Jamming exercise

Nov 13, 2015

Problem setting: A sender wants to send messages to a receiver. The communication channel between sender and receiver consists of C subchannels. The transmission of a message takes T ms. For the transmission of a message, the sender chooses one subchannel and transmits the message through this subchannel. After T ms, it may change the subchannel for the transmission of the next message.

A jammer tries to prevent the message transmission between sender and receiver. It can simultaneously jam C_{jam} subchannels. If it jams a subchannel on which the sender attempts to transmit a message, the transmission attempt fails. Otherwise, the message arrives at the receiver, and the transmission attempt is successful.

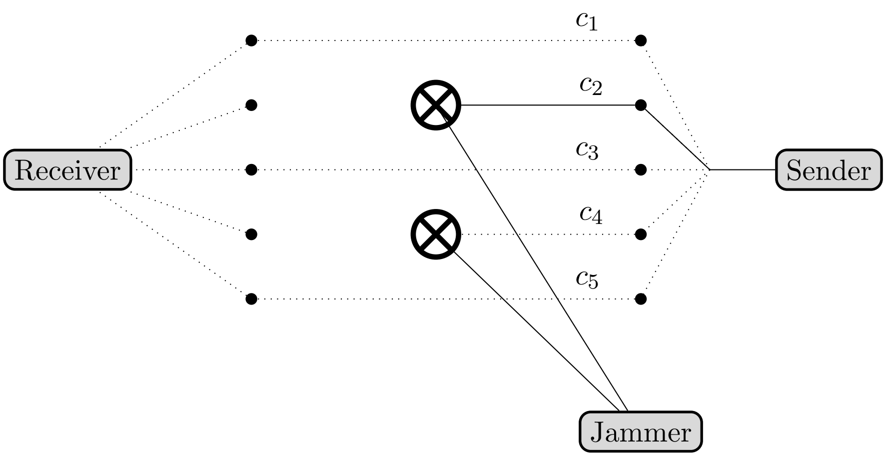

Figure 1: Assume $C = 5$ and $C_{\text{jam}} = 2$. If the sender chooses subchannel c_2 and the jammer chooses to jam on the subchannel subset $\{2, 4\}$, then the transmission attempt fails.

The jammer's strategy consists in choosing, for each time slot of T ms, a subset of C_{jam} subchannels uniformly at random. In the next time slot, it chooses a new subset of the subchannels again uniformly at random, and independently of the previous choice. And so on.

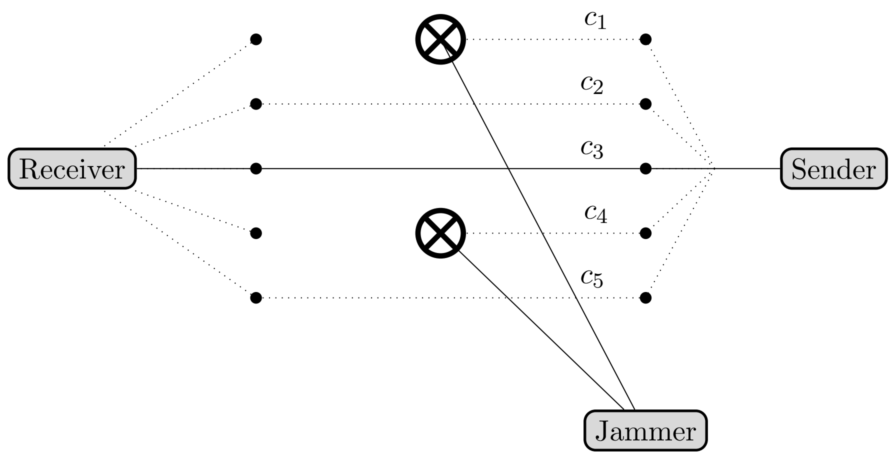

Figure 2: Again assume $C = 5$ and $C_{\text{jam}} = 2$. If the sender chooses subchannel 3 for transmission and the jammer chooses subchannels 1 and 4 to disable communication, then the transmission attempt succeeds.

The sender does not know which subchannel subset the jammer chooses. To counter the jammer's actions, the sender chooses the subchannel for message transmission uniformly at random as well. The jammer does not know which subchannel the sender chooses. Intuitively, if $C_{\text{jam}} < C$, then there will be successful transmission attempts: The jammer will not always choose a subset of the set of subchannels that contains the subchannel chosen by the sender.

Interpretation: The subchannels can be thought of as different frequency bands. There is a broadband channel between sender and receiver which can be partitioned into smaller frequency subbands. Each of the subbands corresponds to one of the above subchannels. The sender strategy of choosing a new frequency subband for each time slot of length T ms is called *frequency hopping*.

Question 1: What is the probability that a single transmission attempt succeeds?

Solution: We need a mathematical model of the sender and the jammer strategies. The set of subchannel indices is $\{1, 2, \ldots, C\}$. We denote the random choice of subchannel made by the sender by X. More generally, X is called a *random variable*. For every $c \in \{1, \ldots, C\}$, the probability that $X = c$ equals

$$\Pr[X = c] = \frac{1}{C}.$$

Note that $\sum_{c=1}^{C} \Pr[X = c] = 1$. This means that with certainty, the sender will choose one of the possible subchannels.

The jammer chooses C_{jam} subchannels at random. Phrased differently, the jammer chooses a C_{jam}-element subset $\Gamma \subset \{1, \ldots, C\}$ of the set of all possible subchannels. For the fact that Γ is a set containing exactly C_{jam} subchannels we write $|\Gamma| = C_{\mathrm{jam}}$. We write $S_{C_{\mathrm{jam}}}$ for the set of subsets Γ of $\{1, \ldots, C\}$ with $|\Gamma| = C_{\mathrm{jam}}$. There are

$$\binom{C}{C_{\mathrm{jam}}} = \frac{C!}{C_{\mathrm{jam}}!(C - C_{\mathrm{jam}})!}$$

subsets of $\{1, \ldots, C\}$ which have C_{jam} elements.

(For a natural number n, we define $n! = n \cdot (n-1) \cdots 2 \cdot 1$, and one says "$n$ factorial". For another natural number k, $\binom{n}{k}$ is a binomal coefficient, and one reads "n choose k".)

We denote the jammer's randomly chosen subset by Y. The probability that $Y = \Gamma$ for a given subset $\Gamma \in S_{C_{\mathrm{jam}}}$ equals

$$\Pr[Y = \Gamma] = \frac{1}{\binom{C}{C_{\mathrm{jam}}}}.$$

Again note that $\sum_{\Gamma \in S_{C_{\mathrm{jam}}}} \Pr[Y = \Gamma] = 1$.

To complete our model, we have to describe the fact that the sender and the jammer make their choices independently of each other (as they do not know each other's choice). We describe this mathematically by the equation

$$\Pr[X = c \text{ and } Y = \Gamma] = \Pr[X = c] \Pr[Y = \Gamma] \tag{1}$$

for every $c \in \{1, \ldots, C\}$ and $\Gamma \in S_{C_{\mathrm{jam}}}$. We say that X and Y are *independent*.

Now what does it mean for the transmission attempt to be successful? Assume that the sender's choice is $c \in \{1, \ldots, C\}$ and the jammer's choice is $\Gamma \in S_{C_{\mathrm{jam}}}$. Then the transmission attempt is successful if and only if $c \notin \Gamma$, i. e. if the sender has chosen a subchannel which is not jammed. We denote the set of all possible pairs (c, Γ) which allow successful transmission by A. That means

$$A := \{(c, \Gamma) : c \in \{1, \ldots, C\}, \Gamma \in S_{C_{\mathrm{jam}}}, c \notin \Gamma\}.$$

The choices of c and Γ are random, so we have to calculate the probability that the pair (X, Y) is contained in A, which is the set of all random choices the sender and jammer can make such that the transmission attempt succeeds. A shorthand for writing $(X, Y) \in A$ is to write $X \notin Y$. The set A consists of mutually exclusive "events" (c, Γ), so its probability is given by the sum of the probabilties of these events. More precisely,

$$\Pr[X \notin Y] = \Pr[(X, Y) \in A] = \sum_{(c,\Gamma) \in A} \Pr[X = c \text{ and } Y = \Gamma].$$

As we know that either $X \in Y$ or $X \notin Y$ (and one of the two is always correct), it is sufficient to calculate $\Pr[X \in Y]$ because then

$$\Pr[X \notin Y] = 1 - \Pr[X \in Y]. \tag{2}$$

We set B to be the set of (c, Γ) where the transmission attempt fails, i. e.

$$B := \{(c, \Gamma) : c \in \{1, \ldots, C\}, \Gamma \in S_{C_{\mathrm{jam}}}, c \in \Gamma\}.$$

Then we have

$$\begin{aligned}
\Pr[X \in Y] &= \Pr[(X,Y) \in B] \\
&= \sum_{(c,\Gamma)\in B} \Pr[X = c \text{ and } Y = \Gamma] \\
&\overset{(a)}{=} \sum_{\Gamma \in S_{C_{\text{jam}}}} \sum_{\substack{c\in\{1,\ldots,C\}:\\ c\in\Gamma}} \Pr[X = c] \Pr[Y = \Gamma] \\
&\overset{(b)}{=} \frac{1}{C} \frac{1}{\binom{C}{C_{jam}}} \sum_{\Gamma \in S_{C_{\text{jam}}}} \sum_{\substack{c\in\{1,\ldots,C\}:\\ c\in\Gamma}} 1 \\
&\overset{(c)}{=} \frac{1}{C} \frac{1}{\binom{C}{C_{jam}}} \sum_{\Gamma \in S_{C_{\text{jam}}}} C_{\text{jam}} \\
&= \frac{C_{\text{jam}}}{C} \frac{1}{\binom{C}{C_{\text{jam}}}} \sum_{\Gamma \in S_{C_{\text{jam}}}} 1 \\
&\overset{(d)}{=} \frac{C_{\text{jam}}}{C}.
\end{aligned}$$

The equality (a) follows from the fact that X and Y are independent (see (1)) and (b) follows from the definitions of the probabilites $\Pr[X = c]$ and $\Pr[Y = \Gamma]$. In (c) we use that $|\Gamma| = C_{\text{jam}}$ for every $\Gamma \in S_{C_{\text{jam}}}$ and in (d) that $S_{C_{\text{jam}}}$ contains exactly $\binom{C}{C_{\text{jam}}}$ different sets. Now, applying (2), we obtain the probability that a single transmission attempt is successful:

$$\Pr[X \notin Y] = 1 - \frac{C_{\text{jam}}}{C}. \tag{3}$$

Note that this probability depends on C_{jam} and can be very small. If $C_{\text{jam}} = C$, then this probability actually is equal to zero, as one would expect intuitively.

Question 2: What is the probability that n subsequent transmission attempts succeed?

Solution: To answer this question, we have to extend our model to cover the choices made by sender and receiver over time. These choices are also supposed to be independent. Let X_i and Y_i be the random choices of the sender and the jammer, respectively, made in the i-th time slot. For every sequence $(c_1, \ldots, c_n)$ of possible sender choices and every sequence of jammer choices $(\Gamma_1, \ldots, \Gamma_n)$, we then require that

$$\Pr[X_1 = c_1, \ldots, X_n = c_n, Y_1 = \Gamma_1, \ldots, Y_n = \Gamma_n] = \prod_{i=1}^{n} \Pr[X_i = c_i] \prod_{j=1}^{n} \Pr[Y_j = \Gamma_j].$$

If we define $\Pr[X_i = c]$ to be equal to $\Pr[X = c]$ for every c and $\Pr[Y_i = \Gamma] = \Pr[Y = \Gamma]$ for every Γ, then the sender and jammer strategies do not change over time and are independent with respect to each other and over time.

The probability we are interested in is

$$\begin{aligned}
&\Pr[X_1 \notin Y_1, \ldots, X_n \notin Y_n] \\
&= \sum_{\substack{(c_1,\ldots,c_n),(\Gamma_1,\ldots,\Gamma_n): \\ (c_i,\Gamma_i)\in A \text{ for every } 1\le i\le n}} \Pr[X_1 = c_1, Y_1 = \Gamma_1, \ldots, X_n = c_n, Y_n = \Gamma_n] \\
&\overset{(e)}{=} \prod_{i=1}^{n} \left(\sum_{(c_i,\Gamma_i)\in A} \Pr[X_i = c_i, Y_i = \Gamma_i] \right) \\
&\overset{(f)}{=} \prod_{i=1}^{n} \Pr[X \notin Y] \\
&\overset{(g)}{=} \left(1 - \frac{C_{\text{jam}}}{C}\right)^n .
\end{aligned}$$

Here, (e) follows from the independence of the sender and jammer choices over time, (f) is due to the definition of A, and in (g) we use the solution to question 1, see (3), together with the fact that all pairs (X_i, Y_i) have the same probability distribution as the pair (X, Y).

Question 3: What is the probability that, within n transmission attempts, exactly the attempts in time slots $i_1, \ldots, i_k$ succeed? Here $1 \le i_1 < \ldots < i_k \le n$, in particular, it is exactly k attempts that succeed.

Solution: The probability we are looking for is

$$\begin{aligned}
\Pr[X_1 \in Y_1, \ldots, X_{i_1-1} \in Y_{i_1-1}, X_{i_1} \notin Y_{i_1}, X_{i_1+1} \in Y_{i_1+1}, \ldots,& \\
X_{i_k-1} \in Y_{i_k-1}, X_{i_k} \notin Y_{i_k}, X_{i_k+1} \in Y_{i_k+1}, \ldots, X_n \in Y_n].& \quad (4)
\end{aligned}$$

This looks complicated, but only because one has to specify the positions of the $i_1, \ldots, i_k$. It looks simpler, for example, if the successful attempts are the first k attempts.

Using the same approach as in the solution to the previous question, in particular the independence of the sender and jammer actions over time, we obtain that the probability in (4) equals

$$\left(1 - \frac{C_{\text{jam}}}{C}\right)^k \left(\frac{C_{\text{jam}}}{C}\right)^{n-k} .$$

Observe that this expression is independent of the exact positions of the k successful transmissions.

Question 4: What is the probability that exactly k out of $n \ge k$ transmission attempts succeed?

Solution: We have to sum the probability from the previous question over all possible sequences of indices $i_1, \ldots, i_k$ with $1 \le i_1 < i_2 \ldots < i_k \le n$. The probability of successes exactly at $i_1, \ldots, i_k$ does not depend on the exact sequence, so we only have to count how many such sequences $i_1, \ldots, i_k$ there are. Observe that each $i_1, \ldots, i_k$ corresponds to exactly one subset of $\{1, \ldots, n\}$ with exactly k elements. There are $\binom{n}{k}$ such subsets, so the probability we are looking for equals

$$\binom{n}{k}\left(1-\frac{C_{\text{jam}}}{C}\right)^k\left(\frac{C_{\text{jam}}}{C}\right)^{n-k}.$$

Remark: If $0 < p < 1$, then

$$\binom{n}{k}(1-p)^k p^{n-k} \tag{5}$$

is the probability that exactly k out of n independent "attempts" are successful if one single attempt has success probability $1-p$. These attempts can describe any random experiment independently repeated n times. The probability distribution on the set $\{0, \ldots, n\}$ where k has the probability (5) is known as the *Binomal distribution* with parameters n and $1-p$.

Question 5: If, as in the above figures, $C = 5$ and $C_{\text{jam}} = 2$, and if 10 messages should be transmitted. How many attempts should be made such that the probability that all messages have gone through is at least 0.9?

Solution: We use the solution to the previous question. If at least k attempts have to be successful, we need

$$\sum_{k=10}^{n}\binom{n}{k}\left(1-\frac{C_{\text{jam}}}{C}\right)^k\left(\frac{C_{\text{jam}}}{C}\right)^{n-k} \geq 0.9.$$

With the given parameters, we have

$$\frac{C_{\text{jam}}}{C} = \frac{2}{5}.$$

For $n = 20$, we have

$$\sum_{k=10}^{n}\binom{n}{k}\left(1-\frac{C_{\text{jam}}}{C}\right)^k\left(\frac{C_{\text{jam}}}{C}\right)^{n-k} \approx 0.8725,$$

and for $n = 21$, we have

$$\sum_{k=10}^{n}\binom{n}{k}\left(1-\frac{C_{\text{jam}}}{C}\right)^k\left(\frac{C_{\text{jam}}}{C}\right)^{n-k} \approx 0.9151.$$

Thus at least 21 attempts have to be made such that the probability of at least k being successful is at least 0.9.

Note that as long as $C_{\text{jam}} < C$, the probability of at least k successful attempts will always exceed any given threshold smaller than 1 if only n is chosen large enough. Thus although the probability of successful transmission in one single step may be small, frequency hopping can serve to transmit an arbitrary number of messages in the presence of a jammer.