IEEE Sensors Letters VOL. 4, NO. 5, MAY 2020

IEEE Sensors Council

Sensor networks

Covert Communications Against an Adversary With Low-SNR Sensing Capability in Nakagami Fading

Shabnam Sodagari*

Department of Electrical Engineering, California State University, Long Beach, CA 90840 USA

**Senior Member, IEEE*

Manuscript received April 2, 2020; revised April 19, 2020; accepted April 25, 2020. Date of publication April 28, 2020; date of current version May 14, 2020.

Abstract—We show how to achieve covert communications in the presence of a warden equipped with sensing capabilities, even at a low signal to noise ratio (SNR). The warden Willie tries to minimize its false alarm and missed detection probabilities for weak signals. To this end, Willie selects optimal detection threshold for sensing particular legitimate users who want to cover their communication. Our solution to guarantee covertness involves deriving the lower bound for the sum of missed detection and false alarm probabilities, i.e., the mistake at the warden. To hide the message exchange, we derive the conditions for the minimum probability of mistake at Willie to be greater than a threshold. Our simulation results elucidate the roles played by various parameters, such as the number of samples, the target mistake threshold, the amount of noise uncertainty, etc., in undetectable communications over Nakagami fading. Our analysis demonstrates the feasibility of positive-rate hidden communications against a watchful adversary whose receiver is designed to be sensitive to weak SNR.

Index Terms—Data security, information security, internet of things, Nakagami fading, wireless sensor networks.

I. INTRODUCTION

Secret communications and the secrecy rate are different from undetectable communications and the privacy rate [1]. In secret communications, the eavesdropper already knows that communication is taking place between two parties. Given this, in calculating the secrecy capacity one derives the maximum possible rates for which the information cannot be decoded by an eavesdropper [2]. However, the goal of undetectable communications is to disable a warden (Willie) from even noticing that any communication is taking place between two legitimate parties: Alice and Bob [3]. If this goal is realized, the eavesdropper or the warden does not even attempt to decode the private message, since the warden remains oblivious to any message exchange taking place.

Without overcoming the challenges caused by well-equipped eavesdroppers and complicated scenarios of undetectable communications, the hurdle of unnoticeable message exchange will likely remain problematic.

The key to realize covert communications is to reverse the objectives of spectrum sensing (e.g., methods used in cognitive radio networks) to disable a warden from sensing the presence of data communications. As such, the outcomes will enable detection-proof communication strategies. We note that once probabilities of false alarm and missed detection are targeted, the warden can be successfully left uninformed and oblivious.

Most existing results on covert communications underestimate the spectrum sensing capabilities of the warden by relying on the assumption that the warden is not prepared to detect signals that have become weak by the time they have arrived at the warden. No previous work considered a warden that is prepared for detecting low signal to noise ratio (SNR) signals, especially in Nakagami fading. Nevertheless, the main contribution of this letter is achieving positive-rate covert communication in the presence of a warden that is capable of sensing and detection at very low SNR.

To this end, we consider the following steps:

1) observing how a smart warden Willie selects his detection threshold for sensing weak signals;
2) deriving and targeting the lower bound for the probability of mistake at the sensitive warden to always let Alice hide her communication;
3) formulating and numerically solving the conditions for hidable communications in spite of such an adversary;
4) deploying the results for Nakagami channels as a proof of concept; and
5) presenting the tradeoffs and the roles of different parameters affecting undetectable communications.

The rest of the letter is organized as follows. A review of related work is presented in Section II. The novel scheme for achieving covert communications in spite of a sensitive warden is elaborated in Section III. In Section IV, the numerical results support the effectiveness of the proposed solutions and illustrate the roles and tradeoffs of different parameters. This is followed by the conclusion in Section V.

II. REVIEW OF RELATED WORK

A traditional and old method of covertness in communications is the spread-spectrum technique and its variants, which were used for military purposes [4]–[6]. However, spread spectrum methods consume a lot of bandwidth that does not contribute to data rate. Earlier studies on covert communications considered only additive white Gaussian noise channel [3]. In addition, the binary symmetric channel (BSC) [7], [8] and the discrete memoryless channel (DMC) [9] were investigated to study the limits of covert communications. However, the above-mentioned channels have limited scope, as they do not capture the realistic and practical models of wireless communications. Nakagami fading is a more generalized model for wireless channels and more accurately models urban radio multipath environments [10].

Corresponding author: Shabnam Sodagari (e-mail: shabnam@ieee.org).
Associate Editor: L. Azpilicueta.
Digital Object Identifier 10.1109/LSENS.2020.2991095

Moreover, the information bits that Alice can transmit to Bob in a covert and reliable manner are limited to $\mathcal{O}(\sqrt{n})$ bits in n channel uses as $n \to \infty$. Surprisingly, this yields the not so fascinating privacy rate of zero due to $\lim_{n\to\infty} \frac{\mathcal{O}(\sqrt{n})}{n} \to 0$ [8], [11].

Later, there were works that achieved positive covertness rates for Alice and Bob. These relied on the assumption that the warden Willie does not have enough and accurate knowledge of his receiver noise power [1], [2], [12]. In general, uncertainty about noise and interference at any receiver increases the signal-to-interference-plus-noise ratio (SINR) wall. SINR wall is the lowest SINR for which the detection can be reliable if sensing time is unlimited [13]. In other words, below the SINR wall the receiver fails to detect, no matter how long the observation interval is [14]. For instance, the results of a variant of this assumption, in which the warden is uncertain about the distribution of its own noise power, were studied in [15]. In addition, the following two other cases were shown to yield positive rate covert communications for Alice and Bob:

1) when the warden Willie is oblivious about when the covert communication happens [16]; and
2) when Alice and Bob take advantage of an uniformed jammer [17], [18].

The assumption that Willie remains oblivious about when the covert communication happens may not always hold true. For example, when the warden Willie periodically performs spectrum sensing in small periods, there are high chances that he becomes aware of the timing of the communication taking place between Alice and Bob.

Some works suggest the use of amiable jammers to cause interference uncertainty at Willie's receiver [17], [18]. Any transmitting device in the vicinity of Willie can help Alice shield its communication from Willie, regardless of whether the device knows that it is helping Alice or not. As such, Willie is confused about setting his detection threshold and cannot detect if Alice is transmitting. However, the assumption that all interferers have the same transmit power may not be realistic. In addition, the assumption about knowing the parameter of the point process may not always be feasible either.

The novel aspect of our work involves achieving covertness in the presence of a smart warden Willie, who optimally sets his detection threshold not to even miss weak signals over Nakagami channels. Nakagami is a realistic and general fading distribution for which some other distributions are only special cases. It also approximates, with high accuracy, the Rician channel model, and approaches the lognormal distribution under certain conditions. Moreover, it allows random length for scatter vectors, as opposed to some other channel models in which the lengths of the scatter vectors are assumed to be equal [19]. The derivations and analysis of covertness for this channel model are different from that of other models, e.g. BSC [7], [8], DMC [9], etc. Also, our method is distinguished from other works in that it enables hiding the message exchange from smart wardens. Another novel aspect of this work is the derived lower bound for the sum of missed detection and false alarm probabilities that allows covertness once it is maximized.

III. COVERT COMMUNICATION IN THE PRESENCE OF A WARDEN EQUIPPED WITH LOW-SNR SENSING

A receiver can optimally set the detection threshold to minimize the sum of probabilities of false alarm and missed detection for low-SNR signals [20]. However, this is based on the assumption that the noise at the receiver is perfectly known. Otherwise, the receiver cannot select an accurate sensing threshold. We denote the probability of false alarm by P_f, the probability of missed detection by P_{md}, and the sum of false alarm and missed detection probabilities by $\xi = P_f + P_{\text{md}}$.

Using the Erfc or complementary error function [21], with low SNR at Willie, $\xi = P_f + P_{\text{md}}$ can be written as [20]

$$\xi = P_f + P_{\text{md}}(\gamma) = \frac{1}{2}\text{Erfc}\left(\frac{\lambda - N\sigma_w^2}{\sqrt{2N}\sigma_w^2}\right) + \left(1 - \frac{1}{2}\text{Erfc}\left(\frac{\lambda - N\sigma_w^2(1+\gamma)}{\sqrt{2N}\sigma_w^2}\right)\right) \tag{1}$$

where σ_w^2 is the power of noise at Willie's receiver, N is the number of samples at Willie, λ is the detection threshold, and γ is the SNR.

However, here, we pursue the opposite goals for spectrum sensing, i.e., for an arbitrary small ϵ we should force $\xi = P_f + P_{\text{md}} \geq 1 - \epsilon$ [2]. As such, we determine the conditions to increase the above probabilities to mislead the wardens. As a result, we will achieve positive privacy rates even when the warden is sensing weak signals.

To obtain the optimal threshold λ^*, Willie calculates $\frac{\partial \xi}{\partial \lambda} = 0$. Calculating the abovementioned derivative, the optimal threshold λ^* in Nakagami-2 fading was obtained in [20, eq. (26)] as

$$\lambda^* = \left(1 + \frac{2}{N\bar{\gamma}} - \frac{1}{2\sqrt{2N}}\left(\sqrt{\pi} - \sqrt{\pi - 8 + 2N\bar{\gamma}^2}\right)\right)N\sigma_w^2 \tag{2}$$

where $\bar{\gamma}$ is the average SNR over Nakagami fading.

From the viewpoint of the warden (Willie), the optimal threshold above, i.e., λ^* minimizes ξ. Therefore, to prepare Alice for the worst case, we insert this optimal threshold λ^* from (2) into (1) for ξ.

For covert communications, the condition of $\xi \geq 1 - \epsilon$ must be satisfied. Let ξ_{lo} denote the lower bound of ξ. To always let Alice achieve covertness, we set the lower bound $\xi_{\text{lo}} \geq 1 - \epsilon$. To this end, we note that the lower and upper bounds for the Erfc function [22] are

$$\frac{2e^{-x^2}}{\sqrt{\pi}(x + \sqrt{x^2+2})} < \text{Erfc}(x) \leq \frac{2e^{-x^2}}{\sqrt{\pi}\left(x + \sqrt{x^2 + \frac{4}{\pi}}\right)}. \tag{3}$$

To obtain ξ_{lo} we insert the lower bound for the Erfc from (3) in the P_f term of (1) and the upper bound from(3) in the P_{md} term of (1). This leads to

$$\xi_{\text{lo}} = \frac{e^{-\left(\frac{\lambda^* - N\sigma_w^2}{\sqrt{2N}\sigma_w^2}\right)^2}}{\sqrt{\pi}\left(\frac{\lambda^* - N\sigma_w^2}{\sqrt{2N}\sigma_w^2} + \sqrt{\left(\frac{\lambda^* - N\sigma_w^2}{\sqrt{2N}\sigma_w^2}\right)^2 + 2}\right)} + \left(1 - \frac{e^{-\left(\frac{\lambda^* - N\sigma_w^2(1+\gamma)}{\sqrt{2N}\sigma_w^2}\right)^2}}{\sqrt{\pi}\left(\frac{\lambda^* - N\sigma_w^2(1+\gamma)}{\sqrt{2N}\sigma_w^2} + \sqrt{\left(\frac{\lambda^* - N\sigma_w^2(1+\gamma)}{\sqrt{2N}\sigma_w^2}\right)^2 + \frac{4}{\pi}}\right)}\right) \geq 1 - \epsilon. \tag{4}$$

The goal is to find out for what ranges of received SNR at Willie, covert communications can be achieved, i.e., (4) holds. This allows deriving the best strategies to hide the message exchange process against a watchful adversary. To solve (4) we note that

$$\frac{e^{-A^2}}{A + \sqrt{A^2+2}} + \epsilon\sqrt{\pi} \geq \frac{e^{-B^2}}{B + \sqrt{B^2 + \frac{4}{\pi}}}. \tag{5}$$

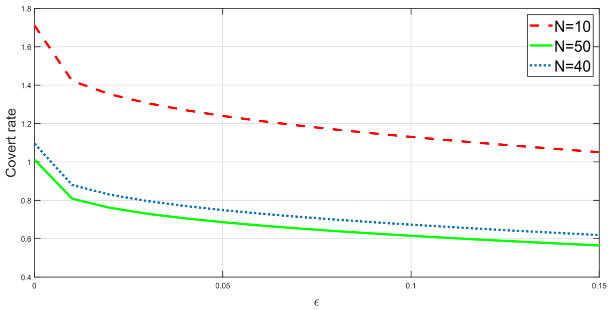

Fig. 1. Covert rate versus ϵ for different numbers of samples at the warden.

In (5)

$$A = \frac{xN - N}{\sqrt{2N}} = \frac{\sqrt{N}(x-1)}{\sqrt{2}}$$

$$B = \frac{xN - N(1+\gamma)}{\sqrt{2N}} = \frac{\sqrt{N}(x-1-\gamma)}{\sqrt{2}} = A\left(1 - \frac{\gamma}{x-1}\right) \tag{6}$$

where

$$x = 1 + \frac{2}{N\bar{\gamma}} - \frac{1}{2\sqrt{2N}}\left(\sqrt{\pi} - \sqrt{\pi - 8 + 2N\bar{\gamma}^2}\right). \tag{7}$$

Then, (5) becomes

$$\frac{e^{-A^2}}{A + \sqrt{A^2+2}} + \epsilon\sqrt{\pi} \geq \frac{e^{-A^2(1-\frac{\gamma}{x-1})^2}}{A(1-\frac{\gamma}{x-1}) + \sqrt{A^2(1-\frac{\gamma}{x-1})^2 + \frac{4}{\pi}}}. \tag{8}$$

By inserting (7) into (8), we obtain (9), shown at the bottom of this page.

The values of γ that satisfy (9) make positive-rate covert communications feasible. In the next section, we present our results by numerically solving (9).

IV. SIMULATION RESULTS

Numerical simulations were conducted in MATLAB. For Nakagami-2 fading the results are shown in Figs. 1 to 4. To summarize, the results verify our method by showing that covert rates are possible even when the warden's receiver is designed to detect low-SNR signals. Specifically, Fig. 1 illustrates the covert rate versus the parameter ϵ for different numbers of samples at Willie's receiver.

When the number of samples at the warden increases, the covert rate decreases. However, the warden needs to wait for a longer time to collect more samples. As ϵ decreases, $1-\epsilon$ increases, which means the mistake probability at the warden increases. Accordingly, the covert rate increases. Fig. 2 shows the changes in covert rate vs. the number of samples taken at the warden with different target values of the parameter ϵ. Note that $1-\epsilon$ represents the minimum probability of mistake at the warden.

Fig. 3 shows the achievable positive covert rates for 5% noise uncertainty at the warden. The variations are demonstrated with respect to the number of samples taken at the warden and the ϵ parameter.

Finally, Fig. 4 shows how even 5% of noise uncertainty (i.e., from 5% to 10%) can boost the covertness of communication in spite of a warden equipped with sensitive detection methods.

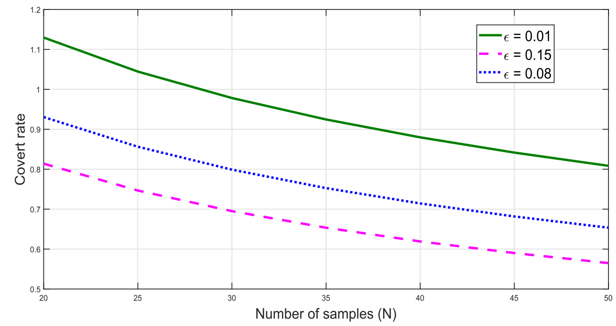

Fig. 2. Covert rate versus the number of samples at the warden.

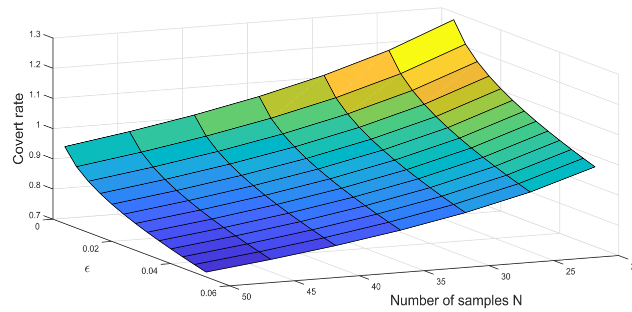

Fig. 3. Covert rate versus the number of samples at the warden and ϵ.

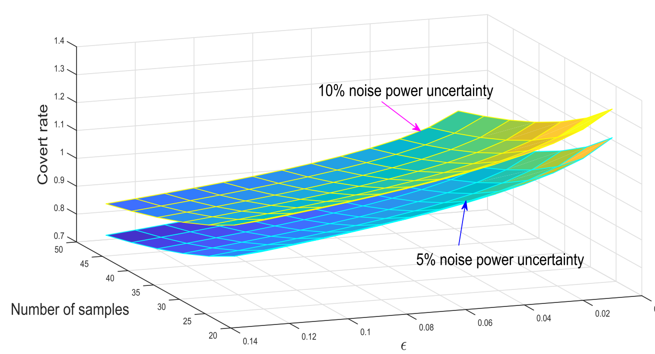

Fig. 4. Effects of the warden's noise power uncertainty on covert rates.

V. CONCLUSION

We considered the problem of hidable communication in the presence of a warden Willie who sets its detection threshold to be optimal for sensing in low SNR. We demonstrated that positive covert rates are possible even in the attendance of such a warden. To always ensure

$$\frac{e^{-A^2}}{A+\sqrt{A^2+2}} + \epsilon\sqrt{\pi} \geq \frac{e^{-A^2\left(1-\frac{\gamma}{\frac{2}{N\bar{\gamma}} - \frac{1}{2\sqrt{2N}}\left(\sqrt{\pi}-\sqrt{\pi-8+2N\bar{\gamma}^2}\right)}\right)^2}}{A\left(1-\frac{\gamma}{\frac{2}{N\bar{\gamma}} - \frac{1}{2\sqrt{2N}}\left(\sqrt{\pi}-\sqrt{\pi-8+2N\bar{\gamma}^2}\right)}\right) + \sqrt{A^2\left(1-\frac{\gamma}{\frac{2}{N\bar{\gamma}} - \frac{1}{2\sqrt{2N}}\left(\sqrt{\pi}-\sqrt{\pi-8+2N\bar{\gamma}^2}\right)}\right)^2 + \frac{4}{\pi}}} \tag{9}$$

covertness, we targeted the lower bound of the mistake probability at the warden. More specifically, we derived the conditions that force the minimum of the warden's probability of mistake to become greater than some value. To do this, we used the lower and upper bounds of the complementary error function.

The rationale underlying this method is that reversing the goals of spectrum sensing in cognitive radio networks and exploiting noise uncertainty yield undetectable communication schemes that cannot be sensed by a warden. By numerical analysis, we demonstrated the effects of different parameters and the tradeoffs among them. These include the number of samples, the target mistake probability, and the noise uncertainty at the warden.

In summary, we showed that in light of the warden's noise power uncertainty, positive-rate covert communication is achievable even for a sensitive warden with low-SNR detection capabilities. As a proof of concept, we considered Nakagami fading. An example of future work is to analyze the possibility of hidable communications for various other types of channels when Willie can set his detection threshold in an optimal manner to sense weak signals. Another future research direction is to exploit the intrinsic architecture of multiuser networks with multiple Alice–Bob links to play the roles of amicable jammers for each other, whereas actually transmitting their own data. As such, we can bypass the need for friendly jammers, whose sole role is to inject interference on the warden's sensor.

REFERENCES

[1] S. Lee, R. J. Baxley, J. B. McMahon, and R. S. Frazier, "Achieving positive rate with undetectable communication over MIMO Rayleigh channels," in *Proc. IEEE 8th Sensor Array Multichannel Signal Process. Workshop*, Jun. 2014, pp. 257–260.

[2] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[3] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas. Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[4] J. Chuang, M. W. DeMay, and R. M. Narayanan, "Secure spread spectrum communication using ultrawideband random noise signals," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2006, pp. 1–7.

[5] M. C. Zari, A. F. Zwilling, D. A. Hess, K. W. Snow, C. S. Anderson, and D. Chiang, "Personnel identification system utilizing low probability of intercept (LPI) techniques for covert operations," in *Proc. 30th Annu. Int. Carnahan Conf. Secur. Technol.*, Oct. 1996, pp. 1–6.

[6] M. Gouda, E. R. Adams, and P. C. J. Hill, "Detection amp; discrimination of covert DS/SS signals using triple correlation," in *Proc. 15th Nat. Radio Sci. Conf.*, Feb. 1998, pp. C35/1–C35/6.

[7] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable, deniable and hidable communication," in *Proc. Inf. Theory Appl. Workshop*, Feb. 2014, pp. 1–10.

[8] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2945–2949.

[9] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[10] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.

[11] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

[12] D. Goeckel, B. A. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 236–239, Feb. 2016.

[13] Y. Zeng, Y. C. Liang, A. T. Hoang, and E. C. Y. Peh, "Reliability of spectrum sensing under noise and interference uncertainty," in *Proc. IEEE Int. Conf. Commun. Workshops*, Jun. 2009, pp. 1–5.

[14] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.

[15] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, Apr. 2017.

[16] B. A. Bash, D. Goeckel, and D. Towsley, "LPD communication when the warden does not know when," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 606–610.

[17] T. V. Sobers, B. A. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert communication with the help of an uninformed jammer achieves positive rate," in *Proc. 49th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 625–629.

[18] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

[19] H. Hashemi, "The indoor radio propagation channel," *Proc. IEEE*, vol. 81, no. 7, pp. 943–968, Jul. 1993.

[20] S. Atapattu, C. Tellambura, H. Jiang, and N. Rajatheva, "Unified analysis of low-SNR energy detection and threshold selection," *IEEE Trans. Veh. Technol.*, vol. 64, no. 11, pp. 5006–5019, Nov. 2015.

[21] M. R. C. Dennis G. Zill, *Differential Equations with Boundary-Value Problems*. Boston, MA, USA: Cengage Learning, 2009.

[22] E. W. Weisstein, *Erfc. From MathWorld–A Wolfram Web Resource*. Accessed: 2020. [Online]. Available: http://mathworld.wolfram.com/Erfc.html.