On the Continuity of the Secrecy Capacity of Wiretap Channels Under Channel Uncertainty

Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany

Rafael F. Schaefer and H. Vincent Poor

Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA

***Abstract*—The performance of a secure communication system such as the wiretap channel is usually characterized by its secrecy capacity. In this paper, the issue of whether or not the secrecy capacity is a *continuous* function of the system parameters is examined. In particular, this is done for channel uncertainty modeled via compound channels and arbitrarily varying channels, in which the legitimate users know only that the true channel realization is from a pre-specified uncertainty set. In the former model, this realization remains constant for the entire duration of transmission, while in the latter the realization varies from channel use to channel use in an unknown and arbitrary manner. The secrecy capacity of the *compound wiretap channel* is shown to be robust in the sense that it is a continuous function of the uncertainty set. Thus, small variations in the uncertainty set lead to small variations in secrecy capacity. However, the secrecy capacity of the *arbitrarily varying wiretap channel* is shown to be *discontinuous* in the uncertainty set meaning that small variations can lead to dramatic losses in capacity.**

I. Introduction

In recent years, *information theoretic approaches to security* have been intensively examined as a complement to cryptographic techniques. Such approaches establish reliable communication and data confidentiality jointly at the physical layer by taking the properties of the noisy channel into account. This line of study was initiated by Wyner, who introduced the wiretap channel in [1]. Recently, this area of research has drawn considerable attention since it provides a promising approach to achieve unconditional security; see for example [2–5] and references therein.

These studies are in particular crucial for wireless communication systems, since they are inherently vulnerable to eavesdropping. Unfortunately, in practical systems channel state information (CSI) will always be limited due to the nature of the wireless channel and estimation/feedback inaccuracy. Furthermore, malevolent eavesdroppers will not provide any information about their channels to legitimate users to make eavesdropping even harder. Accordingly, limited CSI must be assumed to ensure reliability and data confidentiality.

This work of H. Boche was supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050. This work of R. F. Schaefer and H. V. Poor was supported in part by the U.S. National Science Foundation under Grant CMMI-1435778 and in part by the German Research Foundation (DFG) under Grant WY 151/2-1.

A first step in the direction of more realistic CSI assumptions is given by assuming that the actual channel realization is unknown. Rather, it is only known to the legitimate users that the true realization belongs to a known set of channels (uncertainty set) and that it remains constant during the entire transmission. These conditions describe the *compound wiretap channel* which has been studied in [6–8]. Despite these efforts, a general single-letter characterization of the secrecy capacity remains unknown until now. Such a description is known only for special cases such as degraded channels [6, 7] or certain MIMO Gaussian channels [8]. For the general case, only a multi-letter description has been established so far [7].

The quality of CSI is further weakened by the additional assumption that this realization may vary from channel use to channel use in an arbitrary and unknown manner. This is the *arbitrarily varying wiretap channel (AVWC)* [9–11] and it has been shown that it makes a difference in this case whether unassisted or common randomness (CR) assisted codes are used. The unassisted secrecy capacity may be zero, while the CR-assisted secrecy capacity is non-zero. In [10] a complete characterization of the relation between the deterministic and CR-assisted secrecy capacity is established; however, a characterization of the CR-assisted secrecy capacity itself remains open.

The analysis in this paper is driven by the following observation: Obviously, the secrecy capacity depends on the underlying uncertainty set. Now in general, the performance of a communication system (in our case the secrecy capacity) should depend in a *continuous* way on the system parameters (in particular the uncertainty set). Since, if small changes in the parameters would lead to dramatic losses in performance, the approach at hand will most likely not be used. Indeed, one is interested in approaches that are robust against such variations in the sense that small variations in the uncertainty set result in small variations in the secrecy capacity. Such a continuous dependency is in particular desirable in the context of active adversaries who can influence the system parameters in a malicious way. Surprisingly, the question of continuity of capacities is rarely discussed.

In Section II we introduce the compound wiretap channel and a distance concept to measure how "close" two channels are. Then in Section III, we show that the secrecy capacity

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

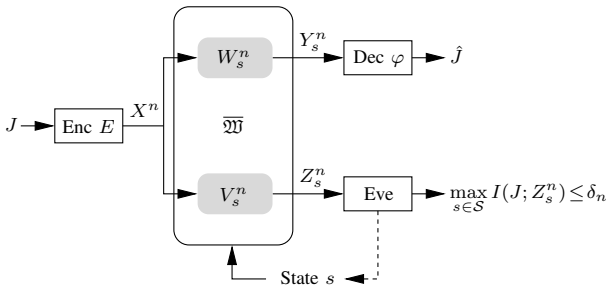

Fig. 1. Compound wiretap channel. The transmitter encodes message J into a codeword $X^n = E(J)$ and transmits it over the compound wiretap channel to the legitimate receiver, which has to decode its intended message $\hat{J} = \varphi(Y_s^n)$ for any channel realization $s \in \mathcal{S}$. At the same time, the eavesdropper has to be kept ignorant of J in the sense that $\max_{s\in\mathcal{S}} I(J;Z_s^n) \leq \delta_n$.

is a continuous function of the uncertainty set. Interpreting the uncertainty set as the strategy space of an adversary, this implies that secure communication over compound channels will be robust against changes in the adversary's strategies.

In Section IV we introduce the AVWC and study its secrecy capacity in Section V. We see that the unassisted secrecy capacity of the AVWC can be discontinuous in the uncertainty set. The practical relevance of this observation is that such unassisted schemes might not be robust in the sense that small variations can lead to dramatic losses in secrecy capacity. In particular in the context of active adversaries this means that small changes in the adversary's strategy can lead to a completely different behavior of the system.[1]

II. Compound Wiretap Channels

We begin with the *compound wiretap channel* in which the actual channel realization is unknown to the users as depicted in Fig. 1. It is known only that it is constant during the entire duration of transmission and lies in a known uncertainty set.

Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$ be an arbitrary state set. Then for given state $s \in \mathcal{S}$ and input and output sequences $x^n \in \mathcal{X}^n$, $y^n \in \mathcal{Y}^n$, and $z^n \in \mathcal{Z}^n$ of length n, the discrete memoryless channels to the legitimate receiver and the eavesdropper are given by $W_s^n(y^n|x^n) := \prod_{i=1}^n W_s(y_i|x_i)$ and $V_s^n(z^n|x^n) := \prod_{i=1}^n V_s(z_i|x_i)$.

Then the (marginal) compound channel to the legitimate receiver is defined by the family of channels for all $s \in \mathcal{S}$ as $\overline{\mathcal{W}} := \{W_s\}_{s\in\mathcal{S}}$. Similarly, we define the compound channel to the eavesdropper as $\overline{\mathcal{V}} := \{V_s\}_{s\in\mathcal{S}}$.

Definition 1. The discrete memoryless *compound wiretap channel* is given by the families of pairs of compound channels with common input as

$$\overline{\mathfrak{W}} := \left\{\overline{\mathcal{W}}, \overline{\mathcal{V}}\right\} = \left\{W_s, V_s\right\}_{W_s\in\overline{\mathcal{W}}, V_s\in\overline{\mathcal{V}}}.$$

[1] *Notation:* $(0,1)$ and $[0,1]$ are the open and closed intervals between 0 and 1; $H_2(\cdot)$ is the binary entropy function; $H(\cdot\|P_{XY})$ and $I(\cdot;\cdot\|P_{XY})$ mean that the entropy and mutual information are evaluated according to the probability distribution P_{XY}; $\mathcal{P}(\mathcal{X})$ denotes the set of all probability distributions on $\mathcal{X}$; $\|P_X - Q_X\|$ is the total variation distance between P_X and Q_X on $\mathcal{X}$ defined as $\|P_X - Q_X\| := \sum_{x\in\mathcal{X}} |P_X(x) - Q_X(x)|$.

We consider a block code of arbitrary but fixed length n. Let $\mathcal{J}_n := \{1, ..., J_n\}$ be the set of confidential messages.

Definition 2. An (n, J_n)*-code* $\mathcal{C}$ consists of a stochastic encoder

$$E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n) \tag{1}$$

and a deterministic decoder at the legitimate receiver

$$\varphi : \mathcal{Y}^n \to \mathcal{J}_n. \tag{2}$$

Remark 1. For the compound wiretap channel it suffices to consider codes as defined above. However, we will see that for the AVWC in Section IV we need more sophisticated code concepts based on common randomness; so-called CR-assisted codes. In this context, we will then refer to codes of Definition 2 as *unassisted codes*.

When the transmitter has sent the message $j \in \mathcal{J}_n$ and the legitimate receiver has received $y^n \in \mathcal{Y}^n$, its decoder is in error if $\varphi(y^n) \neq j$. Then for an (n, J_n)-code $\mathcal{C}$, the average probability of error for channel realization $s \in \mathcal{S}$ is given by

$$\bar{e}_n(s\|\mathcal{C}) := \frac{1}{|\mathcal{J}_n|} \sum_{j\in\mathcal{J}_n} \sum_{x^n\in\mathcal{X}^n} \sum_{y^n:\varphi(y^n)\neq j} W_s^n(y^n|x^n) E(x^n|j).$$

To ensure the confidentiality of the message for all channel realizations $s \in \mathcal{S}$, we require $\sup_{s\in\mathcal{S}} I(J;Z_s^n\|\mathcal{C}) \leq \delta_n$ for some (small) $\delta_n > 0$ with J the random variable uniformly distributed over the set of messages $\mathcal{J}_n$ and $Z_s^n = (Z_{s,1}, Z_{s,2}, ..., Z_{s,n})$ the output at the eavesdropper for channel realization $s \in \mathcal{S}$. This criterion is known as *strong secrecy*.

Definition 3. A rate $R > 0$ is said to be an *achievable secrecy rate* for the compound wiretap channel if for any $\tau > 0$ there exist an $n(\tau) \in \mathbb{N}$, positive null sequences $\{\lambda_n\}_{n\in\mathbb{N}}$, $\{\delta_n\}_{n\in\mathbb{N}}$, and a sequence of (n, J_n)-codes $\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ such that for all $n \geq n(\tau)$ we have $\frac{1}{n}\log J_n \geq R - \tau$, $\sup_{s\in\mathcal{S}} \bar{e}_n(s\|\mathcal{C}_n) \leq \lambda_n$, and

$$\sup_{s\in\mathcal{S}} I(M; Z_s^n\|\mathcal{C}_n) \leq \delta_n.$$

The *secrecy capacity* $C_S(\overline{\mathfrak{W}})$ of the compound wiretap channel with uncertainty set $\overline{\mathfrak{W}}$ is given by the supremum of all achievable secrecy rates R.

In [6] an achievable secrecy rate for finite uncertainty sets and the weak secrecy criterion is established. The result has been strengthened in [7] and [8] to hold also for strong secrecy and arbitrary (not necessarily finite or countable) uncertainty sets. For degraded channels it has been shown in [6] that this secrecy rate is actually the secrecy capacity.

Although a single-letter expression for the secrecy capacity that holds in the general, non-degraded, case is still unknown, a multi-letter description was established in [7].

Theorem 1 ([7]). The secrecy capacity $C_S(\overline{\mathfrak{W}})$ *of the compound wiretap channel with uncertainty set* $\overline{\mathfrak{W}}$ *is*

$$C_S(\overline{\mathfrak{W}}) = \lim_{n\to\infty} \frac{1}{n} \max_{U - X^n - (Y_s^n, Z_s^n)} \times \left(\inf_{s\in\mathcal{S}} I(U;Y_s^n) - \sup_{s\in\mathcal{S}} I(U;Z_s^n) \right) \tag{3}$$

for $U - X^n - (Y_s^n, Z_s^n)$ forming a Markov chain.

III. Continuity of Compound Secrecy Capacity

Here, we analyze the secrecy capacity $C_S(\overline{\mathfrak{W}})$ of the compound wiretap channel and show that it is a *continuous* function of the uncertainty set $\overline{\mathfrak{W}}$. Therefore, we need a concept to measure the distance between two wiretap channels.

A. Distance between Compound Wiretap Channels

Let (W, V) and $(\widetilde{W}, \widetilde{V})$ be two wiretap channels. We define the distance between two (marginal) channels based on the total variation distance as

$$d(W, \widetilde{W}) \coloneqq \max_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \big|W(y|x) - \widetilde{W}(y|x)\big| \tag{4a}$$

$$d(V, \widetilde{V}) \coloneqq \max_{x\in\mathcal{X}} \sum_{z\in\mathcal{Z}} \big|V(z|x) - \widetilde{V}(z|x)\big| \tag{4b}$$

and between the corresponding wiretap channels as

$$d\big((W,V),(\widetilde{W},\widetilde{V})\big) \coloneqq \max\big\{d(W,\widetilde{W}), d(V,\widetilde{V})\big\}.$$

Next, we extend this concept to the compound case. Accordingly, let $\overline{\mathfrak{W}}_1 = (\overline{\mathcal{W}}_1, \overline{\mathcal{V}}_1)$ and $\overline{\mathfrak{W}}_2 = (\overline{\mathcal{W}}_2, \overline{\mathcal{V}}_2)$ with index sets $\mathcal{S}_1$ and $\mathcal{S}_2$ be two uncertainty sets for compound wiretap channels with marginal compound channels $\overline{\mathcal{W}}_i = \{W_{s_i}\}_{s_i\in\mathcal{S}_i}$ and $\overline{\mathcal{V}}_i = \{V_{s_i}\}_{s_i\in\mathcal{S}_i}$, $i = 1, 2$. We define distances between the legitimate compound channels as

$$d_1(\overline{\mathcal{W}}_1, \overline{\mathcal{W}}_2) = \max_{s_2\in\mathcal{S}_2} \min_{s_1\in\mathcal{S}_1} d(W_{s_1}, W_{s_2})$$

$$d_2(\overline{\mathcal{W}}_1, \overline{\mathcal{W}}_2) = \max_{s_1\in\mathcal{S}_1} \min_{s_2\in\mathcal{S}_2} d(W_{s_1}, W_{s_2})$$

and between the eavesdropper compound channels as

$$d_1(\overline{\mathcal{V}}_1, \overline{\mathcal{V}}_2) = \max_{s_2\in\mathcal{S}_2} \min_{s_1\in\mathcal{S}_1} d(V_{s_1}, V_{s_2})$$

$$d_2(\overline{\mathcal{V}}_1, \overline{\mathcal{V}}_2) = \max_{s_1\in\mathcal{S}_1} \min_{s_2\in\mathcal{S}_2} d(V_{s_1}, V_{s_2}).$$

Definition 4. The distance $D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2)$ between two compound wiretap channels with uncertainty sets $\overline{\mathfrak{W}}_1$ and $\overline{\mathfrak{W}}_2$ is defined as

$$\begin{aligned} D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2) = \max\big\{&d_1(\overline{\mathcal{W}}_1, \overline{\mathcal{W}}_2), d_2(\overline{\mathcal{W}}_1, \overline{\mathcal{W}}_2),\\ &d_1(\overline{\mathcal{V}}_1, \overline{\mathcal{V}}_2), d_2(\overline{\mathcal{V}}_1, \overline{\mathcal{V}}_2)\big\}. \end{aligned} \tag{5}$$

The distance $D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2)$ between two compound wiretap channels with uncertainty sets $\overline{\mathfrak{W}}_1$ and $\overline{\mathfrak{W}}_2$ characterizes how "close" or similar these two compound wiretap channels are. Accordingly, it also measures how well one compound wiretap channel can be approximated by another one.

B. Continuity of Compound Secrecy Capacity

Here we study what happens if there are small variations in the uncertainty set. Obviously, it is desirable to have a *continuous* behavior of the secrecy capacity: Small variations in the uncertainty set should only lead to small variations in the corresponding secrecy capacity. For the analysis, we need two important lemmas. Similar results first appeared in [12] and [13] in the context of quantum information theory.

Lemma 1. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite alphabets and $\epsilon \in (0, 1)$ be arbitrary. Then for all joint probability distributions $P_{XY}, Q_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$ with $\|P_{XY} - Q_{XY}\| \leq \epsilon$ it holds that

$$\big|H(Y|X\|P_{XY}) - H(Y|X\|Q_{XY})\big| \leq \delta_1(\epsilon, |\mathcal{Y}|) \tag{6}$$

with $\delta_1(\epsilon, |\mathcal{Y}|) \coloneqq 2\epsilon\log|\mathcal{Y}| + 2H_2(\epsilon)$.

Proof: The proof is an adaptation of the corresponding proof in [12] for quantum sources. For completeness, the proof can be found in the extended version [14]. ∎

Lemma 2. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite alphabets and $W, \widetilde{W} : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ be arbitrary channels with

$$d(W, \widetilde{W}) \leq \epsilon \tag{7}$$

for some $\epsilon > 0$. For arbitrary $n \in \mathbb{N}$, let $\mathcal{U}$ be an arbitrary finite set, $P_U \in \mathcal{P}(\mathcal{U})$ the uniform distribution on $\mathcal{U}$, and $E(x^n|u)$, $x^n \in \mathcal{X}^n$ an arbitrary stochastic encoder, cf. (1)*. We consider the probability distributions*

$$P_{UY^n}(u, y^n) = \sum_{x^n\in\mathcal{X}^n} W^n(y^n|x^n)E(x^n|u)P_U(u)$$

$$\widetilde{P}_{UY^n}(u, y^n) = \sum_{x^n\in\mathcal{X}^n} \widetilde{W}^n(y^n|x^n)E(x^n|u)P_U(u).$$

Then it holds that

$$\big|I(U;Y^n\|P) - I(U;Y^n\|\widetilde{P})\big| \leq n\delta_2(\epsilon, |\mathcal{Y}|) \tag{8}$$

with $\delta_2(\epsilon, |\mathcal{Y}|) \coloneqq 4\epsilon\log|\mathcal{Y}| + 4H_2(\epsilon)$.

Proof: The proof is an adaptation of the proof in [13] for quantum capacities. For completeness, the proof can be found in the extended version of this work [14]. ∎

Note that the right hand sides of (6) and (8) depend only on the size of the output alphabet $\mathcal{Y}$, but they are independent of $\mathcal{X}$ and $\mathcal{U}$ respectively. This will be crucial for Theorem 2.

Theorem 2. Let $\epsilon \in (0, 1)$ be arbitrary. Let $\overline{\mathfrak{W}}_1$ and $\overline{\mathfrak{W}}_2$ be uncertainty sets with corresponding state sets $\mathcal{S}_1$ and $\mathcal{S}_2$ defining two compound wiretap channels. If

$$D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2) \leq \epsilon,$$

then it holds that

$$\big|C_S(\overline{\mathfrak{W}}_1) - C_S(\overline{\mathfrak{W}}_2)\big| \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) \tag{9}$$

with $\delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) \coloneqq 4\epsilon\log|\mathcal{Y}||\mathcal{Z}| + 8H_2(\epsilon)$ a constant depending on the distance ϵ and the alphabet sizes $|\mathcal{Y}|$ and $|\mathcal{Z}|$.

Proof: Let $\xi > 0$ be arbitrary but fixed. There exists an $\hat{s}_1 = \hat{s}_1(\xi)$ such that

$$\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) \geq I(U;Y^n\|P^{\hat{s}_1}) - \xi.$$

By assumption, there also exists an $\hat{s}_2 = \hat{s}_2(\hat{s}_1)$ such that

$$d(W_{\hat{s}_1}, W_{\hat{s}_2}) < \epsilon.$$

This implies

$$\big|I(U;Y^n\|P^{\hat{s}_1}) - I(U;Y^n\|P^{\hat{s}_2})\big| \leq n\delta_2(\epsilon, |\mathcal{Y}|)$$

by Lemma 2, cf. (8). With this we obtain

$$\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) \geq I(U;Y^n\|P^{\hat{s}_2}) - n\delta_2(\epsilon,|\mathcal{Y}|) - \xi \geq \inf_{s_2\in\mathcal{S}_2} I(U;Y^n\|P^{s_2}) - n\delta_2(\epsilon,|\mathcal{Y}|) - \xi. \quad (10)$$

Note that relation (10) holds for all $\xi > 0$. Since, the left hand side does not depend on δ, we obtain

$$\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) \geq \inf_{s_2\in\mathcal{S}_2} I(U;Y^n\|P^{s_2}) - n\delta_2(\epsilon,|\mathcal{Y}|).$$

We observe that if we exchange the roles of $\mathcal{S}_1$ and $\mathcal{S}_2$ in the previous derivation, we end up with a similar expression, where infima over $\mathcal{S}_1$ and $\mathcal{S}_2$ are interchanged. Accordingly,

$$\Big|\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) - \inf_{s_2\in\mathcal{S}_2} I(U;Y^n\|P^{s_2})\Big| \leq n\delta_2(\epsilon,|\mathcal{Y}|).$$

The same arguments lead to

$$\Big|\sup_{s_1\in\mathcal{S}_1} I(U;Z^n\|P^{s_1}) - \sup_{s_2\in\mathcal{S}_2} I(U;Z^n\|P^{s_2})\Big| \leq n\delta_2(\epsilon,|\mathcal{Z}|)$$

so that we conclude

$$\begin{aligned}
&\Big|\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) - \sup_{s_1\in\mathcal{S}_1} I(U;Z^n\|P^{s_1}) \\
&\qquad - \big(\inf_{s_2\in\mathcal{S}_2} I(U;Y^n\|P^{s_2}) - \sup_{s_2\in\mathcal{S}_2} I(U;Z^n\|P^{s_2})\big)\Big| \\
&\leq \Big|\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) - \inf_{s_2\in\mathcal{S}_2} I(U;Y^n\|P^{s_2})\Big| \\
&\qquad + \Big|\sup_{s_1\in\mathcal{S}_1} I(U;Z^n\|P^{s_1}) - \sup_{s_2\in\mathcal{S}_2} I(U;Z^n\|P^{s_2})\Big| \\
&\leq n\delta_2(\epsilon,|\mathcal{Y}|) + n\delta_2(\epsilon,|\mathcal{Z}|) = n\delta(\epsilon,|\mathcal{Y}|,|\mathcal{Z}|)
\end{aligned}$$

with $\delta(\epsilon,|\mathcal{Y}|,|\mathcal{Z}|) = 4\epsilon\log|\mathcal{Y}||\mathcal{Z}| + 8H_2(\epsilon)$. But this implies for the secrecy capacities

$$\begin{aligned}
&\frac{1}{n}\Big(\inf_{s_1\in\mathcal{S}_1} I(U;Y^n\|P^{s_1}) - \sup_{s_1\in\mathcal{S}_1} I(U;Z^n\|P^{s_1})\Big) \\
&\qquad \leq \frac{1}{n}\Big(\inf_{s_2\in\mathcal{S}_2} I(U;Y^n\|P^{s_2}) - \sup_{s_2\in\mathcal{S}_2} I(U;Z^n\|P^{s_2})\Big) \\
&\qquad\qquad + \delta(\epsilon,|\mathcal{Y}|,|\mathcal{Z}|)
\end{aligned}$$

so that

$$C_S(\overline{\mathfrak{W}}_1) \leq C_S(\overline{\mathfrak{W}}_2) + \delta(\epsilon,|\mathcal{Y}|,|\mathcal{Z}|). \quad (11)$$

Again, we can exchange the roles of $\mathcal{S}_1$ and $\mathcal{S}_2$ in the derivation above to obtain a relation as in (11) where $C_S(\overline{\mathfrak{W}}_1)$ and $C_S(\overline{\mathfrak{W}}_2)$ are interchanged. Thus, we have

$$\big|C_S(\overline{\mathfrak{W}}_1) - C_S(\overline{\mathfrak{W}}_2)\big| \leq \delta(\epsilon,|\mathcal{Y}|,|\mathcal{Z}|)$$

which proves the desired result. ∎

Finally, we want to highlight that the continuity of the secrecy capacity was established without having a single-letter description available. Although a multi-letter characterization of the secrecy capacity as given in Theorem 1 might be hard to compute, it is extremely useful for deriving certain properties such as continuity as demonstrated in Theorem 2.

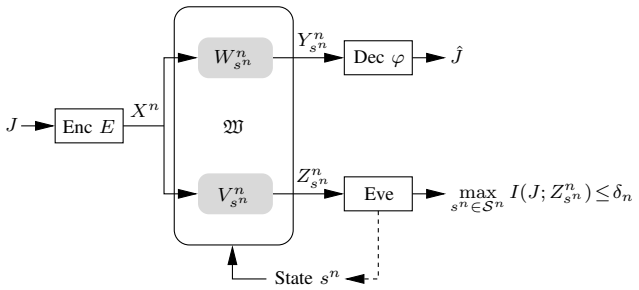

Fig. 2. Arbitrarily varying wiretap channel. In contrast to the compound wiretap channel, the transmission is now governed by an unknown state sequence $s^n \in \mathcal{S}^n$ of length n, which may vary in an unknown manner from channel use to channel use.

IV. Arbitrarily Varying Wiretap Channel

We continue our analysis with the *arbitrarily varying wiretap channel*. In contrast to the previously studied compound wiretap channel, the unknown channel realization may vary in an unknown and arbitrary manner from channel use to channel use as depicted in Fig. 2.

As for the compound wiretap channel in Section II let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$ be a finite state set. Then for a fixed state sequence $s^n \in \mathcal{S}^n$ of length n, the discrete memoryless channel to the legitimate receiver is given by $W_{s^n}^n(y^n|x^n) = W^n(y^n|x^n,s^n) := \prod_{i=1}^n W(y_i|x_i,s_i)$.

Then the family of channels for all $s^n \in \mathcal{S}^n$ defines the (marginal) AVC to the legitimate receiver as $\mathcal{W} := \{W_{s^n}^n\}_{s^n\in\mathcal{S}^n}$. In addition, for any probability distribution $q \in \mathcal{P}(\mathcal{S})$ we define the *averaged channel* as

$$W_q(y|x) = \sum_{s\in\mathcal{S}} W(y|x,s)q(s). \quad (12)$$

An important property of an AVC is the so-called concept of symmetrizability as defined below.

Definition 5. An AVC is called *symmetrizable* if there exists a stochastic matrix $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that

$$\sum_{s\in\mathcal{S}} W(y|x_1,s)\sigma(s|x_2) = \sum_{s\in\mathcal{S}} W(y|x_2,s)\sigma(s|x_1)$$

holds for all $x_1, x_2 \in \mathcal{X}$ and $y \in \mathcal{Y}$.

Roughly speaking, a symmetrizable AVC can "simulate" a valid input, which makes it impossible for the decoder to decide on the correct codeword.

Similarly for the channel to the eavesdropper, we define the discrete memoryless channel as $V_{s^n}^n(z^n|x^n) = V^n(z^n|x^n,s^n) := \prod_{i=1}^n V(z_i|x_i,s_i)$ for given state sequence $s^n \in \mathcal{S}^n$. Further, we set $\mathcal{V} := \{V_{s^n}^n\}_{s^n\in\mathcal{S}^n}$ and $V_q(z|x) = \sum_{s\in\mathcal{S}} V(z|x,s)q(s)$ for $q \in \mathcal{P}(\mathcal{S})$.

Definition 6. The discrete memoryless *arbitrarily varying wiretap channel* is given by the families of pairs of channels with common input

$$\mathfrak{W} := \{\mathcal{W},\mathcal{V}\} = \{W_{s^n}^n, V_{s^n}^n\}_{W_{s^n}^n\in\mathcal{W}, V_{s^n}^n\in\mathcal{V}}.$$

A. Unassisted and CR-Assisted Codes

The definition of an *unassisted* (n, J_n)*-code* $\mathcal{C}$ for the AVWC is the same as for the compound wiretap channel in Definition 2: It consists of a stochastic encoder as in (1) and a deterministic decoder as in (2).

The difference lies in the reliability and secrecy criteria as we have now to consider state sequences $s^n \in \mathcal{S}^n$ of length n. Thus, for given $s^n \in \mathcal{S}^n$ the average probability of decoding error at the legitimate receiver is

$$\bar{e}_n(s^n \| \mathcal{C}) \coloneqq \frac{1}{|\mathcal{J}_n|} \sum_{j \in \mathcal{J}_n} \sum_{x^n \in \mathcal{X}^n} \sum_{\varphi(y^n) \neq j} W^n(y^n | x^n, s^n) E(x^n | j)$$

and the confidentiality of the message is measured by $\sup_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n \| \mathcal{C}) \leq \delta_n$ with $Z_{s^n}^n = (Z_{s_1}, Z_{s_2}, ..., Z_{s_n})$.

Definition 7. A rate $R > 0$ is said to be an *achievable secrecy rate* for the AVWC if for any $\tau > 0$ there exist an $n(\tau) \in \mathbb{N}$, positive null sequences $\{\lambda_n\}_{n \in \mathbb{N}}$, $\{\delta_n\}_{n \in \mathbb{N}}$, and a sequence of (n, J_n)-codes $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ such that for all $n \geq n(\tau)$ we have $\frac{1}{n} \log J_n \geq R - \tau$, $\sup_{s^n \in \mathcal{S}^n} \bar{e}_n(s^n \| \mathcal{C}_n) \leq \lambda_n$, and

$$\sup_{s^n \in \mathcal{S}^n} I(J; Z_{s^n}^n \| \mathcal{C}_n) \leq \delta_n. \tag{13}$$

The *unassisted secrecy capacity* $C_S(\mathfrak{W})$ of the AVWC with uncertainty set $\mathfrak{W}$ is given by the supremum of all achievable secrecy rates R.

Unfortunately, such unassisted approaches do not suffice to establish reliable communication over *symmetrizable* AVCs, cf. Definition 5; indeed, the corresponding capacity is zero in this case [10, 11]. This necessitates the use of more sophisticated strategies based on *common randomness*. It enables the transmitter and the receiver to coordinate their choices of the encoder (1) and the decoder (2) according to $\gamma \in \mathcal{G}_n$.

The reliability and secrecy constraints from above extend to CR-assisted codes in a natural way. Then, the definitions of a *CR-assisted achievable secrecy rate* and the *CR-assisted secrecy capacity* $C_{S,\mathrm{CR}}(\mathfrak{W})$ follow accordingly.

B. Capacity Results

Studies have been undertaken in order to understand the secrecy capacity of the AVWC [9–11] and the relation between the secrecy capacities for unassisted and CR-assisted codes has been completely characterized in [10, Theorem 2].

Theorem 3 ([10]). If the CR-assisted secrecy capacity satisfies $C_{S,CR}(\mathfrak{W}) > 0$*, then the unassisted secrecy capacity is given by*

$$C_S(\mathfrak{W}) = C_{S,CR}(\mathfrak{W})$$

if and only if the AVC $\mathcal{W}$ *to the legitimate receiver is non-symmetrizable. If the AVC* $\mathcal{W}$ *is symmetrizable, then* $C_S(\mathfrak{W}) = 0$*. If* $C_S(\mathfrak{W}) = 0$ *and* $C_{S,CR}(\mathfrak{W}) > 0$*, then the AVC* $\mathcal{W}$ *is symmetrizable.*

The unassisted secrecy capacity $C_S(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ is completely known in terms of its CR-assisted secrecy capacity $C_{S,\mathrm{CR}}(\mathfrak{W})$. However, a characterization of $C_{S,\mathrm{CR}}(\mathfrak{W})$ itself remains open. Only for the special case of a best channel to the eavesdropper is an achievable secrecy rate known [10].

V. Discontinuity of AVWC Secrecy Capacity

Here we study the continuity of the unassisted secrecy capacity $C_S(\mathfrak{W})$ of the AVWC with uncertainty set $\mathfrak{W}$. Theorem 3 provides only a characterization in terms of its corresponding CR-assisted secrecy capacity $C_{S,\mathrm{CR}}(\mathfrak{W})$, but unfortunately, no explicit characterization is known in terms of entropic quantities. Thus, the analysis becomes much more complicated and involved compared to the compound wiretap channel where such a (multi-letter) characterization is known.

Nonetheless, we will be able to show that the unassisted secrecy capacity $C_S(\mathfrak{W})$ is discontinuous in the uncertainty set $\mathfrak{W}$. Similar to the compound wiretap channel, we ask the question: if the distance between two AVWCs is small, i.e., $D(\mathfrak{W}_1, \mathfrak{W}_2) < \epsilon$, does this imply that $C_S(\mathfrak{W}_1) - C_S(\mathfrak{W}_2)$ is small as well?

In more detail, let $\{\mathfrak{W}_n\}_{n \in \mathbb{N}}$ be a sequence of finite uncertainty sets, which converge to a finite set $\mathfrak{W}^*$ in terms of D-distance. The question is then whether or not this implies

$$\lim_{n \to \infty} C_S(\mathfrak{W}_n) = C_S(\mathfrak{W}^*). \tag{14}$$

Since no complete characterization of $C_S(\mathfrak{W}^*)$ is known, we will examine this question via a simple example to show that (14) does not hold in general. However, this simple example already indicates the fundamentally different behavior compared to the compound wiretap channel.

A. Secrecy Capacity with Discontinuity Point

The aim of this part is to construct an AVWC whose unassisted secrecy capacity has a discontinuity point. To do so, we consider a communication scenario with input and output alphabets of sizes $|\mathcal{X}| = 2$, $|\mathcal{Y}| = 3$, $|\mathcal{Z}| = 2$, and $|\mathcal{S}| = 2$.

Let us first consider the communication channel to the legitimate receiver. To construct a suitable AVC for this link, we make use of an example [15, Example 1]. We follow this example and construct an AVC to the legitimate receiver with uncertainty set

$$\mathcal{W} = \{W_1, W_2\} \tag{15}$$

where

$$W_1 \coloneqq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad W_2 \coloneqq \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

We know from [15] that $\mathcal{W}$ then defines a symmetrizable AVC so that its unassisted capacity is zero, i.e., $C(\mathcal{W}) = 0$.

Further, with the channel

$$\hat{W} \coloneqq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

we define the trivial AVC whose two elements are identical as

$$\hat{\mathcal{W}} = \{\hat{W}, \hat{W}\}. \tag{16}$$

Now, for the channel to the eavesdropper, we define the "useless" channel

$$V \coloneqq \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}. \tag{17}$$

Then the set $\mathcal{V} = \{V, V\}$ defines a corresponding AVC to the eavesdropper.

These definitions finally create with (15), (16), and (17) the following two AVWCs specified by their uncertainty sets:

$$\mathfrak{W} \coloneqq \big\{\mathcal{W}, \mathcal{V}\big\} \quad \text{and} \quad \hat{\mathfrak{W}} \coloneqq \big\{\hat{\mathcal{W}}, \mathcal{V}\big\},$$

Moreover, we can define a convex combination of these two AVWCs as

$$\mathfrak{W}(\lambda) = \big\{\{W_1(\lambda), W_2(\lambda)\}, \mathcal{V}\big\} \quad \text{for } 0 \leq \lambda \leq 1.$$

with convex combinations

$$W_1(\lambda) = W_{1,\lambda} = (1-\lambda)W_1 + \lambda\hat{W}$$
$$W_2(\lambda) = W_{2,\lambda} = (1-\lambda)W_2 + \lambda\hat{W}.$$

This is indeed a convex combination of the eavesdropper AVC as well which is trivial as we have identical elements.

Now, the following result shows that the unassisted secrecy capacity $C_S(\mathfrak{W}(\lambda))$ is discontinuous in λ.

Theorem 4. The following holds for the previous example:

1) *The CR-assisted secrecy capacity $C_{S,CR}(\mathfrak{W}(\lambda))$ is continuous in λ for all $\lambda \in [0,1]$ and it holds that*

$$\min_{\lambda\in[0,1]} C_{S,CR}(\mathfrak{W}(\lambda)) > 0. \tag{19}$$

2) *The unassisted secrecy capacity $C_S(\mathfrak{W}(\lambda))$ is continuous in λ for all $\lambda \in (0,1]$. It holds that $C_S(\mathfrak{W}(0)) = 0$ and further that*

$$\lim_{\lambda\searrow 0} C_S(\mathfrak{W}(\lambda)) > 0, \tag{20}$$

i.e., $\lambda = 0$ is a discontinuity point of $C_S(\cdot)$.

Proof: Due to space constraints the proof is relegated to the extended version of this work [14]. ∎

Remark 2. Now for the case $\lambda = 0$ in Theorem 4 we see the following: Whenever the legitimate users try to communicate at a positive rate, the adversary can jam the communication such that the decoding error at the legitimate receiver is always greater than $1/4$ since the $\mathcal{W}$ is symmetrizable (see also [11] for a more detailed discussion). Although the secrecy criterion is satisfied, no reliable communication is possible. See [14] for further details.

On the other hand, for $\lambda > 0$ we have $C_S(\mathfrak{W}(\lambda)) > 0$ so that in this case reliable and secure communication is possible. However, from this we cannot draw conclusions about $C_S(\mathfrak{W}(0))$ by taking the limit $\lambda \to 0$, since $\lambda = 0$ is a discontinuous point. Thus, it is not robust since small variations can result in a dramatic loss in secrecy capacity.

Remark 3. This technique can easily be extended to obtain examples with discontinuities for general sets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{S}$; cf. [14].

Remark 4. In principle, the eavesdropper has different jamming strategies: increasing the secrecy leakage $I(J; Z_{s^n}^n \| \mathcal{C})$ or increasing the decoding error $\bar{e}_n(s^n \| \mathcal{C})$ of the legitimate receiver. The example above shows that the second strategy is particularly effective for AVWCs.

VI. Conclusion

The analysis of this paper was motivated by the question of whether the secrecy capacity depends *continuously* on the uncertainty set or not. Obviously, a continuous behavior is desirable as then small changes in the uncertainty set result in only small changes in the secrecy capacity. This becomes particularly relevant in the context of active adversaries where the uncertainty set describes the strategy space of an adversary. In addition, such a continuous behavior is also a necessary condition for the existence of codes that are robust against uncertainties. Since if the secrecy capacity is already discontinuous, a robust code design will not be possible at all.

Surprisingly, the answer to this question depends highly on the abilities of the adversary – even for the simplest case of an uncertainty set containing two elements. If the actual realization from this uncertainty set remains constant, this is the compound wiretap channel and the corresponding secrecy capacity is continuous. However, if the adversary is allowed to vary in an unknown and arbitrary manner between these two realizations during the transmission, the legitimate users have to deal with an AVWC and its unassisted secrecy capacity can be discontinuous in the uncertainty set.

References

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[4] R. F. Schaefer and H. Boche, "Physical Layer Service Integration in Wireless Networks – Signal Processing Challenges," *IEEE Signal Process. Mag.*, vol. 31, no. 3, pp. 147–156, May 2014.

[5] G. Fettweis, H. Boche, T. Wiegand, and et al., "The Tactile Internet," ITU-T Tech. Watch Rep., Tech. Rep., Aug. 2014. [Online]. Available: http://www.itu.int/oth/T2301000023/en

[6] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound Wiretap Channels," *EURASIP J. Wireless Commun. Netw.*, vol. Article ID 142374, pp. 1–13, 2009.

[7] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy Results for Compound Wiretap Channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[8] R. F. Schaefer and S. Loyka, "The Secrecy Capacity of a Compound MIMO Gaussian Channel," in *Proc. IEEE Inf. Theory Workshop*, Seville, Spain, Sep. 2013, pp. 104–108.

[9] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary Jamming Can Preclude Secure Communication," in *Proc. 47th Annual Allerton Conf. Commun., Control, Computing*, Urbana-Champaign, IL, USA, Sep. 2009, pp. 1069–1075.

[10] I. Bjelaković, H. Boche, and J. Sommerfeld, *Information Theory, Combinatorics, and Search Theory*. Springer, 2013, ch. Capacity Results for Arbitrarily Varying Wiretap Channels, pp. 123–144.

[11] H. Boche and R. F. Schaefer, "Capacity Results and Super-Activation for Wiretap Channels With Active Wiretappers," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1482–1496, Sep. 2013.

[12] R. Alicki and M. Fannes, "Continuity of Quantum Conditional Information," *J. Phys. A: Math. Gen.*, vol. 37, no. 5, pp. L55–L57, 2004.

[13] D. Leung and G. Smith, "Continuity of Quantum Channel Capacities," *Commun. Math. Phys*, vol. 292, no. 1, pp. 201–215, 2009.

[14] H. Boche, R. F. Schaefer, and H. V. Poor, "On the Continuity of the Secrecy Capacity of Compound and Arbitrarily Varying Wiretap Channels," *submitted*, available online at http://arxiv.org/abs/1409.4752.

[15] R. Ahlswede, "Elimination of Correlation in Random Codes for Arbitrarily Varying Channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978.