Coding against a Limited-view Adversary: The Effect of Causality and Feedback

Qiaosheng (Eric) Zhang\textsuperscript{1} \hspace{1cm} Swanand Kadhe\textsuperscript{2}
Mayank Bakshi\textsuperscript{1} \hspace{1cm} Sidharth Jaggi\textsuperscript{1} \hspace{1cm} Alex Sprintson\textsuperscript{2}
\textsuperscript{1}Chinese University of Hong Kong \hspace{1cm} \textsuperscript{2}Texas A&M University

Abstract—We consider the problem of communication over a multi-path network in the presence of a causal adversary. The limited-view causal adversary is able to eavesdrop on a subset of links and also jam on a potentially overlapping subset of links based on the current and past information. To ensure that the communication takes place reliably and secretly, resilient network codes with necessary redundancy are needed. We study two adversarial models – additive and overwrite jamming and we optionally assume passive feedback from decoder to encoder, \textit{i.e.}, the encoder sees everything that the decoder sees. The problem assumes transmissions are in the large alphabet regime. For both jamming models, we find the capacity under three scenarios – reliability without feedback, reliability and secrecy without feedback, and jamming with feedback. We observe that, in comparison to the non-causal setting, the capacity with a causal adversary is strictly increased for a wide variety of parameter settings and present our intuition through several examples.

Index Terms—adversary, jamming, secrecy, causal, feedback

I. INTRODUCTION

We consider the following communication problem. Alice wishes to wirelessly transmit a message $m$ to receiver Bob by communicating over $C$ different frequencies. Their communication is intercepted by a limited-view adversary Calvin who has his receivers tuned to subset $Z_R$ of the frequencies, and has jammers tuned to a potentially overlapping subset $Z_W$. Due to the online nature of the channel, Calvin can only see the signal up to the current time to maliciously determine his jamming strategy for the current time instant. We wish to answer the following question: “\textit{What is the maximum rate such that Bob can decode the message successfully without knowing Calvin’s malicious strategy while keeping the message secret from Calvin?}” Additionally, when Alice can also hear the channel output, we wish to understand whether this knowledge can improve the best possible rate.

We model this problem as that of communication over a noiseless multi-path network consisting of $C$ parallel links between the sender and the receiver. As mentioned above, the adversary Calvin can eavesdrop on a subset $Z_R$ and jam on a subset $Z_W$. Subsets $Z_{RW}$, $Z_{RO}$ and $Z_{WO}$ represent the links that Calvin can both eavesdrop on and jam, only eavesdrop on (but not jam) and only jam (but not eavesdrop on) respectively. In addition, the sizes of $Z_{RW}$, $Z_{RO}$ and $Z_{WO}$ are bounded from $z_{RW}$, $z_{RO}$ and $z_{WO}$. The adversarial vector $\vec{z} = (z_{RW}, z_{RO}, z_{WO})$ measures Calvin’s power. Moreover, Calvin also knows the encoding and decoding schemes so that he may mimic Alice’s behavior to confuse Bob. We consider a causal constraint on Calvin’s behaviors, \textit{i.e.}, Calvin can only use the knowledge of symbols up to the current time slot to decide his jamming strategy.

The problem of communicating against a malicious adversary has been well studied in the past and the maximum possible rate has been characterized under various settings – both causal and non-causal. The non-causal setting is relatively well understood both in the classical error-correction setup \cite{1, 2, 3, 4} and the network error correction setting \cite{5, 6, 7, 8}. A key feature of these results is that in many of these, Calvin can decrease the capacity by one unit for each link that can be detected by Bob as having been corrupted and inflict “double-damage” on links which Bob cannot detect as having been corrupted. This heuristic also suggests an intuitive scheme for Alice – try to detect as many corrupted links as possible and treat those as erasures. Roughly speaking, the adversary’s ability can cause “double-damage” depends on whether or not it can induce a large enough set of links whose codewords are consistent with each other but decode to a possibly different message. Critically, this depends on his ability to be able to see the full codeword for each link in $Z_R$ before determining the optimal jamming strategy for $Z_W$.

In contrast, in the causal setting, by using stochastic encoding, the adversary may not be able to predict some of the future symbols, which can then be used to detect the set $Z_W$. Causal adversaries for classical channel coding and network coding problems have also been well studied \cite{9, 10, 11}. However, apart from special cases, the question of capacity remains open.

\textbf{Our contributions}

We consider the problem of causal jamming with an optional secrecy requirement. Taking cue from our prior work \cite{8}, we consider a finer characterization of the adversary’s power by classifying his controlled links into read-only, write-only, and read-and-write subsets. We examine this problem in two settings – additive and overwrite jamming. The motivation for an additive adversary comes from wireless networks, where, the adversary may add his own signal to the transmitted signal. On the other hand, the overwrite adversary models the adversarial action in a wired network, where the adversary is more likely to completely replace the true
transmitted packets with fake packets of his choice.\footnote{Notice that for a write only link, the overwrite adversary knows the output codewords while the additive adversary has no way to learn the output codewords.}  

In the setting without feedback, Theorems \ref{Theorem 3} and \ref{Theorem 4} state the capacity when secrecy is not required. Theorems \ref{Theorem 5} and \ref{Theorem 6} state our results with secrecy requirement and also without feedback. When passive feedback is available to the encoder, we characterize the capacity in Theorems \ref{Theorem 7} and \ref{Theorem 8}.

The rest of this paper is organized as follows. In Section II, we illustrate the role of causality in limiting the adversary’s power by giving three examples. We formally define the problem in Section III and state our main results with short proof sketches in Section IV. The detailed proofs are presented in Appendices A-D.

**II. Key ideas**

We use the following examples to illustrate the main ideas behind our schemes. To build some intuition into the problem, we first consider both non-causal and causal additive jamming on a simple network with seven parallel links, i.e., \(C = 7\).

**A. Prior works (Non-causal case)**

**Example 1** (Idea of achievability, pairwise-hashing scheme \cite{5}). The work of \cite{5} first came up with the pairwise-hashing scheme in 2005 and it considered the presence of a read/write adversary, namely \(z_{ro} = z_{wo} = 0\) in our scenario. Assume \(C = 7\) and \(z_{rw} = 3\). In this case, the maximum achievable rate is \(C - z_{rw} = 4\) by using the “pairwise-hashing” scheme (see Figure 1) to detect adversarial attacks (the proof is presented in Appendix B). In order to avoid potential jamming from the hidden adversary, the encoder encodes the message using a \((7, 4)\) Reed-Solomon code. The seven sub-codewords are transmitted on seven wireless channels separately. Moreover, the encoder also appends headers to the end of each codeword. The headers contain “hash keys” as well as “pairwise hashes” (Figure 1), which are used to “corroborate” the information of one link from the others. The adversary is able to replace the payloads, hash keys as well as “pairwise hashes” belonging to the code and also adopts “pairwise-hashing” scheme. Regardless of which attack the adversary attempts to impose, it is unable to figure out all the four uncorrupted links corresponding to the fake message \(m'\) which has same sub-codeword on \(Z_{RW}\). In this setting, the maximum achievable rate is \(C - z_{rw} = 2\) by using the “symmetrization” argument (correct RW corresponding to the seven links) for each link. For instance, the hash key \(\rho_1\) is generated for \(X_1\). Besides, we also append the hashes of each payload \((X_1, X_2, ..., X_7)\) and the hash key \(\rho_1\). The hashes of \(X_i\) and \(\rho_1\) is denoted by \(h_i\), so that the seven appended pairwise hashes are \(h_{41}, h_{42}, ..., h_{47}\).

The decoder cannot figure out the corrupted links belonging to \(Z_{RW}\) because of the “symmetrization” argument (correct message \(m\) vs fake message \(m'\)). In this setting, the maximum rate \(C - z_{wo} - 2z_{rw} = 1\) is achieved by Reed-Solomon code and no higher rate is possible.

**B. Causal case**

Now, we consider a causal restriction on the adversary, which limits his power. In the following example, we show that a higher rate is achievable with a causal adversary under the same parameter setting as in Example 2.

**Example 3** (Idea of achievability: Correspond to Theorem 1). Assume \(z_{ro} = 1, z_{wo} = 2\) and \(z_{rw} = 2\). In this scenario, \cite{8} shows that the maximum achievable rate is \(C - z_{rw} - z_{ro} = 3\). The encoder encodes the message using a \((7, 3)\) Reed-Solomon code and also adopts “pairwise-hashing” scheme. Regardless of which attack the adversary attempts to impose, it is unable to perform a “replacement” attack to prevent the decoder from figuring out the subset \(Z_{RW}\) with high probability. In the worst case, it can first eavesdrop any three channels \((z_{ro} + z_{rw})\) and choose a fake message \(m'\) which has same sub-codeword on \(Z_{RO}\). The adversary then “replaces” the sub-codewords on \(Z_{RW}\) with the new sub-codewords corresponding to \(m\). Therefore, the three links belonging to \(C - (Z_{RW} + Z_{WO})\) correspond to the correct message \(m\) while the three links belonging to \(Z_{RO} \cup Z_{RW} \) correspond to the fake message \(m'\). Moreover, the adversary can also choose one more link (belong to \(Z_{WO}\)) to corrupt, even if the link cannot map to \(m'\).

The decoder cannot figure out the corrupted links belonging to \(Z_{RW}\) because of the “symmetrization” argument (correct message \(m\) vs fake message \(m'\)). In this setting, the maximum rate \(C - z_{wo} - 2z_{rw} = 1\) is achieved by Reed-Solomon code and no higher rate is possible.
to eavesdrop the headers of $Z_{RO}$ when modifying the sub-codewords of $Z_{RW}$ because of causality. Therefore the adversary can only ensure the corroboration among $Z_{RW}$ and induce a fake 2-clique $\bar{z}$ ($z_{rw} = 2$). The two links comprising $Z_{WO}$ can be individually detected to have been jammed by the decoder $\mathcal{B}$ since a jamming attack on links which are unobserved by the jammer appear as “nonsense” and can be easily detected. The three sub-codewords ($C - z_{rw} - z_{wo}$), also form a correct 3-clique. By adopting the “finding largest clique” strategy (correct 3-clique > fake 2-clique), the decoder is able to decode the message $m$ using the three correct sub-codewords and $(7,3)$ Reed-Solomon code. In this scenario, the maximum achievable rate is $C - z_{rw} - z_{wo} = 3$.

If the adversary is able to access more links, we show that even if with causality, no reliable communication is possible.

**Example 4** (Idea of converse: Correspond to Theorem 1). Assume $z_{ro} = 1$, $z_{wo} = 3$ and $z_{rw} = 2$. In this scenario, the rate is limited to zero. For instance, if the same encoding scheme as Example 3 is performed, we know the adversary can induce a fake 2-clique while the uncorrupted links also form a correct 2-clique. The decoder would be confused by this “symmetrization” and as a result, cannot distinguish $m$ and $m'$. In Appendix B we prove that reliable communication is impossible no matter which encoding schemes are adopted. The maximum rate is $C - z_{wo} - 2z_{rw} = 0$.

### III. PROBLEM STATEMENT

The multi-path network model and the encoding/decoding processes are illustrated in Figure 2. In our setting, the multi-path network consists of $C$ parallel, directed links $L_1, L_2, \ldots, L_C$. For the equal link capacity network, each link is of unit capacity (one bit per channel use). For a general unequal link capacity network, the capacity of link $L_i$ is denoted by $u_i, \forall i \in \{0, 1, \ldots, C\}$. The total capacity of an unequal link capacity network is defined as $C$ bits per channel use, where $C := \sum_{i=1}^{C} u_i$. Notice that the capacity of the equal link capacity is $C$ bits per channel use. We also optionally consider passive feedback available causally at the transmitter, i.e., the transmitter overhears the received symbols at the decoder causally.

We begin by formally describing the encoder, decoder, and possible adversarial actions for a code of block length $n$, i.e., for a code that operates over $n$ time steps and $r$ rounds ($r \leq n$ with $r = 1$ denoting the case without feedback). For simplicity, we consider all the details for the equal link capacity case, and briefly present the results for the unequal link capacity case.

In the following, matrices $X = [X^{(1)} \cdots X^{(r)}]$ and $Y = [Y^{(1)} \cdots Y^{(r)}]$ respectively denote the collection of transmitted and received codewords across all links for all rounds. Here, $X^{(j)}$ (resp. $Y^{(j)}$) is a matrix whose $i$-th row $\vec{x}_i$ (resp. $\vec{y}_i$) denotes the transmitted (resp. received) codeword on link $L_i$ in the $j$-th round.

#### A. Encoder

The transmitter Alice encodes an $nR$-bit message $m$, where $R$ stands for the message rate. The message $m$ is assumed to be uniformly distributed over $\{0, 1\}^{nR}$. To perform stochastic encoding, Alice also generates a random key $k$, which is uniformly distributed over the finite field $\mathbb{F}_2$.

In the first round, Alice encodes $m$ into a collection of $C$ length-$n$ codewords $X^{(1)}, X^{(2)}, \ldots, X^{(C)}$. In this case, the encoder function for the first round takes the form

$$\Psi^{(1)} : \{0, 1\}^{nR} \times \mathbb{F}_2 \to \{0, 1\}^{Cn^{(1)}}.$$ 

If no feedback is present, no further actions are performed by Alice. In this case, $n^{(1)} = n$.

If feedback is present, in each subsequent round $j$, Alice’s codewords $X^{(j)}, X^{(j)}, \ldots, X^{(j)}_C$ are each of length $n^{(j)}$ and are determined by the message $m$, the random key $k$, and the feedback from prior rounds $Y^{(1)}, Y^{(j-1)}$. Formally, Alice’s encoder for the $i$-th round takes the form

$$\Psi^{(j)} : \{0, 1\}^{nR} \times \mathbb{F}_2 \times \prod_{i=1}^{j-1} \{0, 1\}^{Cn^{(i)}} \to \{0, 1\}^{Cn^{(j)}},$$ 

where, $\sum_{j=1}^{r} n^{(j)} = n$.

#### B. Decoder

The decoder Bob receives the code matrix $Y$, which may be different from $X$ and outputs a decoded message $\hat{m}$. The decoding function takes the form

$$\gamma(Y) : \{0, 1\}^{nC} \to \{0, 1\}^{nR}.$$ 

#### C. Adversary

Out of the $C$ links of the multi-path network, the adversary Calvin is able to eavesdrop (but not jam) a subset $Z_{RO}$ of size $z_{ro}$, jam (but not eavesdrop) a subset $Z_{WO}$ of size $z_{wo}$, both eavesdrop and jam a subset $Z_{RW}$ of size $z_{rw}$. Calvin’s power is measured by the adversarial vector $\vec{z} = (z_{rw}, z_{ro}, z_{wo}).$ The encoding and decoding strategies are known to Calvin. However, the two end users do not know how Calvin chooses $Z_{RO}, Z_{WO}$ and $Z_{RW}$ in advance.

---

**Fig. 2: System diagram for a multi-path network consisting of $C$ parallel links ($C = 7$ in this example).**
1) Additive and Overwrite Jamming: An additive jammer may induce additive bias on the transmitted codeword. Assume the codeword transmitted on $L_i$ is $\vec{X}_i$ and the bias is $\vec{E}_i$, the received codeword would be $\vec{Y}_i = \vec{X}_i + \vec{E}_i$. On the other hand, an overwrite adversary can overwrite the transmitted codeword by its own one directly. If the codeword is $\vec{X}_i$ and the bias is $\vec{E}_i$, the received codeword will be $\vec{Y}_i = \vec{E}_i$.

2) Causal Adversary: We restrict the adversary to be causal, i.e., the adversary is only allowed to jam the symbol of current time slot based on the observations of current and past time slots. More specifically, at any given time $t$, given a $C \times n$ code matrix $X$, the adversary can use the knowledge of only the first $t$ symbols from rows in subset $Z_{RW} \cup Z_{RO}$ in order to jam the $t$-th symbols from the rows in $Z_{RW} \cup Z_{WO}$.

In contrast, a non-causal adversary (see [8]) enjoys the full knowledge of all the symbols in the rows belonging to $Z_{RW} \cup Z_{RO}$ at all times. Obviously, the non-causal adversary has a stronger power and leads to a potentially lower rate.

3) Reliability and Security: Instead of a zero-error probability, we aim to achieve an $\varepsilon$-error probability. The communication is reliable if for any $\varepsilon > 0$, by choosing $n$ large enough, there exists a code of block length $n$ such that the error probability $P_e = Pr[m \neq \hat{m}] < \varepsilon$.

In terms of security, we aim to achieve the information-theoretically perfect secrecy. Assume the subset Calvin can eavesdrop is $Z_R = \{i_1, i_2, \ldots, i_z\}$ and the sub-codeword on $Z_R$ links is $X_{Z_R} = [\vec{X}_{i_1}, \vec{X}_{i_2}, \ldots, \vec{X}_{i_z}]$. To achieve security, the mutual-information between the message and Calvin’s observation should be zero, i.e., $I(M; X_{Z_R}) = 0$.

### IV. Main Results

In this section, we present the main results and sketch their proofs. The full proofs of the results can be found in Appendices B-D. We group our results into three parts – reliability without feedback, reliability and secrecy without feedback, and reliability with feedback. For each of these cases, we discuss the additive jamming and the overwrite jamming separately.

#### A. Reliability without feedback

For both additive and overwrite jammers, we obtain a two-part rate-region, i.e. positive-rate regime and zero-rate regime. The positive-rate regime for additive jamming is

$$Z_{pos,nf}^{add} = \{ \vec{z}: z_{wo} + 2z_{rw} < C \},$$

whereas for overwrite jamming, the positive-rate regime is

$$Z_{pos,nf}^{ow} = \{ \vec{z}: 2z_{wo} + 2z_{rw} < C \}.$$

The zero-rate regime equals the complement of the positive-rate regime. In the positive-rate regime, the achievability relies on erasure codes coupled with the pairwise-hashing scheme. The rate is limited to zero in the zero-rate regime.

First we consider the scenario when reliable communication is the only objective. For equal and unequal link capacity networks, for any $\vec{z} = (z_{rw}, z_{ro}, z_{wo})$ such that $z_{rw} + z_{ro} + z_{wo} \leq C$, the maximum achievable reliable rates for additive and overwrite jamming are characterized in the following.

**Theorem 1** (Additive jamming for equal link capacities). Under additive causal jamming, the maximum achievable reliable rate is

$$R_{j}^{add}(C, \vec{z}) = \begin{cases} C - (z_{rw} + z_{wo}), & \text{if } \vec{z} \in Z_{pos,nf}^{add} \\ 0, & \text{otherwise.} \end{cases}$$

**Theorem 2** (Overwrite jamming for equal link capacities). Under overwrite causal jamming, the maximum achievable reliable rate is

$$R_{j}^{ow}(C, \vec{z}) = \begin{cases} C - (z_{rw} + z_{wo}), & \text{if } \vec{z} \in Z_{pos,nf}^{ow} \\ 0, & \text{otherwise.} \end{cases}$$

For additive jamming and overwrite jamming, the two-part rate-regions are slightly different though the expressions are similar. Note that, regardless of the coding scheme, the best rate that we can hope for is $C - z_w$ since the adversary can corrupt any $z_w$ links. In the positive-rate regime, the best rate $C - z_w$ is indeed achievable. To achieve it, the encoder would use an erasure code to encode the message and apply the pairwise-hashing scheme to help detect errors. The decoder detects the corrupted links first (which are regarded as erasures) and then the message will be retrieved from the sub-codewords carried by the uncorrupted links.

However, no coding scheme (including pairwise-hashing) works for the zero-rate regime. The adversary can always adopt a “symmetrization” strategy so that the decoder is unable to distinguish the correct message and the fake message. The proof of the converse relies on an argument based on the Singleton bound [2] that we present in Appendix B.
Unequal link capacities: To incur maximum damage, the adversary may choose links with highest sum-rate to attack. We define the total capacity of any subset of size \( w \) links as \( U_w \). Different choice of the subsets may incur different values of \( U_w \). Typically, the notation \( (U_w)_{\text{max}} \) is used to denote the maximum value of \( U_w \), i.e., the largest sum-capacity of all possible subsets of size \( w \). Similar to the situation with equal link capacities, the main idea is also encoding by erasure codes as well as采用“pairwise-hashing” scheme to detect adversarial attacks. However, the only difference is that the maximum rate depends on Calvin’s ability to corrupt the links with largest sum-capacities.

**Theorem 3** (Additive jamming for unequal link capacities). Under additive causal jamming, the maximum achievable reliable rate is

\[
R_{j,\text{add}}(\vec{z}) = \begin{cases} \hat{C} - (U_{z_{rw} + z_{wo}})_{\text{max}}, & \text{if } \vec{z} \in Z_{\text{pos},n,f}^{\text{add}} \\ 0, & \text{otherwise} \end{cases}
\]

**Theorem 4** (Overwrite jamming and unequal link capacities). Under overwrite causal jamming, the maximum achievable reliable rate is

\[
R_{j,\text{ow}}(\vec{z}) = \begin{cases} \hat{C} - (U_{z_{rw} + z_{wo}})_{\text{max}}, & \text{if } \vec{z} \in Z_{\text{pos},n,f}^{\text{ow}} \\ 0, & \text{otherwise} \end{cases}
\]

B. Reliability and secrecy without feedback

In this section, we consider the scenario wherein Calvin tries to learn some information about Alice’s message from the links he eavesdrops. Besides reliable communication, we also want to prevent Calvin from gaining any information about the message. For this, we consider information-theoretically perfect secrecy, which requires that \( I(M; X_{Z_R}) = 0 \), where \( X_{Z_R} \) is the sub-codeword transmitted on the links in \( Z_R \). In the following, we characterize the reliable and secure rate region in the equal link capacity case for the causal adversary.

**Theorem 5** (Additive, causal jamming with secrecy, equal link capacities). Under additive causal jamming, the maximum achievable reliable and secret rate is

\[
R_{j,\text{add}}(\vec{z}) = \begin{cases} (C - (z_{wo} + z_{ro} + 2z_{rw}))^{+}, & \text{if } \vec{z} \in Z_{\text{pos},n,f}^{\text{add}} \\ 0, & \text{otherwise} \end{cases}
\]

where \((x)^+\) is defined as \( (x)^+ = \max \{0, x\} \).

**Theorem 6** (Overwrite, causal jamming with secrecy, equal link capacities). Under overwrite causal jamming, the maximum achievable reliable and secret rate is

\[
R_{j,\text{ow}}(\vec{z}) = \begin{cases} (C - (z_{wo} + z_{ro} + 2z_{rw}))^{+}, & \text{if } \vec{z} \in Z_{\text{pos},n,f}^{\text{ow}} \\ 0, & \text{otherwise} \end{cases}
\]

where \((x)^+\) is defined as \( (x)^+ = \max \{0, x\} \).

The converse for the positive-rate regime (for both additive and overwrite jamming) follows from the standard information-theoretic inequalities, where we use the secrecy condition that any subset of \( z_r = (z_{rw} + z_{ro}) \) links cannot carry any meaningful information. In the achievable scheme, Alice needs to mix her message with \( z_r \) random keys and then use the reliable encoding scheme consisting of pairwise hashing and erasure coding. For the zero-rate regime, the converse is based on the Singleton-type arguments similar to the only reliability case. We present the detail proof in Appendix C.

C. Reliability with passive feedback

In this section, we examine the effect of passive feedback on the capacity under jamming for both additive and overwrite settings. For both these cases, the parameter space again decomposes into two parts - the weak adversary regime and strong adversary regime.

The main idea for achievability of the claimed rate in the weak adversary regime is to use a two-round code. The first round involves sending a code that can handle up to \( z_{rw} + z_{wo} \) erasures. At the end of the first round, Alice sees the codewords received by Bob and determines the links which have been corrupted. In the next round, Alice sends a random hash of all the received codewords by Bob on the uncorrupted links from first round. Bob can then check the received values from the second round to determine the links where the hash values do not match the received codeword and treat those links as erasures.

The above scheme works as long as there is at least one link whose output is not seen by Calvin. This corresponds exactly to the condition for the weak adversary in the following theorems. If Calvin is able to see the output of all the links, he is as powerful as Alice and feedback no longer helps.

**Theorem 7** (Additive Jamming with Causal Feedback). Under an additive jamming with causal feedback, the capacity is

\[
R_{j,\text{add}}^{\text{add}} = \begin{cases} 0, & \text{if } z_r = C \text{ and } C \leq 2z_w \\ C - z_w, & \text{otherwise} \end{cases}
\]

**Theorem 8** (Overwrite Jamming with Causal Feedback). Under an overwrite jamming with causal feedback, the capacity is

\[
R_{j,\text{ow}}^{\text{add}} = \begin{cases} \max \{C - 2z_w, 0\}, & \text{if } z_{ro} + z_{rw} + z_{wo} = C \\ C - z_w, & \text{otherwise} \end{cases}
\]

As earlier, we present the detailed proof in Appendix D.
REFERENCES

[1] I. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960. [Online]. Available: [http://dx.doi.org/10.1137/01080018](http://dx.doi.org/10.1137/01080018)

[2] R. C. Singleton, “Maximum distance q-nary codes,” *Information Theory, IEEE Transactions on*, vol. 10, no. 2, pp. 116–118, Apr 1964.

[3] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II,” in *Proc. EUROCRYPT 84 workshop on Advances in cryptography: theory and application of cryptographic techniques*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 33–51.

[4] A. Lapidoth and P. Narayan, “Reliable communication under channel uncertainty,” *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.

[5] S. Jaggi, M. Langberg, T. Ho, and M. Effros, “Correction of adversarial errors in networks,” in *Proceedings of International Symposium in Information Theory (ISIT 2005)*, Adelaide, Australia, 2005, pp. 1455–1459.

[6] H. Yao, D. Silva, S. Jaggi, and M. Langberg, “Network codes resilient to jamming and eavesdropping,” in *Proc. Workshop on Network Coding Theory and Applications*, Toronto, Canada, Jun. 9–11 2010.

[7] S. Jaggi and M. Langberg, “Network security,” in *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, Eds. Academic Press, 2012.

[8] Q. Zhang, S. Kadhe, M. Bakshi, S. Jaggi, and A. Sprintson, “Talking reliably, secretly, and efficiently: A complete characterization,” Accepted for ITW 2015. Long version available at [http://personal.ie.cuhk.edu.hk/~muyank/ZhangKBJS14.pdf](http://personal.ie.cuhk.edu.hk/~muyank/ZhangKBJS14.pdf)

[9] B. Dey, S. Jaggi, and M. Langberg, “Codes against online adversaries, part i: Large alphabets,” *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3304–3316, 2013.

[10] L. Nutman and M. Langberg, “Adversarial models and resilient schemes for network coding,” in *Proc. IEEE Int. Symp. Information Theory*, Toronto, Canada, Jul. 6–11, 2008, pp. 171–175.

[11] D. Blackwell, L. Breiman, and A. Thomasian, “The capacities of certain channel classes under random coding,” *Annals of Mathematical Statistics*, vol. 31, no. 3, pp. 558–567, 1960.

APPENDIX A

**AUXILIARY LEMMAS**

**Definition 1** (Matrix-hashing). For any $N \times N$ square matrix $A$ and vector $\hat{\rho}$ of length $N$, the matrix-hash $h(A, \hat{\rho})$ is defined as $\hat{\rho} = A\hat{\rho}$, where $\hat{\rho}$ is also of length $N$.

**Lemma 1.** Let $q$ be a prime power. Suppose the $N \times N$ matrix $A$ is uniformly distributed over $\mathbb{F}^N \setminus \{0\}$ and the length-$N$ non-zero vector $\hat{\rho}$ is also uniformly distributed over $\mathbb{F}^N_0 \setminus \{0\}$. Let $\hat{A}$ be a random matrix independent from $A$ and $\hat{\rho}$ be distributed over $\mathbb{F}^N_q$ with some distribution $P_{A,\hat{\rho}}(\cdot)$. Then for any $\hat{\rho}$ not equal to zero,

$$\Pr_{A,\hat{\rho}}[\hat{A}\hat{\rho} = A\hat{\rho}] \leq \frac{1}{q}.$$

**Proof:** The matrices $A$ and $\hat{A}$ are uniformly distributed over finite field $\mathbb{F}_q$, and they are also independent from each other. Therefore the difference of the two matrices $\hat{A} - A$ should also be a matrix which is uniformly distributed over $\mathbb{F}^N_q \setminus \{0\}$. We use the fact that a random matrix over $\mathbb{F}_q$ is non-invertible with probability at most $\frac{1}{q}$. Since $\hat{\rho}$ is non-zero, the equation $(\hat{A} - A)\hat{\rho} = 0$ only if the matrix $\hat{A} - A$ is non-invertible. Therefore we conclude that

$$\Pr_{A,\hat{\rho}}[\hat{A}\hat{\rho} = A\hat{\rho}] = \Pr_{A,\hat{\rho}}[(\hat{A} - A)\hat{\rho} = 0] \leq \frac{1}{q}.$$

**Lemma 2.** Let $q$ be a prime power and suppose the $N \times N$ matrix $A$ is uniformly distributed over $\mathbb{F}^N_q$. Let $\theta$ be a random length-$N$ vector distributed over $\mathbb{F}^N_q$ independently from $A$ and according to an arbitrary distribution $P_{\theta}(\cdot)$. Then for any non-zero length-$N$ vector $\hat{\rho}$,

$$\Pr_{A,\hat{\rho}}[A\hat{\rho} = \theta] \leq \frac{N}{q}.$$

**Proof:** Each row $\hat{A}_i$ of matrix $A$ is uniformly distributed over the finite field $\mathbb{F}_q^N$ and independent from vector $\hat{\rho}$ by the definition of matrix $A$. For every $i$ s.t. $1 \leq i \leq N$, $\hat{\theta}_i = \hat{A}_i\hat{\rho}$ is also uniformly distributed over $\mathbb{F}_q^N$. Therefore, the vector $\hat{\theta}$ is uniformly distributed over $\mathbb{F}_q^N$ and for each $i$,

$$\Pr_{A,\hat{\rho}}[\hat{\theta}_i = \hat{\theta}_i] \leq \frac{1}{q},$$

by Schwartz-Zipple Lemma. By applying the Union bound, we conclude that

$$\Pr_{A,\hat{\rho}}[A\hat{\rho} = \theta] = \Pr_{A,\hat{\rho}}[\hat{\theta} = \theta] \leq \frac{N}{q}.$$

**APPENDIX B**

**PROOFS FOR RELIABILITY WITHOUT FEEDBACK**

In the presence of a causal adversary, a two-part rate-region is presented in Section IV. In this Appendix we provide supporting proofs for Theorems 1 and 2, which provide the claimed characterizations of the two-part rate-regions for additive jamming and overwrite jamming.
A. Proof of Theorem 1

1) Achievability for positive-rate regime: Since the adversary can only jam in a causal manner, a pairwise-hashing scheme is helpful to achieve the best rate for the positive-rate regime.

Encoder: The encoder operates over a finite field $\mathbb{F}_q$, where $q = 2^k$ and we set $b = \log(nC)$ for equal link capacities while $b = \log(nC)$ for unequal link capacities. Choose $N$ such that $N^2 + N(C + 1) = \frac{n}{\beta}$. The codeword consists of $C$ vectors $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_C$, each of length $N^2 + N(C + 1)$ over the finite field $\mathbb{F}_q$. Each $\vec{x}_i$ is of the form

$$\vec{x}_i = [\vec{U}_i, \vec{K}_i, \vec{h}_i1, \vec{h}_i2, \ldots, \vec{h}_iC].$$

Here, $\vec{U}_i$ is such that $\vec{U}_1, \vec{U}_2, \ldots, \vec{U}_C$ together form the codeword corresponding to the length-$n$ payload bit message $m$ using a Reed-Solomon code of length $C$ and rate $C - z_{rw} - z_{wo}$ over the finite field $\mathbb{F}_q$. $\vec{K}_i$ is the hash key generated for each row. The value of hash function $h(\vec{U}_j, \vec{K}_i)$ is defined as $\vec{h}_{ij}$. For each link $L_i$, the encoder also appends $C$ pairwise hashes $\vec{h}_i1, \vec{h}_i2, \ldots, \vec{h}_iC$ corresponding to the $C$ links (see Figure 1 in Section II).

Hash Function: The idea of Matrix-hashing (see Lemma 1 in Appendix A) is used for the hash function. Notice that the randomly generated hash keys are of size $N$ and each length-$N^2$ payload $\vec{U}_i$ can be rearranged as a $N \times N$ matrix $\vec{D}_i$. We pad auxiliary bits before the packets if a square matrix cannot be formed. The hashes $\vec{h}_{ij}$ is obtained from the hash function $h(\vec{U}_j, \vec{K}_i) = \vec{D}_j\vec{h}_i$.

Decoder: After transmission, the received packet of the $i$-th link $L_i$ is of the form

$$\vec{Y}_i = [\vec{U}_i, \vec{K}_i, \vec{h}_i1^T, \vec{h}_i2^T, \ldots, \vec{h}_iC^T].$$

For each $i, j$, link $L_i$ and $L_j$ are consistent if and only if $\vec{h}_{ij} = h(\vec{U}_j, \vec{K}_i)$ and $\vec{h}_{ji} = h(\vec{U}_i, \vec{K}_j)$. In particular, link $L_i$ is called self-consistent if and only if $\vec{h}_{ii} = h(\vec{U}_i, \vec{K}_i)$.

The decoder Bob first removes the links that belong to $Z_{WO}$ by checking self-consistency. Then Bob constructs an undirected graph with $C$ vertices and for $i,j$, he connects the two vertices $v_i$ and $v_j$ if $L_i$ and $L_j$ are consistent. To detect the uncorrupted links, Bob adopts a "finding largest clique" strategy, i.e., a link is assumed to be uncorrupted if its corresponding vertex belongs to the largest clique. Finally, Bob decodes the message from the $C - z_w$ uncorrupted links by Reed-Solomon code.

Analysis: Before transmission, any two links are consistent and the clique formed by Alice is of size $C$. After adversarial corruption, the size of clique formed by Alice (correct clique) is of size at least $C - z_w$. On the other hand, Calvin may mimic the behavior of Alice and and attempt to form a fake clique that is as large as possible. For any two links belonging to $Z_{RW}$, Calvin is able to make them consistent since he can modify the payload first, and then compute matching hashes to insert. However, if link $L_i$ belongs to $Z_{RW}$ and link $L_j$ belongs to $Z_{RO}$, Calvin cannot induce consistency since $\vec{h}_{ij} \neq h(\vec{U}_i, \vec{K}_j^T)$ with high probability. This is because with causality, Calvin doesn’t have the ability to observe $\vec{K}_j$ and $\vec{h}_j$ when modifying $\vec{U}_i$. In this scenario, the probability that Calvin can induce $\vec{h}_{ij} = h(\vec{U}_i, \vec{K}_j^T)$ is at most $\frac{1}{n}$ over finite field $\mathbb{F}_q$ (see Lemma 1 in Appendix A). We would like to make $q$ larger, i.e., enlarge the size of the field, to reduce the error probability.

In conclusion, Calvin is able to form a fake clique of size at most $z_{rw}$. If Bob wishes to figure out the uncorrupted links by finding largest clique, the size of correct clique should be larger than the fake clique, i.e. $C - z_w > z_{rw}$. Therefore we derive the condition for our positive-rate regime, which is $z_{wo} + 2z_{rw} < C$, and the rate $R = C - z_{rw} - z_{wo}$ can be achieved.

2) Converse for positive-rate regime: Irrespective of the encoding/decoding scheme, Calvin can always add uniformly random noise to any $z_w$ links. No information can be recovered from the $z_{wo}$ links and thus no rate higher than $C - z_w$ is possible.

3) Converse for zero-rate regime: In the zero-rate regime ($z_{wo} + 2z_{rw} \geq C$), we prove that no reliable communication is possible no matter which encoding scheme Alice will use. To confuse Bob, the causal adversary Calvin will always adopt the following “symmetrization” strategy: (a) corrupt the last $z_{wo}$ (resp. $z_{wo} + 1$) links by adding random noise if $C - z_w$ is even (resp. odd), and (b) “attack” either the top half or the bottom half of the remaining $C' = C - z_w$ (resp. $C' = C - z_w - 1$) links, where the “attack” is defined below. This is a viable jamming strategy for Calvin since $z_{rw} \geq (C - z_w)/2$ in the zero-rate regime. The specific attack Calvin chooses is to pick a message $m'$ first and substitute the original codewords belong to $Z_{RW}$ by the codewords corresponding to $m'$. In this way, Bob has no idea whether $m$ or $m'$ was transmitted.

We assume the message $M$ is uniformly distributed from the message set $\mathcal{M}$, denoted by $U_M$. Let $X_R$ be the random variable of the codeword. Moreover, $X_R(M)$ is used to represent the random variable of the codeword conditioned on message $m$. The event $\Gamma(m, k, m', k')$ stands for the scenario when Alice chooses a message $m$ and a random key $k$ while Calvin chooses a message $m'$ and a random key $k'$. We can show that the probability of the event $\Gamma(m, k, m', k')$ and the event $\Gamma(m', k', m, k)$ are exactly the same.

$$\Pr[\Gamma(m, k, m', k')] = U_M(m)P_{X_R(m)}(X)U_M(m')P_{X_R(m')}(X') = U_M(m')P_{X_R(m')}(X')U_M(m)P_{X_R(m)}(X) = \Pr[\Gamma(m', k', m, k)]$$

Let $P_q(m, k, m', k')$ and $P_q(m', k', m, k)$ denote the distributions of the received codeword conditioned on the events $\Gamma(m, k, m', k')$ and $\Gamma(m', k', m, k)$ respectively. Given the

\footnote{Notice that the links belong to $Z_w$ are also detectable by simply checking the self-consistency. We claim a link belongs to $Z_{WO}$ if it is not self-consistent. However, this process is not necessary since we can detect the uncorrupted links by finding the largest clique.}
event $\Gamma(m, k, m', k')$, the received codeword would be either
$$[\overrightarrow{X}_1, ..., \overrightarrow{X}_{C'}, \overrightarrow{X}_{C'+1}, ..., \overrightarrow{X}_{C'}, \overrightarrow{C'}+1, ..., \overrightarrow{C}]$$
or
$$[\overrightarrow{X}'_1, ..., \overrightarrow{X}'_{C'}, \overrightarrow{X}'_{C'+1}, ..., \overrightarrow{X}'_{C'}, \overrightarrow{N}_{C'+1}, ..., \overrightarrow{N}]$$
with equal probability. The same distribution of the codeword will be received when the event $\Gamma(m', k', m, k)$ happens. We conclude that the distributions $P_B(m, k, m', k')$ and $P_B(m', k', m, k)$ are exactly the same. Therefore Bob cannot distinguish the events $\Gamma(m, k, m', k')$ and $\Gamma(m', k', m, k)$ when decoding, and thus has no idea whether $m$ or $m'$ are transmitted. The error probability is
$$\Pr(error) = \frac{1}{2}(1 - \frac{1}{2^{nR_{max}}})$$
if Bob uses an optimal maximum-likelihood decoder (the term $1 - 2^{nR_{max}}$ is due to the “small” probability that the message $m'$ Calvin chooses to use to confuse Bob happens to actually match Alice’s message $m$).

**B. Proof of Theorem 2**

1) **Achievability for the positive-rate regime:** The pairwise-hashing scheme also works for the overwrite jammer. The encoding scheme here is the same as that in the additive case. We briefly describe it below for completeness. As earlier, we first generate a payload $\overrightarrow{U}_i$ for each link $L_i$ using a Reed-Solomon code. Next, we append the hash key and pairwise hashes to the the payload to obtain the codeword $\overrightarrow{X}_i = [\overrightarrow{U}_i \overrightarrow{K}_i h_{i1}, h_{i2}, ..., h_{iC}]$. After transmission, the received packet is denoted by $\overrightarrow{Y}_i = [\overrightarrow{U}'_i \overrightarrow{K}'_i h_{i1}', h_{i2}', ..., h_{iC}']$. As in the additive case, the decoder forms an undirected decoding graph with $C$ nodes and connects two vertices $v_i$ and $v_j$ if $L_i$ and $L_j$ are consistent. Finally, the decoder finds the largest clique in the decoding graph to determine the set of uncorrupted links. Although the same encoding strategy is applied, a different rate-regime is obtained since the overwrite jammer is slightly stronger than the additive one.

**Analysis:** After transmission, the size of the correct clique is at least $C - z_w$ since Calvin doesn’t have privilege to jam on these links. At the same time, Calvin is able to induce a fake clique of size no larger than $z_{rw} + z_{wo}$. This is because on the links that belong to $Z_{RW}$ and $Z_{WO}$, Calvin can overwrite the payloads first and then overwrite the hash vectors with appropriately computed replacements. Therefore the corresponding vertices will form a clique of size $z_{rw} + z_{wo}$. Notice that from the receiver’s perspective, the subset $Z_{RW}$ is equivalent to $Z_{WO}$ with overwrite jamming. With additive jamming, we have proved that the fake clique that Calvin may induce is of size $z_{rw}$. Therefore as long as $z_{rw} + z_{wo} < C - z_w$, the rate $R = C - z_w$ is achievable.

2) **Converse for positive-rate regime:** Irrespective of the encoding/decoding scheme, Calvin can always arbitrarily choose a subset $Z_{RW}$ and overwrite these links by adding noises. As a result, at most $C - z_w$ links can carry useful information and thus the maximum rate is at most $C - z_w$.

3) **Converse for zero-rate regime:** The condition for zero-rate regime is $z_{rw} + z_{wo} \geq C/2$ with overwrite jamming. In this regime, the adversary is able to jam at least half of the $C$ links and may perform a similar “symmetrization” strategy. Irrespective of the coding scheme, Calvin will (a) first pick a message $m'$ and a key $k'$ randomly to obtain the corresponding codeword $X'$, (b) then attack either the top half or the bottom half (If $C$ is odd, Calvin will first “erase” one link by overwrite it with a zero packet). In this case, the messages $m$ and $m'$ are perfectly symmetric so that Bob is unable to distinguish them.

If the event $\Gamma(m, k, m', k')$ happens, the received codeword would be either
$$[\overrightarrow{X}_1, ..., \overrightarrow{X}_{C'}, \overrightarrow{X}_{C'+1}, ..., \overrightarrow{X}_{C'}, \overrightarrow{N}_{C'+1}, ..., \overrightarrow{N}]$$
or
$$[\overrightarrow{X}'_1, ..., \overrightarrow{X}'_{C'}, \overrightarrow{X}'_{C'+1}, ..., \overrightarrow{X}'_{C'}, \overrightarrow{N}_{C'+1}, ..., \overrightarrow{N}]$$
with equal probability. Meanwhile, the received codeword has the same distribution when the event $\Gamma(m', k', m, k)$ happens. Therefore the distributions $P_B(m, k, m', k')$ and $P_B(m', k', m, k)$ are also the same and Bob is unable to decide which message is transmitted. The error probability is equal to $\Pr(error) = \frac{1}{2}(1 - \frac{1}{2^{nR_{max}}})$ if a random decision is made.

**APPENDIX C**

**PROOFS FOR RELIABILITY AND SECRECY WITHOUT FEEDBACK**

A. **Proof of Theorem 3**

1) **Positive-rate Regime:**

**Converse:** Consider the following strategy for Calvin. First, on the links in $Z_{W}$ he adds uniformly random noise that is independent of the codewords on other links. Next, he eavesdrops on all $Z_{R}$ links. We show that, using standard information-theoretic inequalities, that it is not possible for Alice to reliably and secretly transmit at any rate more than $C - z_w - z_r$. Notice that Calvin can jam any $z_w$ links and can eavesdrop any $z_r$ links. Consider a code of length $n$ that achieves an error probability $\epsilon_n$ and achieves perfect secrecy. The following set of inequalities follow.

$$H(M) = H(M|Y) + I(M; Y)$$

$$\leq n\epsilon_n + I(M; Y)$$

(a) $$\leq n\epsilon_n + I(M; Y_1^{z_w}) + I(M; Y_{z_w+1}^{z_{rw}})$$

(b) $$\leq n\epsilon_n + I(M; X_{z_w}^{C-z_w})$$

(c) $$\leq n\epsilon_n + I(M; X_{z_w}^{C-z_w})$$

(d) $$\leq n\epsilon_n + I(M; X_{z_w}^{C-z_w}) + I(M; X_{z_w+1}^{z_{rw}+1})$$

(e) $$\leq n\epsilon_n + H(X_{z_w+1}^{C-z_w})$$

(f) $$\leq n\epsilon_n + C - z_w - z_r,$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$. Here, (a) follows from Fano’s inequality. Inequalities (b) and (d) follow from the chain rule for mutual information. To obtain (c), we assume without loss of generality that Calvin jams first $z_w$. 


links. Then, we get $I(M; Y_{1:n}^w) = 0$, as Calvin adds uniform random noise independent of Alice’s transmissions. Also, $I(M; Y_{z_w+1}^C Y_{z_r}^w) = I(M; Y_{z_r}^C)$ due to independence of added noise. Finally, we use the fact that for the set of uncorrupted links, we have $Y_{\setminus Z_w} = X_{\setminus Z_w}$, which gives $I(M; Y_{z_w+1}^C) = I(M; X_{z_w+1}^C)$. For getting (e), we use the fact that for any subset $Z_R$ of links of size $z_r$, the secrecy requirement imposes that $I(M; X_{Z_R}) = 0$. Thus, $I(M; X_{z_w+1}^C)$ is zero. In addition, we have $I(M; X_{z_w+1}^C|X_{z_w+1}^C) \leq \mathcal{H}(X_{z_w+1}^C|X_{z_w+1}^C)$. Finally, (f) follows from the fact $H(X_{z_w+1}^C|X_{z_r+1}^C) \leq 0$ where the second inequality is due to unit link capacities.

**Achievability:** Alice first appends $n(C - z_w - z_r)$ message symbols with $nz_r$ uniform random key symbols to form $n(C - z_w)$ super-message symbols. Then, she uses the achievable scheme mentioned in the proof of Theorem 1 (case 1) composed of a $(C, C - z_w)$ Reed-Solomon code together with the pairwise hashing scheme. We require that the generator matrix of the Reed-Solomon code consists of a Cauchy matrix.

Now, Bob can locate the set $Z_W$ of corrupted links using pairwise hashing and uses the Reed-Solomon code to decode the super-message symbols from the remaining links. Then, Bob separates the random keys and the message symbols from the super-message symbols, since the first $n(C - z_w - z_r)$ symbols of the super-message are the message symbols.

For secrecy, we show that Calvin cannot infer any information from the links he eavesdrops. We denote the set of random keys by $k$ and the corresponding random variable by $K$. Further, let $X_{Z_R}$ denote the links being eavesdropped. Consider the following set of inequalities:

$$I(M; X_{Z_R}) = H(X_{Z_R}) - H(X_{Z_R}|M) \leq n z_r - H(X_{Z_R}|M)$$

$$\leq n z_r - H(X_{Z_R}|M) + H(X_{Z_R}|M, K)$$

$$= n z_r - I(X_{Z_R}; K|M)$$

$$= n z_r - K|M + H(K|M, X_{Z_R})$$

$$\leq n z_r - H(K|M, X_{Z_R})$$

$$\leq H(K|M, X_{Z_R})$$

(2)

where (g) follows from the fact that each link has unit capacity and Calvin can eavesdrop at most $z_r$ links, (h) follows from the non-negativity of entropy, (i) and (j) follow from the definition of mutual information, (k) follows because keys are independent of the message, and (l) follows from the fact that the keys are uniform random, giving $H(K) = n z_r$. Now, in order to prove secrecy, we need to show that $H(K|M, X_{Z_R}) = 0$. In other words, one can decode the keys from $X_{Z_R}$ and $M$. Let $G(x_{Z_R})$ denote the rows of the Cauchy generator matrix corresponding to the symbols $X_{Z_R}$. Therefore, we have

$$X_{Z_R} = G(x_{Z_R}) \begin{bmatrix} M \\ K \end{bmatrix}.$$  

To prove that $H(K|M, X_{Z_R}) = 0$, one needs to show that the following system of linear equations can be solved.

$$X_{Z_R} = \begin{bmatrix} G(x_{Z_R}) \\ I \end{bmatrix} \begin{bmatrix} M \\ K \end{bmatrix},$$

(3)

where $I$ denotes identity matrix of size $n(C - z_w - z_r) \times n(C - z_w - z_r)$, and $O$ denotes zero matrix of size $n(C - z_w - z_r) \times n z_r$. First notice that $G(x_{Z_R})$ is a Cauchy matrix since it is a sub-matrix of a Cauchy matrix. Then, using the property that any square sub-matrix of a Cauchy matrix is non-singular, it is straightforward to show that the matrix $\begin{bmatrix} G(x_{Z_R}) \\ I \end{bmatrix}$ is invertible. Therefore, the linear system (3) can be inverted, and we have $H(K|M, X_{Z_R}) = 0$.

2) **Zero-rate Regime:** Notice that even in the absence of secrecy, no positive rate is achievable in this regime. Adding the extra requirement of secrecy can only decrease the communication rate. Thus no communication at positive rate is possible in this regime.

**B. Proof of Theorem 5**

For the positive-rate case, the converse and achievability proofs follow from the same arguments as in the proof of Theorem 5 and is omitted for brevity.

For the zero-rate regime, the rate without the secrecy requirement is zero. This implies that no positive rate is possible when secrecy condition is added on top of reliability.

**APPENDIX D**

**CAUSAL JAMMING WITH PASSIVE FEEDBACK**

**A. Proof of Theorem 7**

Noting that the rate cannot exceed $C - z_w$ even with feedback (since Calvin can always inject random noise on $z_w$ links). Therefore, to prove the claim of Theorem 7 it suffices to show the following:

(a) $C - z_w$ is achievable whenever $z_r < C$ or $C > 2 z_w$.

(b) No positive rate is possible when $z_r = C$ and $C \leq 2 z_w$.

1) **Proof of (a):** We prove the achievability of the rate $C - z_w$ by partitioning the parameter set $Z_{\text{add}} = \{ z_r < C \} \cup \{ C > 2 z_w \}$ into disjoint sets $Z_1 = \{ z_r < C \}$ and $Z_2 = \{ z_r = C \} \cap \{ C > 2 z_w \}$, and using different coding schemes in the two sets.

**Achievability for $Z_1$:** The code operates over two rounds. In the first round, Alice uses an erasure code of length $C$ capable of correcting up to $z_r$ erasures. Upon observing the codewords received by Bob (through passive feedback), Alice computes random hashes of each of the $C$ received codewords and sends these hashes on the links which are not corrupted in the first round.

Formally, we show that the rate $C - z_w$ is achievable (and hence, any smaller rate is also achievable). Alice first chooses a blocklength $n > \lfloor \log_2 C \rfloor$ and encodes an $n$-bit message over $n + C \sqrt{n}$ time slots using a two-round scheme as follows. **Round 1:** In the first round, Alice uses $n$ time slots to transmit using the following scheme. Alice treats $m$ as $R$ consecutive symbols $m_1, m_2, \ldots, m_R$ from a finite field $\mathbb{F}_{2^n}$ of size $2^n$. Next, Alice encodes $(m_1, m_2, \ldots, m_R)$ to
\[ X^{(1)} = (x_1^{(1)}, x_2^{(1)}, \ldots, x_C^{(1)}) \] using a Reed-Solomon code capable of correcting up to \( z_w \) erasures and sends \( x_i^{(1)} \) on the link \( L_i \) for each \( i = 1, 2, \ldots, C \). These codewords are corrupted by Calvin and Bob receives \( Y^{(1)} = (y_1^{(1)}, y_2^{(1)}, \ldots, y_C^{(1)}) \). Alice also observes \( Y^{(1)} \) causally using the passive feedback available to her. Based on her observation, Alice partitions \( L_1, L_2, \ldots, L_C \) into two sets – \( Z_{\hat{y}} \) consisting of all links \( L_i \) where \( x_i^{(1)} = y_i^{(1)} \) and \( Z_x \) consisting of all links \( L_i \) where \( x_i \neq y_i \). Note that \( Z_x \subset Z_W \subset \{ L_1, L_2, \ldots, L_C \} \).

**Round 2:** In the second round, Alice uses the feedback seen from first round and transmits random hashes over \( 2C\sqrt{n} \) time slots using the following scheme. Alice picks \( C \) independent random keys \( \rho_1, \rho_2, \ldots, \rho_C \) and computes hashes \( h(y_1^{(1)}, \rho_1), h(y_2^{(1)}, \rho_2), \ldots, h(y_C^{(1)}, \rho_C) \), each of length \( \lceil \sqrt{n} \rceil \) using the matrix hash scheme (See Appendix A). Next, Alice transmits the codeword \( x_1^{(2)} = [h(y_1^{(1)}, \rho_1) h(y_2^{(1)}, \rho_2) \ldots h(y_C^{(1)}, \rho_C) \rho_1 \rho_2 \ldots \rho_C] \) on every link \( L_i \in Z_{\hat{y}} \) and a random length-2C\sqrt{n} vector \( x_2^{(2)} \) on every link \( L_i \in Z_x \).

**Decoding:** Bob first partitions the set of links into sets \( Z_{\hat{y}} \) and \( Z_x \) using the following classification.

- If Bob determines that the hash values and keys specified by \( y_i^{(2)} \) are consistent with all the received codewords in the first round, i.e., \( Y^{(1)} \), he assigns \( L_i \) to \( Z_{\hat{y}} \).
- Else, Bob assigns \( L_i \) to \( Z_x \).

Finally, if the size of \( Z_{\hat{y}} \) is at least as large as \( C - z_w \), Bob uses the codewords \( (x_i^{(1)} : L_i \in Z_{\hat{y}}) \) to decode the message. Else, he declares an error.

**Analysis:** Note that \( Z_{\hat{y}} \) includes every link that is not corrupted by Calvin (and possibly some other links as well). Thus, \( |Z_{\hat{y}}| \geq C - z_w \). Since the Reed-Solomon erasure correcting code can recover \( X^{(1)} \) from any \( C - z_w \) correct symbols out of \( x_1^{(1)}, x_2^{(1)}, \ldots, x_C^{(1)} \), in order to prove that Bob can successfully decode \( m \) with a high probability, it is sufficient to show that \( Z_x \subseteq Z_{\hat{y}} \) with a high probability. Without loss of generality, we show the above when \( z_w < C \) (since zero rate is trivially achieved when \( z_w = C \)).

Let \( L_s \in Z_{\hat{y}} \). Since \( z_s < C \), there is at least one link \( L_t \) such that \( y_t^{(1)} \) is observed by Bob (and hence by Alice), but not by Calvin. This implies that in the second round, even if Calvin knows \( \rho_t \), he can only randomly guess a consistent replacement for \( h(y_t^{(1)}, \rho_t) \). Thus,

\[
\Pr \left( Z_x \notin Z_{\hat{y}} \right) \\
\quad \leq \Pr \left( s \in Z_{\hat{y}} \mid s \in Z_x \right) \\
\quad = \Pr \left( y_s^{(2)} = [h(y_1^{(1)}, \rho_1) \ldots h(y_C^{(1)}, \rho_C) \rho_1 \ldots \rho_C] \right. \\
\quad \quad \quad \text{for some } \rho_1, \ldots, \rho_C \rangle \\
\quad \leq \Pr \left( y_s^{(2)} = [h(y_1^{(1)}, \rho_1) \rho_1] \right. \\
\quad \quad \quad \text{for some } \rho_1, \ldots, \rho_C \rangle \\
\quad \leq 2^{-\sqrt{n}}.
\]