since Willie knows h_{aw} in each round, Willie can adjust $Reof_p$ By a substitution f^{22} to intent? 22 and sensite in each round. probability density function (PDF) of Rayleigh fading channel, the average detection error probability can be expressed as

$$\frac{\overline{\xi}\left(\tau_{7}^{*}\right)}{\overline{P_{P_{a}}}\left(\frac{\sigma^{2}+P_{a}\left|h_{aw}\right|^{2}}{P_{P_{a}}\left(\frac{\sigma^{2}+P_{a}\left|h_{aw}\right|^{2}}{\sigma^{2}}\right)}\right)} \ln\left(\frac{\sigma^{2}+P_{a}\left|h_{aw}\right|^{2}}{\sigma^{2}}\right).$$
(8)

Notably, from the perspective of Alice, of $\frac{n\sigma^2 + x}{\sigma^2}$ attacked CSI is available. Therefore, the average detection error probability is derived as the covertness metric [?].

TlByrsubstitutligex avetag θ into (??) can drapplying a fality iant Chibbys bey [Quadrature detectionabely eshteleral pexpressione] [2]. (32) near/benoblained, anddtheyproofs is completed.

Due to the complicated form of (??), it is intractable to further guide the system design. Thus, a tractable lower approximation of the detection error probability in one transmission round is derived first, and then a lower approximation of the average detection error probability of the remaining of the minimum detection error probability in one transmission round is given by (9) where B is the parameter of Gaussian-Chebyshev Quadrature, and $\theta_i = \frac{e^{-h_n p}}{e^{-\frac{1}{4}n}} \ln \left(\cos \frac{\frac{P_n |h_n p|}{2B}}{2B} \right)$. Proof. By substituting (??) into (??) and considering th probability density function (PDF) of Rayleigh fading Proof:eSethAppendixe? Pletection error probability can be expressed as

The lower approximation of the minimum detection error probability of (??) is tighter than the approximation based on KL divergence (i.e., $\xi^{(n)} = 1 - \sqrt{\frac{1}{2}\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)}$, see Appendix ??/for the detailed definition), which is widely used to evaluate the covertness, performance in the existing works [7], [7]. The

detailed proof is given in Appendix ??. The above concise approximation facilitates the performance of the per By substituting $x = \tan \theta$ into (?/) and applying mance analysis and optimization design for the covert configuration system. It can be used as a metric for the system expression (4, (?/) can be obtained and the proof is expression (1) can be obtained, and the proof is with AWGN channels [?] or the fading channels when only considering one transmission round [?]. Besides, it can also be Didepted the analyzeitheed verage detection ierroripte bability in fadingechannids as followen? dealen. Thus, a tractable lo-Based on The ortion 2 of hel average the tection remon problability an Willians and enjoyed as a follows erived first, and then a lower approximation of the average detection error probability is derived. $e^{-n_n n} - 1$ Theorem 2. $\int \frac{e^{\frac{P_n \lambda_{nw}}{\lambda_{nw}}}}{\text{lower} P_d \text{oper}} \left(1 - \frac{e^{-n} n^n}{\text{ckimaFion}} \right) \ln \left(1 + \frac{x}{\sigma^2 \text{intermediate}} \right) dx$ detection error probability in one transmission round is given $\underbrace{\frac{b_v^{-n}n^n}{\Gamma(n)}e^{\frac{\sigma^2}{P_n\lambda_{aw}}}}_{1-\frac{e^{-n}n^n}{\Gamma(n)}\ln(1+\frac{P_a|\lambda_{aw}|}{\sigma^2})$, $\underbrace{\frac{\sigma^2}{P_a|\lambda_{aw}}e^{\frac{\Gamma(n)}{e^{-n}n^n}}}_{\sigma^2}$, $\underbrace{\frac{\sigma^2}{P_a|\lambda_{aw}}e^{\frac{\Gamma(n)}{e^{-n}n^n}}}_{\sigma^2}$ (12) The expression of average detection error probability (??) and its approximation (??) can be extended to the cov communication scenario with a passive warder by setting Proof. SeBeaidsenthe lower approximation of the detection error probability in one transmission round given in (??) can also be extended to the scenario with a passive warder Group probability of which team replace the approximation hooroxomakibrdiwateryners éte in Ethe existing Dorksostince the proposed concise approximation is figher than the conventional one datoproved the Appendixt 22ss performance in the existing works [?], [?]. The detailed proof is given in Appendix ??. IV_{TIR}ELIABILITY PERFORMANCE ANALYSIS AND SYSTEM formance analysis and optimization design for the covert

collections to tenally a the breliability performance; the

desodingvietro AlbiGbabilitymists derived. t Hardadithe edifications

throughput domaiakimized by riginally soptimizing the Basishist

prowen, the ctransmission drate and three blocklength ewhere cboth the governass and the adiability requirements are considered.

Based on Theorem 2, the average detection error prob-A. Average Decoding Error, Probability at Bob ability at Willie is derived as follows.

Since both the transmit power at Alice and the jamming power at Willie affect) the received SNR at Bob, considering the fading channels, the PDF of SNR can be derived as dx

$$f_{\gamma_{b}}(t) = \frac{d \operatorname{Pr}(\gamma_{b} < t)}{e^{-n} n^{n} dt} \underbrace{\frac{P_{a} \lambda_{aw}}{dt} \operatorname{Pr}\left(P_{a} | h_{ab}|^{2} < tP_{w} | h_{wb}|^{2} + t\sigma_{b}^{2}\right)}_{C} = 1 \underbrace{\frac{P_{a} \lambda_{aw}}{e^{-n} n^{n} dt} \underbrace{\frac{\sigma^{2}}{e^{-n} P_{w}} \lambda_{wb}^{E}(P_{a} | h_{ab}|^{2} < tP_{w} | h_{wb}|^{2} + t\sigma_{b}^{2}\right)}_{(P_{a} \lambda_{ab} \lambda_{wb}^{2} + P_{w} \lambda_{wb}^{E})} \underbrace{\sum_{P_{a} \lambda_{bw}} \underbrace{\sum_{P_{a} \lambda_{bw}} \sum_{P_{a} \lambda_{bw}^{2} \lambda_{bw}^{2} + e^{-n} n^{n}}_{C}}_{(P_{a} \lambda_{ab} + P_{w} \lambda_{wb} t)^{2}} \underbrace{13)}_{(12)}$$

The expression of average detection error probability Based on the linear approximation of Q-function given in [?] and its approximation (?!) can be extended to the [?] and the PDF of SNR given above, the average decoding overt communication scenario with a passive warder by error probability can be derived as setting $F_w = 0$. Besides, the lower approximation of the detection error probability in one transmission round given $\ln_{\epsilon}(??)$ can also be extended to the scenario with a passive warder by setting $P_w = 0$, which can replace the KL divergence approximation widely used in the existing works since the proposed concise approximation is tigher than the conventional one as $pg(\text{yed } \frac{1}{\ln})$ Appendix ??

IV. Reliability Performance Analysis and System Design where this section, to analyze the reliability performance

the decoding error probability is derived. Then, the effrotive throughout is maxinated by jointly optimizing the transmit power, the transmission rate and the blocklength, Where both the coveriness and the reliability requirements ard borabove desult can be extended to the scenario with a passive warder by replacing $P_{\rm F}=0$, and the corresponding Average Lecoding Error probability at Bob average decoding error probability can be simplified as

Since both the transmit power at Alice and the jamming power at With the affect the received SNR, at Boh, consider ing the fading channels, the PDF of SNR can be derived

& Effective Throughput Maximization Optimization

Based of the above analysis, an optimization problem can be formulated to maximize the effective throughput of the system, (slib)out to the other to mb med we onstraints of covertiess reliability, blocklength, and transmit power.

Based on the linear approximation of Q-function given in [?] and the PDF of SNR given above, the average decoding error probability can be derived as (16a)

$$\overline{\delta} \approx \int_{0}^{\alpha - \frac{1}{2\beta}} f_{\gamma_{b}}(t) dt + \int_{n_{min}}^{\beta} \left[\frac{d}{2} \frac{P_{\alpha\beta}^{max}}{f(t - \alpha)} \right] f_{\gamma_{b}}(t) dt + \int_{n_{min}}^{\beta} \left[\frac{d}{2} \frac{P_{\alpha\beta}^{max}}{f(t - \alpha)} \right] f_{\gamma_{b}}(t) dt \tag{16c}$$
(16d)

(16d)

where (16a) and (16b) denote the covertness and reliability constraints with predetermined covertness and reliability requirements & respectively (16c) denutes the transmit power constraints at Alice with the maximum power P_a^{max} . Besides, (16d) denotes the blocklength constraint due to delay require ments and channel coding requirements with the maximum blocklength and the infilming blockl

To solve this optimization problem with coupled optimization variables P_k , R and h, pa joint optimization framework is Thopased eases follows: by higher which cirtholyce martwoylayer process. Marche hinnerslayerg tRe, optimaldtrånsmitr powerdiRg and the obtaind transmission bate | R\(\) are derived without given blocklength $p_{i,\lambda}$ In the outer-layer, the optimal blocklength n^* can be obtained via an exhaustive search over ham, n 15 where P_a^* and R^* are calculated with each value of n. Finally, the grobally optimal solutions P_a^* , R^* and n point be obtained by Ruseabove thannelwork a ruly details are titubertaien bereldem carnherformulatede.towneximizegthen, effective in har oughout of which can stander while the the minimple of ponstraints por sovert normi or lightity; blocklength and transmit powered $\bar{\delta}$ decrease with $P_{a,\text{nand}}$ the effective throughput increases with P_a . After the optimal transmit power P_a^* is obtained, we can obtain the optimal transmission rate R^* as follows 1648verified that the effective throughput is a first-increasing and then-deceasing function of Ra[?]. Consequently, the optimal R^o that maximizes η^a can be effectively calculated using the bisection method. Considering the retrability constraint (??), thberna(tifin) much an sin) scionotrate in Royert cans be added with the solving.ints=with Thuslethenopternal transmission drate in Bility rein $\{R_{ij}^{max}\}$, respectively. (16c) denotes the transmit poOuter-dayeraistagert Chlisideviitgh that then blocklengthver affects the substrainfel()? the (32) and the lobjective function; airis difficult the derive the roptimal solutions directly of Bugexhaustive search owithovere [maximum], the eldebatth optimal solutions form(Ph)mandothdemaxlimum, effective throughput η^* can be obtained we this optimization problem with coupled optimization variables P_a , R and n, a joint optimization framework is pyoposed as followed which involves a two-layer process. In the inner-layer, the optimal transmit polnethis sectione wet provide numerical results to a show that GOVER'S AND SEPARATE FOR THE SECRET PROPERTY OF THE SPECIAL SECRET SEPARATE hication system (against ob preactive awarder.h The i parameter settings, are as followse unless specified atherwised the fading parameters $\lambda_{ob} = 5 \text{Fink} 0^{-2}_{V}$, they gto bally = 0 D time 1 hso AWGNPariances of n ear be Ubtain W), but leself interference wear. quilation spefficient $\phi_{\text{trad}} = 100$, the minimum:blocklangthWhem = i50; tha, maximum:blocklength power =a200e the inaximum transmit (pewer, P_a^{or}), where (V)thet becomes n requirement $\varepsilon_1 = \varepsilon.10$ This and the or realizabilityrequirement case 10 ith All the simulation results shown in this paperare obtained by Arveraging over 1.0° (channel realizations: is bbdaiga2d, thee impact befaithe transmit (jamming) is power and the averageweetection/enfordprobabilityeffsednivestigated; highe isurvesfiwithni:Simsing Exad (9)ien Appeast 2g", fand til KL afpR denote the acsults lobtained by thumbright simulations, the exact analyticalflexpressionadf (22); thus approximation (32) narth the filmenical integration about bined swith the? KL t divergence of (???) srespectively. At Riff becseen that the our wes swith numerical Simulations, (63) and (33) almost coincide... However, arsignificantugaplexists shetween the ideriven with the KIb kirkelingence approximation and the simulation results. Busidesethelayeriage fletection, citrois pdoffability t dedreases with oPt in and sincreases whither tPy... By hesch results evalidate the results given ring Section HL halplying that the proposed approximation expression (32) effectievadoptedglsparcovertness/penformande metric to replace

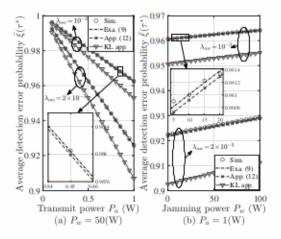


Fig. 2. The detection or qualified like in the strain of the power.

V. Numerical Significant Passive

In this section, we provide inimerical results to show the covert and reliable department of the short-packet communication system against a practive warder. The parameter settings are as follows, that the field of the erwises the fading parameters $\lambda_{ab} = 5 \times 10^{-2}$, $\lambda_{aw} = \lambda_{wb} = 10^{-3}$, the AWGN largingers $\sigma_b^2 = \sigma_w^2 = 10^{-1}$ (W), the self-interference cancellation coefficient $\phi = 10^{-4}$, the blocklength n = 100, the minimum blocklength $a_{min} = 50$, the maximum blocklength $n_{max} = 200$, the maximum transmit power $P_a^{max} = 5(W)$ the covertness requirement $\varepsilon = 10^{-1}$ and the reliability requirement $\kappa = 10^{-1}$. All the simulation results shown in this paper are obtained by averaging over 10^{-1} channel realizations.

Fig. 13. Fig. 2011 be impact of the transmit, (jamming) power on the average detection error probability is investigated. The curves with "Sim.", "Exa. (9)", "App. (12)", and "KL app." denote the results obtained by numerical simulations, the the widely weed Kladivergence on etric due to sits be on a senses and tightness numerical integration combined with the KL distriffig.c3.othe?felationship.ioniongtthe.achievalencohortudes requirementh muandrithd sichidvationreliabilitymdequirementost issinvicktigHedve-ltercan begreiferanfromathexfigures-elargen # lis tolerant, wand smallful redean demachieved x Conversely adarger sinialtolorantesants, smalletes; tan becachieved edicaides roit can blobilise and that eather system Paer formance of coveriness. And feliabilitysperformänka); is ldegradedsby the proastive ovarder Papty in 0, that (W) prompared with the prissive cones Pon 4? 0. The shereadhat shows that other thrade offerforween ctransmission contracts and deliability i Kthaliged by the projetive warders and the proposed technomance evalutions in Sections III and IVInaFibe adopted-to-guidehtheasystam dasignhia-this casertnela Figutithe impact of bldcklength voicthe difficitive throughputnis /showin wheiga the. tlansmis shon scate fsocither of figurer bptimizeds Thereurtyes with malarked solid-lineshiand-draftked detted lines denote the system performance in the system with B psidestive twarder and shan with a passive wander prespectively.

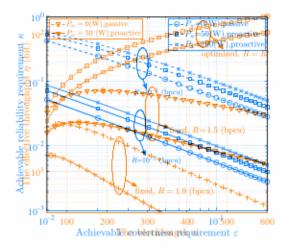


Fig. 4. The effective-blarough-putity-ith-optimized/fixed-ut-at-smisshin-values worsers the short-length ent.

The red dots in the figure indicate the optimal blocklength that maximizes the throughput. It can be seen that in the system with fixed transmission rules, the effective throughput first increases and then decreases with n. This is because when n is too small, η is directly limited by the blocklength. On the contrary, when his too large, the transmit power is limited by the covertness constraint and the decoding error is too large, resulting in the reduction of effective throughput. In addition, the effective throughput with an optimized transmission rate is always higher than that with a fixed transmission rate, which demonstrates the feasibility of the proposed optimization framework. These tesuits imply that for the system with optimized rates, a longer blocklength is always beneficial to improve the effective iffroughput. However, for the system with a fixed rate, the optimal blocklength is not necessarily the maximum one, which is critical for the system design, rates versus the blocklength. CONCLUSION

In this paper, we investigated the reliable and covert performarteesef ashdrt-plackeli (gomerfinicatione) syistedegraghidstb u phoaotivectivardeardSpcEifical50, 160 (aMéragendetectionitlenfor probability.earld, its (approximation) svehovdefined the tevaluate thet wovertness:perform ance: the additionel the layer age idecode ing terropropropriate invalues derive the pevaluate the registration to penfortitancen Bastition Hiteraria I Visa abbyer dan teptimization frameworkswassproposethis maximize the effective throughput. Numerical4 results inverified of thologensibility of the proposed abproximations shody they be timize the artisanies work: a The's petfore france to set bringe ht. The correspond howardered as lith visitie and compared with the epassive to the and the optimal blocklength to steax i mizb the reffective whirderhoud what elaborated swith different systems vely. The red dots in the figure indicate the optimal blocklength that maximizes the throughput. It can be seen that in the system with fixed transmission rates, the effective throughput first increases and then delYedenoterth (4) This is to charle twhen file is to be limber to indlige(ct)y = linf(ted leg the blookhength. = Or the eorlinathe

highncoveriness sterguiother through it provedes selected the coveriness requirement, and the gold of the person is and finge, resulting in, the expedent then approximated through we for the person in the person

Thus, for $0 \le x < e^{\frac{\Gamma(n)}{n-nn}} - 1$, we can obtain $\xi^l(\tau^*) = \frac{\ln_1 \tan_2 n}{\ln_1 \ln_1 + x} < 1 - \frac{\ln_2 \tan_2 n}{\ln_2 \ln_2 n}$ and Theorem 2 is proved. performance of short-packet communication systems against a proactive warders specifically, the average detection cropagns or billy weed its approximate. In addition, the By adopting the Pinsker's inequality, a lower bound of average decoding error probability was derived to evaluate the reliability performance. Based on the analysis above, an optimization framework was proposed to maximize the effective throughput. Numerical results verified the feasibility of the proposed approximations, and the optimization framework the probability distributions of timization framework. The performance loss brought by the observations at Wille under H_0 and H_1 , respectively. Disconstite warder was investigated compared with the passive and the optimal blocklength to maximize the effective throughout was elaborated with different systems, we prove that (??) is tighter than the KL divergence (1.5).

approximation, i.e., $\xi\left(\tau^*\right) > \xi^l(\tau^*) > \xi^{KL}$.

We denote $f_3(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln^2x + \ln x + \frac{1}{x} - 1$ with $\frac{df_3(x)}{dx} = \frac{1}{x}(-2e^{-\Delta n}pandix\Gamma^{\Delta}(n))^{-2}\ln x + 1 - \frac{1}{x})$. In addition, we denote $f_4(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln x + 1 - \frac{1}{x}$. In addition, we denote $f_4(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln x + 1 - \frac{1}{x}$. Where $f_4(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln x + 1 - \frac{1}{x}$ with $\frac{df_4(x)}{dx} = x^{-2} - 2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}x^{-1}$ where $f_4(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}x^{-1}$ where $f_4(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}x^{-1}$ where $f_4(x) = -2e^{-2n}n^{2n-1}$, we can obtain $f_4(x) = -2e^{-2n}n^{2n-1}$, $f_4(x) = -2e^{-2n}n^{2n-1}$, we can obtain $f_4(x) = -2e^{-2n}n^{2n-1}$, $f_4(x) = -2e^{-2n}n^{2n-1}$,

 $f_3(x)$, and adopting the Applits distribed above, we can obtain $\xi^l(\tau^*)$ Comparison by $(x_n)^2$ and $(x_n)^2$ and $(x_n)^2$ of $(x_n)^2$ of (

Besides, when $\frac{P_a|h_{aw}|^2}{\sigma^2} > e^{\frac{\Gamma(n)}{\Gamma^2 nna}} - 1, \xi^I(\tau^*) = 0 > \xi^{KL}$. Note that the above results-hold $\mathfrak{P}(\mathbb{R}_0)$ the assumption $n \not \geq 2$ which is always true in short-packet communications, where \mathbb{P}_0 and \mathbb{P}_1 denote the probability distributions of the observations at Willie under \mathcal{H}_0 and \mathcal{H}_1 , respectively. $\mathcal{D}\left(\mathbb{P}_0||\mathbb{P}_1\right)$ is the KL divergence from \mathbb{P}_0 to \mathbb{P}_1 as $\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1) = n\left(\ln\left(1 + \frac{P_a|h_{aw}|^2}{\sigma^2}\right) + \frac{\sigma^2}{\sigma^2 + P_a|h_{aw}|^2} - 1\right)$.

Then, we prove that (??) is tighter than the KL divergence approximation, i.e., $\xi(\tau^*) > \xi^l(\tau^*) > \xi^{KL}$. We denote $f_3(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln^2 x + \ln x + \frac{1}{x}$

We denote $f_3(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln^2 x + \ln x + \frac{1}{x} - 1$ with $\frac{df_3(x)}{dx} = \frac{1}{x}(-2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln x + 1 - \frac{1}{x})$. In addition, we denote $f_4(x) = -2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}\ln x + 1 - \frac{1}{x}$ with $\frac{df_4(x)}{dx} = x^{-2} - 2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}x^{-1}$, where $2e^{-2n}n^{2n-1}(\Gamma(n))^{-2} < 1$, proved as follows.

 $2e^{-2n}n^{2n-1}(\Gamma(n))^{-2} < 1, \text{ proved as follows.}$ By denoting $M_1(n) = \frac{\Gamma(n)}{\sqrt{2ne^{-n}n^{n-1}}}, \text{ we can obtain }$ $\frac{\partial M_1(n)}{\partial n} = -\frac{\sqrt{2}}{4}e^nn^{-n-3/2}n! \left(2n\log(n) - 2n\psi^{(0)}(n) - 1\right) < 0, \text{ and } M_1(1) = \frac{e}{\sqrt{2}} > 1, \lim_{n \to \infty} M_1(n) = \sqrt{\pi} + \mathcal{O}\left(\frac{1}{n}\right) > 1.$ Thus, $2e^{-2n}n^{2n-1}(\Gamma(n))^{-2} \in \left(\frac{1}{\pi}, \frac{2}{e^2}\right).$ Therefore, $f_4(x)$ increases in $\left[1, \frac{1}{2}e^{2n}n^{1-2n}(\Gamma(n))^2\right)$

Therefore, $f_4(x)$ increases in $\left[1,\frac{1}{2}e^{2n}n^{1-2n}(\Gamma(n))^2\right)$ and decreases in $\left(\frac{1}{2}e^{2n}n^{1-2n}(\Gamma(n))^2,+\infty\right)$. In addition, $f_4(1)=0$ and $f_4(x)$ is larger than 0 in the interval $[1,\kappa_1)$ and less than 0 in the interval $(\kappa_1,+\infty)$, where κ_1 is the solution to $-2e^{-2n}n^{2n-1}(\Gamma(n))^{-2}x\ln x + x = 1$ except 1. Futhermore, $f_3(x)$ increases in $[1,\kappa_1)$ and decreases in $(\kappa_1,+\infty)$. When $x=e^{\frac{\Gamma(n)}{e^{-n}n^n}}$, we can obtain $f_3(e^{\frac{\Gamma(n)}{e^{-n}n^n}})=\frac{1}{n}\left(n\left(\frac{\Gamma(n)}{e^{-n}n^n}+e^{-\frac{\Gamma(n)}{e^{-n}n^n}}-1\right)-2\right)$, where the sequence $M_2(n)=n\left(\frac{\Gamma(n)}{e^{-n}n^n}+e^{-\frac{\Gamma(n)}{e^{-n}n^n}}-1\right)$ is monotonically increasing with n and $M_2(1)=1.78<2$, $M_2(2)=2.01>2$. Therefore, $f_3(x)>0$ in $\left[1,e^{\frac{\Gamma(n)}{e^{-n}n^n}}\right]$ with $n\geq 2$. And by substituting $x=1+\frac{P_n|h_{aw}|^2}{\sigma^2}$ into $f_3(x)$, and adopting the results derived above, we can obtain $\xi^l(\tau^*)=1-\frac{e^{-n}n^n}{\Gamma(n)}\ln\left(1+\frac{P_a|h_{aw}|^2}{\sigma^2}\right)>1-\sqrt{\frac{1}{2}}\mathcal{D}\left(\mathbb{P}_0||\mathbb{P}_1\right)$ for $0<\frac{P_a|h_{aw}|^2}{\sigma^2}\leq \left(e^{\frac{\Gamma(n)}{e^{-n}n^n}}-1\right)$.

Besides, when $\frac{P_a|\hat{h}_{aw}|^2}{\sigma^2} > e^{\frac{\Gamma'(n)}{\sigma^2n^n}} - 1, \xi^l(\tau^*) = 0 > \xi^{KL}$. Note that the above results hold with the assumption $n \ge 2$, which is always true in short-packet communications.