Comparison of Different Attack Classes in Arbitrarily Varying Wiretap Channels

Holger Boche and Rafael F. Wyrembelski

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany
{boche, wyrembelski}@tum.de

***Abstract*—For communication over arbitrarily varying channels (AVC), common randomness is an important resource to establish reliable communication, especially if the AVC is symmetrizable. In this paper the *arbitrarily varying wiretap channel (AVWC) with active wiretapper* is studied. Here the wiretapper is active in the sense that it can exploit the knowledge about the common randomness to control the channel conditions of the legitimate users. The common randomness assisted secrecy capacity of the AVWC with active wiretapper is analyzed and is related to the corresponding secrecy capacity of the AVWC with passive wiretapper. If the active secrecy capacity is positive, it equals the corresponding passive secrecy capacity. The case of zero active capacity is also studied.**

I. Introduction

Rapid developments in communication systems make information available almost everywhere. Along with this, the security of sensitive information from unauthorized access becomes an important task and a common approach is the use of cryptographic techniques to keep information secret. Such techniques have a wide variety of use and are based on the assumption of insufficient computational capabilities of non-legitimate receivers. Due to increasing computational power, improved algorithms, and recent advances in number theory, these techniques are becoming more and more insecure.

Wireless communication systems are inherently vulnerable for eavesdropping due to the open nature of the wireless medium. The physical properties of the wireless channel make the communication accessible to external wiretappers but, on the other hand, also offer possibilities to establish security by other approaches than cryptographic techniques.

In this context the concept of information theoretic, or physical layer, security is becoming more and more attractive, since it solely uses the physical properties of the wireless channel to establish security. So, regardless of what the wiretapper does with the received signal, the confidential information cannot be reproduced with high probability. Information theoretic security was initiated by Wyner, who introduced the *wiretap channel* [1]. This is the simplest scenario involving security with one legitimate transmitter-receiver pair and one wiretapper to be kept ignorant. Recently, there is growing interest in information theoretic security; for instance see [2–5].

WIFS'2012, December, 2-5, 2012, Tenerife, Spain.
978-1-4673-2287-4/12/$31.00 ©2012 IEEE.

Another challenge in wireless networks is the question of sufficient channel state information at the users. Due to the nature of the wireless channel, in practical systems there is always uncertainty in channel state information. Since this has a huge impact on the performance of wireless systems, the analysis of information theoretic security for different models of channel uncertainty is an important research field and, thus, indispensable for bringing this concept into practice.

A reasonable model is to assume that the exact channel realization is not known; rather, it is only known that it belongs to a pre-specified set of channels. If this channel remains fixed during the whole transmission of a codeword, this is the *compound wiretap channel* which is studied in [6–8].

In this paper we go one step further and additionally allow the channel to vary in an unknown and arbitrary manner from symbol to symbol. This is the concept of *arbitrarily varying wiretap channels (AVWC)*, which provides a suitable and robust model for secure communication under channel uncertainty, especially for such scenarios where the legitimate users are confronted with unknown varying interference induced by other coexisting transmitters.

If the wiretapper is unaware of the actual channel realization or is not able to influence the channel conditions of the legitimate users, the wiretapper is called *passive*. But AVWCs also serve as a model for scenarios with a more powerful wiretapper which can maliciously influence the channel conditions. A wiretapper, which can control the actual state sequence of the legitimate users, is called an *active wiretapper.*

These models immediately define different classes of attacks against which the communication should be protected. *Passive attacks* and the corresponding AVWC with passive wiretapper is analyzed in [9–11], where the latter use the *strong secrecy criterion* [12]. In this paper we analyze *active attacks* and show that the common randomness assisted secrecy capacity of the AVWC with active wiretapper is equal to the corresponding one with passive wiretapper in several cases.[1]

II. Arbitrarily Varying Wiretap Channels

We start with some basic definitions. Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$ be a finite state set. Then for

[1] *Notation:* Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters; $I(\cdot;\cdot)$ is the mutual information; $X-Y-Z$ denotes a Markov chain of random variables X, Y, Z in this order; $\mathcal{P}(\cdot)$ and $\mathbb{E}[\cdot]$ are the set of all probability distributions and the expectation.

given state sequence $s^n = (s_1, s_2, ..., s_n) \in \mathcal{S}^n$ of length n, the discrete memoryless channel to the legitimate receiver is given by the stochastic matrix

$$W^n(y^n|x^n, s^n) \coloneqq \prod_{i=1}^{n} W(y_i|x_i, s_i)$$

for all $y^n \in \mathcal{Y}^n$ and $x^n \in \mathcal{X}^n$. Then the *arbitrarily varying channel (AVC)* $\mathcal{W}$ to the legitimate receiver is given by the family of channels for all state sequences $s^n \in \mathcal{S}^n$, i.e.,

$$\mathcal{W} \coloneqq \big\{W^n(\cdot|\cdot, s^n) : s^n \in \mathcal{S}^n\big\}.$$

Further, for any probability distribution $q \in \mathcal{P}(\mathcal{S})$ we define the *averaged channel* to the legitimate receiver as

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

Similarly, for given state sequence $s^n \in \mathcal{S}^n$ we define the channel to the wiretapper as $V^n(z^n|x^n, s^n) \coloneqq \prod_{i=1}^{n} V(z_i|x_i, s_i)$ for all $z^n \in \mathcal{Z}^n$ and $x^n \in \mathcal{X}^n$, and, accordingly, $\mathcal{V} \coloneqq \{V^n(\cdot|\cdot, s^n) : s^n \in \mathcal{S}^n\}$ and $V_q(z|x) = \sum_{s\in\mathcal{S}} V(z|x, s)q(s)$ for $q \in \mathcal{P}(\mathcal{S})$.

Definition 1: The *arbitrarily varying wiretap channel (AVWC)* $\mathfrak{W}$ is given by the families of pairs of channels with common input as

$$\mathfrak{W} \coloneqq \big\{\big(W^n(\cdot|\cdot, s^n), V^n(\cdot|\cdot, s^n)\big) : s^n \in \mathcal{S}^n\big\}.$$

The task is now to establish a reliable communication between the transmitter and the legitimate receiver in the presence of unknown varying channel conditions and, at the same time, keeping the confidential information secret from the wiretapper. This is formalized as follows.

Definition 2: A *deterministic* (n, J_n)*-code* $\mathcal{C}_{\text{det}}$ for the AVWC $\mathfrak{W}$ consists of a stochastic encoder

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

i.e., a stochastic matrix, with a set of confidential messages $\mathcal{J}_n \coloneqq \{1, ..., J_n\}$ and a collection of disjoint decoding sets

$$\big\{\mathcal{D}_j \subset \mathcal{Y}^n : j \in \mathcal{J}_n\big\}.$$

Using the code $\mathcal{C}_{\text{det}}$, the average probability of error at the legitimate receiver for state sequence $s^n \in \mathcal{S}^n$ is given by

$$\bar{e}_n(s^n|\mathcal{C}_{\text{det}}) \coloneqq \frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{x^n\in\mathcal{X}^n} E(x^n|j)W^n(\mathcal{D}_j^c|x^n, s^n).$$

We further define the maximum as

$$\bar{e}_n(\mathcal{C}_{\text{det}}) \coloneqq \max_{s^n\in\mathcal{S}^n} \bar{e}_n(s^n|\mathcal{C}_{\text{det}}).$$

To ensure that the confidential message is kept secret from the wiretapper for all state sequences $s^n \in \mathcal{S}^n$, we require $\max_{s^n\in\mathcal{S}^n} I(J; Z_{s^n}^n|\mathcal{C}_{\text{det}}) \le \epsilon_n$ for some (small) $\epsilon_n > 0$ with J the random variable uniformly distributed over the set of confidential messages $\mathcal{J}_n$ and $Z_{s^n}^n = (Z_{s_1}, Z_{s_2}, ..., Z_{s_n})$ the output at the wiretapper for state sequence $s^n \in \mathcal{S}^n$. This criterion is known as *strong secrecy* [12].

Definition 3: A non-negative number R_S is an *achievable secrecy rate* for the AVWC $\mathfrak{W}$ if for all $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of (n, J_n)-codes $\mathcal{C}_{\text{det}}$ such that for all $n \ge n(\delta)$ we have $\frac{1}{n}\log J_n \ge R_S - \delta$ and

$$\max_{s^n\in\mathcal{S}^n} I(J; Z_{s^n}^n|\mathcal{C}_{\text{det}}) \le \epsilon_n$$

while $\bar{e}_n(\mathcal{C}_{\text{det}}), \epsilon_n \to 0$ as $n \to \infty$. The *secrecy capacity* $C_S(\mathfrak{W})$ is given by the largest achievable secrecy rate.

Remark 1: Note that the definitions require that we have to find codes such that $\bar{e}_n(s^n|\mathcal{C}_{\text{det}}) \to 0$ and $I(J; Z_{s^n}^n|\mathcal{C}_{\text{det}}) \to 0$ as $n \to \infty$ for all state sequences $s^n \in \mathcal{S}^n$ simultaneously. This means the codes are universal with respect to the state sequences.

III. The Role of Common Randomness

Here we assume that all parties, i.e., the legitimate users and the wiretapper, have access to a common randomness. This assumption can be motivated by the fact that this is realized over a public channel which is open to the wiretapper.

Remark 2: If the wiretapper has no access to the common randomness, the legitimate users can immediately use this resource to create a secret key corresponding to the size of the common randomness and therewith keep the confidential information completely secret from the wiretapper.

But even if common randomness cannot be used as a secret key, it is an important resource to establish reliable communication over arbitrarily varying channels. It has been shown for ordinary AVCs [13–16] that for symmetrizable channels the random code capacity is positive while the deterministic code capacity is zero. Thus, in these scenarios common randomness is a necessary and important resource for reliable communication.

But common randomness has also an impact on the behavior and the abilities of potential wiretappers. A passive wiretapper is unaware of the actual channel conditions or at least does not exploit the knowledge about the common randomness to influence the channel conditions. On the other hand, an active wiretapper can advantageously use this knowledge to influence and control the actual state sequence of the legitimate users. This is further analyzed in the following.

IV. Passive Wiretappers

A passive wiretapper does not influence the channel conditions of the legitimate users and, accordingly, simply tries to eavesdrop the communication. Then, the state sequence only reflects the influence of channel uncertainty and, in particular, does not depend on the common randomness. This is the classical wiretap scenario which is analyzed for arbitrarily varying channels in [10, 11] under the strong secrecy criterion.

If common randomness is available, the legitimate users can use this resource to coordinate their choice of encoder and decoder. This leads to the following definition.

Definition 4: A *random* $(n, J_n, \mathcal{U}_n, P_U)$*-code* $\mathcal{C}_{\text{ran}}$ for the AVWC $\mathfrak{W}$ with passive wiretapper is given by a family of deterministic codes $\{\mathcal{C}_{\text{det}}(u) : u \in \mathcal{U}_n\}$ together with a random variable choosing u according to $P_U \in \mathcal{P}(\mathcal{U}_n)$.

Using the random code $\mathcal{C}_{\text{ran}}$, the mean average probability of error at the legitimate receiver for state sequence $s^n \in \mathcal{S}^n$ is then given by $\bar{e}_n(s^n|\mathcal{C}_{\text{ran}}) = \mathbb{E}_U \bar{e}_n(s^n|\mathcal{C}_{\text{det}}(U))$, i.e.,

$$\bar{e}_n(s^n|\mathcal{C}_{\text{ran}}) := \frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{u\in\mathcal{U}_n}\sum_{x^n\in\mathcal{X}^n} E(x^n|j,u) \times W^n\big((\mathcal{D}_j(u))^c|x^n,s^n\big)P_U(u) \tag{1}$$

and, the maximum by $\bar{e}_n(\mathcal{C}_{\text{ran}}) := \max_{s^n\in\mathcal{S}^n} \bar{e}_n(s^n|\mathcal{C}_{\text{ran}})$.

The definitions of a common randomness assisted achievable secrecy rate and the corresponding secrecy capacity $C_{S,\text{ran}}(\mathfrak{W})$ are defined accordingly by replacing the code $\mathcal{C}_{\text{det}}$ by $\mathcal{C}_{\text{ran}}$ in Definition 3 as following.

Definition 5: A non-negative number R_S is a *common randomness assisted achievable secrecy rate* for the AVWC $\mathfrak{W}$ with passive wiretapper if for all $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, J_n, \mathcal{U}_n, P_U)$-codes $\mathcal{C}_{\text{ran}}$ such that for all $n \geq n(\delta)$ we have $\frac{1}{n}\log J_n \geq R_S - \delta$ and

$$\max_{s^n\in\mathcal{S}^n} \mathbb{E}_U I(J; Z^n_{s^n}|\mathcal{C}_{\text{det}}(U)) \leq \epsilon_n \tag{2}$$

while $\bar{e}_n(\mathcal{C}_{\text{ran}}), \epsilon_n \to 0$ as $n \to \infty$. The *common randomness assisted secrecy capacity* or *passive secrecy capacity* $C_{S,\text{ran}}(\mathfrak{W})$ is given by the largest achievable secrecy rate.

Definition 6: A channel to the wiretapper is called a *best channel* if there exists a channel $V_{q^*} \in \{V_q : q \in \mathcal{P}(\mathcal{S})\}$ such that all other channels from $\{V_q : q \in \mathcal{P}(\mathcal{S})\}$ are degraded versions of V_{q^*}. Then it holds

$$X - Z_{q^*} - Z_q \qquad \text{for all } q \in \mathcal{P}(\mathcal{S})$$

where Z_q denotes the output of the channel V_q, $q \in \mathcal{P}(\mathcal{S})$.

With this we get an achievable secrecy rate for the AVWC with passive wiretapper.

Proposition 1 ([10, 11]): Under the assumption of a best channel to the wiretapper, for the common randomness assisted secrecy capacity $C_{S,\text{ran}}(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ with passive wiretapper it holds that

$$C_{S,\text{ran}}(\mathfrak{W}) \geq \max_{p\in\mathcal{P}(\mathcal{X})}\big(\min_{q\in\mathcal{P}(\mathcal{S})} I(p,W_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(p,V_q)\big).$$

For the following observation we need the concept of symmetrizability.

Definition 7: An AVC $\mathcal{W}$ is called *symmetrizable* if there exists a stochastic matrix $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that

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

holds for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$.

Then, the common randomness assisted secrecy capacity displays the following behavior.

Proposition 2 ([10, 11]): If the common randomness assisted secrecy capacity of the AVWC $\mathfrak{W}$ with passive wiretapper satisfies $C_{S,\text{ran}}(\mathfrak{W}) > 0$, then the deterministic code secrecy capacity is given by

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

if and only if the AVC $\mathcal{W}$ is non-symmetrizable.

If the AVC $\mathcal{W}$ is non-symmetrizable, then it always holds that $C_S(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$.

V. Active Wiretappers

An active wiretapper exploits its knowledge about the common randomness to maliciously influence the channel conditions of the legitimate users. Accordingly, the state sequence depends now on the outcome of the random experiment.

The definitions of a *common randomness assisted achievable secrecy rate* and the *common randomness assisted secrecy capacity* or *active secrecy capacity* $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W})$ for the AVWC $\mathfrak{W}$ with active wiretapper are defined accordingly, by letting the state sequence in (1) and (2) in Definitions 4 and 5 be depend on the outcome of the random experiment, i.e., $s^n = s^n(u) \in \mathcal{S}^n$. Thus, the probability of error is given by

$$\bar{e}_n(\mathcal{C}^{\text{active}}_{\text{ran}}) := \frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{u\in\mathcal{U}_n}\sum_{x^n\in\mathcal{X}^n} E(x^n|j,u) \times W^n\big((\mathcal{D}_j(u))^c|x^n,s^n(u)\big)P_U(u) \tag{3}$$

and the mean secrecy criterion by

$$\mathbb{E}_U I(J; Z^n_{s^n(U)}|\mathcal{C}_{\text{det}}(U)) \leq \epsilon_n. \tag{4}$$

Conditions (3) and (4) show that an active wiretapper has different strategies. One the one hand, it can try to maximize the information leaked to him by choosing the state sequence such that (4) is maximized. Another strategy is to disturb the communication of the legitimate users by choosing the state sequence such that the probability of decoding error is maximized. Of course, any combination is also valid.

Obviously, since an active wiretapper is more powerful than a passive wiretapper, it must always hold that

$$C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) \leq C_{S,\text{ran}}(\mathfrak{W}). \tag{5}$$

A. Positive Active Secrecy Capacity

In the following we show that if $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) > 0$, we actually have equality in (5), i.e., $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$.

Theorem 1: If $C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) > 0$, then

$$C^{\text{active}}_{S,\text{ran}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W}).$$

Proof: The proof strategy is inspired by techniques for the ordinary AVC; more precisely the *random code reduction* [10, 11, 14] and the *elimination of randomness* [14].

Let $\delta > 0$, $\lambda > 0$, and $\epsilon' > 0$ be arbitrary. Now, we start with a random $(n, J_n, \mathcal{U}_n, P_U)$-code $\mathcal{C}_{\text{ran}}$ for the AVWC $\mathfrak{W}$ with passive wiretapper, cf. Definition 4, which is optimal in the sense that it achieves the secrecy rate $R_S \geq C_{S,\text{ran}}(\mathfrak{W}) - \delta$ with $\bar{e}_n(\mathcal{C}_{\text{ran}}) = \max_{s^n\in\mathcal{S}^n} \mathbb{E}_U \bar{e}_n(s^n|\mathcal{C}_{\text{det}}(U)) \leq \lambda$ and $\max_{s^n\in\mathcal{S}^n} \mathbb{E}_U I(J; Z^n_{s^n}|\mathcal{C}_{\text{det}}(U)) \leq \epsilon'$. So far we cannot say anything about the common randomness that is needed for this code to be optimal, especially the size of $\mathcal{U}_n$ can be arbitrary large. But from the *random code reduction* in [10, 11] we can conclude on the following.

Lemma 1 ([10, 11]): Let $\mathcal{C}_{\text{ran}}$ be a random $(n, J_n, \mathcal{U}_n, P_U)$-code for the AVWC $\mathfrak{W}$ with passive wiretapper consisting of a family $\{\mathcal{C}_{\text{det}}(u) : u \in \mathcal{U}_n\}$ of deterministic codes where u is chosen according to the distribution $P_U \in \mathcal{P}(\mathcal{U}_n)$. Then let

$$\bar{e}_n(\mathcal{C}_{\text{ran}}) \leq \lambda, \quad \text{and} \quad \max_{s^n\in\mathcal{S}^n} \mathbb{E}_U I(J; Z^n_{s^n}|\mathcal{C}_{\text{det}}(U)) \leq \epsilon'. \tag{6}$$

Then for any ϵ and K that satisfy

$$\epsilon > 4\max\{\lambda, \epsilon'\} \quad \text{and} \quad K > \frac{2n\log|\mathcal{X}|}{\epsilon}(1 + n\log|\mathcal{S}|),$$

there exist K codes $\mathcal{C}_{\text{det}}(i)$, $i = 1, ..., K$ chosen from the random code $\mathcal{C}_{\text{ran}}$ by random selection such that

$$\frac{1}{K}\sum_{i=1}^{K} \bar{e}_n(s^n|\mathcal{C}_{\text{det}}(i)) \leq \epsilon \text{ and } \frac{1}{K}\sum_{i=1}^{K} I(J; Z_{s^n}^n|\mathcal{C}_{\text{det}}(i)) \leq \epsilon \quad (7)$$

for all $s^n \in \mathcal{S}^n$.

Lemma 1 shows that for any random code $\mathcal{C}_{\text{ran}}$ for the AVWC $\mathfrak{W}$ with passive wiretapper, there exists another "reduced" random code $\tilde{\mathcal{C}}_{\text{ran}}$ uniformly distributed over K deterministic codes with an average probability of error and a mean secrecy criterion which fulfill (7).

Furthermore, from Lemma 1, cf. also [10, 11], we see that it is sufficient to select no more than $K = n^3$ deterministic codes to obtain a random code $\tilde{\mathcal{C}}_{\text{ran}}$ with the desired properties achieving the same secrecy rate as the original code $\mathcal{C}_{\text{ran}}$.

Up to now we have ensured that there is a random code $\tilde{\mathcal{C}}_{\text{ran}}$ with polynomial many elements for the AVWC $\mathfrak{W}$ with passive wiretapper with the desired properties. The next step is to make this code suitable for the case with an active wiretapper as well.

We follow the idea of *elimination of randomness* and combine the reduced random code $\tilde{\mathcal{C}}_{\text{ran}}$ with a code $\mathcal{C}_{\text{ran}}^{\text{active}}$ suitable for the AVWC $\mathfrak{W}$ with active wiretapper. Since $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$, this code achieves positive secrecy rate and, thus, is suitable to indicate which element of $\tilde{\mathcal{C}}_{\text{ran}}$ is actually used in the following. Since $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$ there exists a random code $\mathcal{C}_{\text{ran}}^{\text{active}}$ for the AVWC $\mathfrak{W}$ with active wiretapper consisting of a family $\{\mathcal{C}_{\text{det}}^{\text{active}}(u) : u \in \mathcal{U}_n\}$ with stochastic encoder

$$E' : \{1, ..., n^3\} \times \mathcal{U}_n \to \mathcal{P}(\mathcal{X}^{k_n}),$$

and a collection of disjoint decoding sets

$$\left\{\mathcal{D}_l'(u) \subset \mathcal{Y}^{k_n} : l \in \{1, ..., n^3\}, u \in \mathcal{U}_n\right\}$$

with $\frac{k_n}{n} \to 0$ as $n \to \infty$ with probability of error

$$\frac{1}{n^3}\sum_{l=1}^{n^3}\sum_{u\in\mathcal{U}_n}\sum_{x^{k_n}\in\mathcal{X}^{k_n}} E'(x^{k_n}|l, u) \times W^{k_n}\big((\mathcal{D}_l'(u))^c|x^{k_n}, s^{k_n}(u)\big)P_U(u) \leq \epsilon_n$$

and further

$$\mathbb{E}_U I(L; Z_{s^n(U)}^n|\mathcal{C}_{\text{det}}^{\text{active}}(U)) \leq \epsilon_n$$

for all $s^{k_n}(u) \in \mathcal{S}^{k_n}$ with $\epsilon_n \to 0$ as $n \to \infty$.

Now, the final code for the AVWC $\mathfrak{W}$ with active wiretapper is given by the composition of encoders $E'(x^{k_n}|l, u)E(x^n|j, l)$ transmitting a message from $\{1, ..., n^3\} \times \mathcal{J}_n$ of length $k_n + n$, and decoding sets $\mathcal{D}_l'(u)\mathcal{D}_j(l)$, where the channel is determined by the state sequence $s^{k_n+n} \in \mathcal{S}^{k_n+n}$.

Since $\frac{k_n}{n} \to 0$ as $n \to \infty$, the resources "wasted" for indicating which code is actually used, vanishes so that we end up with $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$ completing the proof. Note that Lemma 1 ensures that the ratio $\frac{k_n}{n}$ vanishes by letting $\tilde{\mathcal{C}}_{\text{ran}}$ be of polynomial size only. ∎

With this and Proposition 1 we immediately obtain an achievable secrecy rate for the AVWC with active wiretapper.

Corollary 1: If $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$ and if there exists a best channel to the wiretapper, then for $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ with active wiretapper it holds that

$$C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) \geq \max_{p\in\mathcal{P}(\mathcal{X})}\big(\min_{q\in\mathcal{P}(\mathcal{S})} I(p, W_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(p, V_q)\big).$$

The previous discussion shows that the strategy of an active wiretapper must be to choose the state sequence in such a way that the active secrecy capacity becomes zero, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$. Since otherwise, we have $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$, cf. Theorem 1, which means that the legitimate users can operate at the same rate as if the wiretapper would be passive, i.e., not controlling the channel state.

B. Zero Active Secrecy Capacity

For the AVWC $\mathfrak{W}$ with passive wiretapper we know from Proposition 2, cf. also [10, 11], that if $C_{S,\text{ran}}(\mathfrak{W}) > 0$ and $C_S(\mathfrak{W}) = 0$, then the AVC $\mathcal{W}$ to the legitimate receiver must be symmetrizable, cf. Definition 7. Thus, symmetrizability is a necessary condition condition for $C_S(\mathfrak{W}) = 0$. But from [10, 11] we know that if $C_{S,\text{ran}}(\mathfrak{W}) > 0$, this is condition is also sufficient for $C_S(\mathfrak{W}) = 0$.

Here we want to study the AVWC $\mathfrak{W}$ with active wiretapper in a similar way. If $C_{S,\text{ran}}(\mathfrak{W}) > 0$ and $C_{\text{ran}}^{\text{active}}(\mathcal{W}) > 0$, the question is if it is possible to have $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$.

Remark 3: For a positive active secrecy capacity of the AVWC $\mathfrak{W}$ with active wiretapper, it is clear that the active capacity of the AVC $\mathcal{W}$ to the legitimate receiver must be positive. Since otherwise, no communication would be possible even in the absence of the wiretapper. Thus, $C_{\text{ran}}^{\text{active}}(\mathcal{W}) > 0$ is a necessary condition for $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$.

Proposition 3: If $C_{S,\text{ran}}(\mathfrak{W}) > 0$, then symmetrizability of the AVC $\mathcal{W}$ is a necessary condition for $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$.

Proof: We prove the proposition by contradiction. We assume that the AVC $\mathcal{W}$ is non-symmetrizable. Then we know from [10, 11] that the deterministic code and common randomness assisted code secrecy capacities are equal, i.e., $C_S(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W}) > 0$. This means that there is a deterministic code which achieves the desired rate. Such a code can be considered as a special random code with cardinality $|\mathcal{U}_n| = 1$. The consequence is that the active wiretapper "becomes" a passive wiretapper since its knowledge about the common randomness is useless. Thus, we end up with $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$ which contradicts the assumption. This establishes symmetrizability as a necessary condition for $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$. ∎

Next we show for a special case that a certain symmetrizability condition is also sufficient for $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$.

1) Definitions and Associated AVC: We follow [17] and assume the common randomness U to be binary, i.e., $\mathcal{U}^n := \mathcal{U}_n = \{0, 1\}^n$. Further, all users observe a sequence $u^n = (u_1, ..., u_n) \in \mathcal{U}^n$ of length n and input x^n and state sequences

s^n depend on the common randomness by binary-valued functions g and f so that $x^n = g^n(u^n)$ and $s^n = f^n(u^n)$. Then we have a set of codewords $\{g_j^n(u^n) \in \mathcal{X}^n : j \in \mathcal{J}_n, u^n \in \mathcal{U}^n\}$ and a collection of disjoint decoding sets $\{\mathcal{D}_j(u^n) \subset \mathcal{Y}^n : j \in \mathcal{J}_n, u^n \in \mathcal{U}^n\}$.

Further, the active wiretapper exploits its knowledge about the common randomness in such a way that it has a function $f^n : \mathcal{U}^n \to \mathcal{S}^n$ for selecting the state sequence. Then the corresponding average probability of a successful transmission to the legitimate receiver over the AVC $\mathcal{W}$ is

$$\frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{u^n\in\mathcal{U}^n} P_U^n(u^n)W^n\big(\mathcal{D}_j(u^n)|g_j^n(u^n), f^n(u^n)\big) > 1-\lambda \tag{8}$$

for some (small) $\lambda > 0$, cf. also (3).

In the following we restrict the possible strategies of the wiretapper. As in [17] we restrict the class of functions g^n and f^n to be of the form

$$g_j^n(u^n) = \big(g_{j,1}(u_1), ..., g_{j,n}(u_n)\big) \tag{9a}$$
$$f^n(u^n) = \big(f_1(u_1), ..., f_n(u_n)\big). \tag{9b}$$

This means the encoding and state selection process depend only on the current realization of the common randomness and not on the whole sequence. Therefore, we have sets of functions $\mathcal{G} := \{g : \mathcal{U} \times \mathcal{J}_n \to \mathcal{X}\}$ and $\mathcal{F} := \{f : \mathcal{U} \to \mathcal{S}\}$.

Similarly as in [17], we define an associated AVC $\hat{\mathcal{W}}$ as

$$\hat{\mathcal{W}} := \big\{\hat{W}(\cdot,\cdot|\cdot, f) : f \in \mathcal{F}\big\}$$

with inputs $g : \mathcal{U} \to \mathcal{X}$, states $f : \mathcal{U} \to \mathcal{S}$, and output $(y, v) \in \mathcal{Y} \times \mathcal{V}$. In more detail, we set

$$\hat{W}(y, v|g, f) = P_V(v)\sum_{u=0}^{1} P_{U|V}(u|v)W\big(y|g(u), f(u)\big). \tag{10}$$

Here, $P_{U|V}$ is given by the 2×2 identity matrix so that $U = V$. Basically, we introduced the auxiliary random variable V to make use of proof techniques from [17]. With

$$\hat{\mathcal{D}}_j = \bigcup_{u^n\in\mathcal{U}^n}\big(\mathcal{D}_j(u^n)\times u^n\big) = \bigcup_{v^n\in\mathcal{V}^n}\big(\mathcal{D}_j(v^n)\times v^n\big)$$

and (9)-(10), we get for the probability of a successful transmission, cf. 8,

$$\begin{aligned}
&\frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{u^n\in\mathcal{U}^n} P_U^n(u^n)W^n\big(\mathcal{D}_j(u^n)|g_j^n(u^n), f^n(u^n)\big)\\
&\quad= \frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{v^n\in\mathcal{V}^n} P_V^n(v^n)\sum_{u^n\in\mathcal{U}^n} P_{U|V}^n(u^n|v^n)\\
&\qquad\qquad\times W^n\big(\mathcal{D}_j(v^n)|g_j^n(u^n), f^n(u^n)\big)\\
&\quad= \frac{1}{J_n}\sum_{j=1}^{J_n}\hat{W}^n\Big(\bigcup_{v^n\in\mathcal{V}^n}(\mathcal{D}_j(v^n)\times v^n)|g_j^n, f^n\Big)\\
&\quad= \frac{1}{J_n}\sum_{j=1}^{J_n}\hat{W}^n\big(\hat{\mathcal{D}}_j|g_j^n, f^n\big).
\end{aligned}$$

Thus, the random code capacity $C_{\text{ran}}^{\text{active}}(\mathcal{W})$ of the AVC $\mathcal{W}$ to the legitimate receiver (under the restrictions (9)) equals the deterministic code capacity $C_{\text{det}}(\hat{\mathcal{W}})$ of the associated AVC $\hat{\mathcal{W}}$, i.e.,

$$C_{\text{ran}}^{\text{active}}(\mathcal{W}) = C_{\text{det}}(\hat{\mathcal{W}}). \tag{11}$$

Thus, instead of analyzing $C_{\text{ran}}^{\text{active}}(\mathcal{W})$ directly, it suffices to study $C_{\text{det}}(\hat{\mathcal{W}})$.

Recall that we are interested in the case $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$ so that we study $C_{\text{ran}}^{\text{active}}(\mathcal{W}) = 0$ in the following. By (11) it suffices to study what happens if $C_{\text{det}}(\hat{\mathcal{W}}) = 0$.

2) Associated AVC with Zero Capacity: From [15] we know that the deterministic code capacity of an AVC $\hat{\mathcal{W}}$ is zero if $\hat{\mathcal{W}}$ is symmetrizable, i.e., we study if the condition

$$\sum_{f\in\mathcal{F}}\hat{W}(y, v|g, f)\tau(f|g') = \sum_{f\in\mathcal{F}}\hat{W}(y, v|g', f)\tau(f|g) \tag{12}$$

holds for every $g, g' \in \mathcal{G}$ and $(y, v) \in \mathcal{Y}\times\mathcal{V}$ for some stochastic matrix $\tau : \mathcal{G} \to \mathcal{F}$, cf. also Definition 7.

As in [17] we want to show that this implies the existence of a channel $\overline{W}$ whose ordinary capacity is zero so that $C_{\text{ran}}(\mathcal{W}) = 0$ and therewith $C_{S,\text{ran}}(\mathfrak{W}) = 0$ as well, cf. Remark 3.

In the following we analyze (12) in detail. Since $\hat{W}(y, v|g, f) = P_V(v)\sum_{u=0}^{1} W\big(y|g(u), f(u)\big)P_{U|V}(u|v)$, condition (12) yields

$$\begin{aligned}
&\sum_{f\in\mathcal{F}} P_V(v)\sum_{u=0}^{1} W\big(y|g(u), f(u)\big)P_{U|V}(u|v)\tau(f|g')\\
&\quad= \sum_{f\in\mathcal{F}} P_V(v)\sum_{u=0}^{1} W\big(y|g'(u), f(u)\big)P_{U|V}(u|v)\tau(f|g)\\
&\quad= P_V(v)\sum_{f\in\mathcal{F}}\sum_{u=0}^{1} W\big(y|g'(u), f(u)\big)P_{U|V}(u|v)\tau(f|g)\\
&\quad= P_V(v)\sum_{f\in\mathcal{F}}\sum_{u=0}^{1} W\big(y|g(u), f(u)\big)P_{U|V}(u|v)\tau(f|g').
\end{aligned}$$

Since $P_V(v) > 0$ for all $v \in \mathcal{V} = \{0, 1\}$, we have

$$\begin{aligned}
&\sum_{f\in\mathcal{F}}\sum_{u=0}^{1} W\big(y|g(u), f(u)\big)P_{V|U}(v|u)\tau(f|g')\\
&\qquad= \sum_{f\in\mathcal{F}}\sum_{u=0}^{1} W\big(y|g'(u), f(u)\big)P_{V|U}(v|u)\tau(f|g).
\end{aligned}$$

Since $P_{U|V}(u|v) = 1$ if $u = v$ and zero otherwise, this simplifies for $u = 0$ as

$$\sum_{f\in\mathcal{F}} W\big(y|g(0), f(0)\big)\tau(f|g') = \sum_{f\in\mathcal{F}} W\big(y|g'(0), f(0)\big)\tau(f|g) \tag{13}$$

and for $u = 1$ as

$$\sum_{f\in\mathcal{F}} W\big(y|g(1), f(1)\big)\tau(f|g') = \sum_{f\in\mathcal{F}} W\big(y|g'(1), f(1)\big)\tau(f|g). \tag{14}$$

For any $s \in \mathcal{S}$ and $u \in \mathcal{U} = \{0,1\}$ we define $\mathcal{F}_{u,s} = \big\{f \in \mathcal{F} : f(u) = s\big\}$, then (13) is equivalent to

$$\begin{aligned}\sum_{s\in\mathcal{S}} W(y|g(0),s) \sum_{f\in\mathcal{F}_{0,s}} \tau(f|g') \\ = \sum_{s\in\mathcal{S}} W(y|g'(0),s) \sum_{f\in\mathcal{F}_{0,s}} \tau(f|g)\end{aligned} \tag{15}$$

and, similarly, (14) is equivalent to

$$\begin{aligned}\sum_{s\in\mathcal{S}} W(y|g(1),s) \sum_{f\in\mathcal{F}_{1,s}} \tau(f|g') \\ = \sum_{s\in\mathcal{S}} W(y|g'(1),s) \sum_{f\in\mathcal{F}_{1,s}} \tau(f|g).\end{aligned} \tag{16}$$

3) Evaluation of Special Case: In the following we evaluate the case where it suffices for the wiretapper to choose a function of the form $f(u) = s$ for $u = 0, 1$, which means that W already has the property that (15) and (16) are satisfied. Similarly as in [17], let $\mathcal{X} = \{0, 1, ..., |\mathcal{X}|-1\}$ and set further

$$\hat{g}_0(0) = \hat{g}_0(1) = 0, \quad \hat{g}_i(0) = i, \quad \hat{g}_i(1) = (i+1) \mod |\mathcal{X}|.$$

Then (15) and (16) imply

$$\begin{aligned}\sum_{s\in\mathcal{S}} W(y|\hat{g}_i(0),s)\tau(s|\hat{g}_0) = \sum_{s\in\mathcal{S}} W(y|\hat{g}_0(0),s)\tau(s|\hat{g}_i) \\ = \sum_{s\in\mathcal{S}} W(y|0,s)\tau(s|\hat{g}_i) = \sum_{s\in\mathcal{S}} W(y|\hat{g}_i(1),s)\tau(s|\hat{g}_0)\end{aligned}$$

so that

$$\sum_{s\in\mathcal{S}} W(y|i,s)\tau(s|\hat{g}_0) = \sum_{s\in\mathcal{S}} W(y|i+1,s)\tau(s|\hat{g}_0)$$

for all $i = 0, 1, ..., |\mathcal{X}| - 1$. So for $q^* \in \mathcal{P}(\mathcal{S})$ defined by $q^*(s) = \tau(s|\hat{g}_0)$ we get

$$\sum_{s\in\mathcal{S}} W(y|x,s)q^*(s) = \sum_{s\in\mathcal{S}} W(y|x',s)q^*(s)$$

for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$. Hence the corresponding channel $\overline{W}(\cdot|\cdot) := \sum_{s\in\mathcal{S}} W(\cdot|\cdot,s)q^*(s)$ has identical rows so that its capacity is zero, i.e., $C(\overline{W}) = 0$, and so $C_{\text{ran}}(\mathcal{W}) = 0$ and $C_{S,\text{ran}}(\mathfrak{W}) = 0$.

Thus, we established equality of the random secrecy capacities of the AVWC $\mathfrak{W}$ for passive and active wiretappers,

$$C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W}) = 0.$$

VI. Discussion

For an AVC $\mathcal{W}$ it is shown that its deterministic capacity $C_{\text{det}}(\mathcal{W})$ displays a dichotomy behavior: it either equals its random capacity $C_{\text{ran}}(\mathcal{W})$ or else is zero [14, 15]. The main techniques to characterize this behavior are the *random code reduction*, *elimination of randomness*, and *symmetrizability*.

In this paper we analyzed the active secrecy capacity $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ with active wiretapper. We tried to characterize the relation between the active and passive secrecy capacities $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ and $C_{S,\text{ran}}(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ with active and passive wiretapper, respectively, in a similar fashion as for the deterministic code and random code capacities $C_{\text{det}}(\mathcal{W})$ and $C_{\text{ran}}(\mathcal{W})$ of an ordinary AVC $\mathcal{W}$.

Inspired by the techniques mentioned above, we were able to show that if the active secrecy capacity is positive, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$, then it is actually equal to its passive secrecy capacity, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$. For the case of a zero active secrecy capacity, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$, we showed that there exist situations where the passive secrecy capacity is also zero resulting again in equality, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$.

We established symmetrizability as a necessary condition for $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$. We were also able to establish a sufficient condition. A complete characterization is still open, i.e., if the discovered equality of active and passive secrecy capacities holds in general or if the active secrecy capacity can display a similar behavior as the deterministic code capacity of ordinary AVCs, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ can be zero while $C_{S,\text{ran}}(\mathfrak{W})$ is positive.

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] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

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

[5] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: proximity-based secure pairing using ambient wireless signals," in *Proc. Int. Conf. on Mobile Systems, Applications, and Services*, Washington, DC, USA, Jun. 2011, pp. 211–224.

[6] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity Results for Compound Wiretap Channels," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 60–64.

[7] 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.

[8] E. Ekrem and S. Ulukus, "On Gaussian MIMO Compound Wiretap Channels," in *Proc. Conf. Inf. Sciences and Systems*, Baltimore, MD, USA, Mar. 2010, pp. 1–6.

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

[10] I. Bjelaković, H. Boche, and J. Sommerfeld, "Strong Secrecy in Arbitrarily Varying Wiretap Channels," in *Proc. IEEE Inf. Theory Workshop*, Lausanne, Switzerland, Sep. 2012.

[11] ——, "Capacity Results for Arbitrarily Varying Wiretap Channels," will be published in Springer LNCS in Memory of Rudolf Ahlswede.

[12] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *EUROCRYPT 2000, Lecture Notes in Computer Science*. Springer-Verlag, May 2000, vol. 1807, pp. 351–368.

[13] D. Blackwell, L. Breiman, and A. J. Thomasian, "The Capacities of Certain Channel Classes under Random Coding," *Ann. Math. Stat.*, vol. 31, no. 3, pp. 558–567, 1960.

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

[15] I. Csiszár and P. Narayan, "The Capacity of the Arbitrarily Varying Channel Revisited: Positivity, Constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.

[16] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.

[17] R. Ahlswede and N. Cai, "Correlated Sources Help Transmission Over an Arbitrarily Varying Channel," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1254–1255, Jul. 1997.