

IDENTIFICATION PLUS TRANSMISSION

Te Sun Han
Department of Information Systems
Senshu University
Kawasaki, Japan

Sergio Verdú
Department of Electrical Engineering
Princeton University
Princeton, NJ, USA

Consider the communication problem depicted in the Figure, where there is one transmitter and N receivers. The transmitter desires to reliably transmit information to *one* of the receivers, whose identity is not predetermined. Every potential receiver listens to the noisy channel and must decide whether it is indeed the intended recipient of the message, and if so, it decodes the message sent by the transmitter. This is a very common situation in practical applications such as local-area networks, radio networks, and downlink satellite communication where a common broadcast channel is provided in order for the central station to communicate with the terminals. The central station is required to deliver a sequence of messages, each intended for one of the terminals.

The straightforward solution to the problem posed here is to encode the address of the destination $a \in \{1, \dots, N\}$ in a header followed by a codeword representing the message $m \in \{1, \dots, M\}$. If αn and $(1 - \alpha)n$ symbols are devoted to the transmission of address and message, respectively, then the Shannon theorem ensures that reliable communication is possible if M and N grow with n as

$$\frac{1}{n} \log N \rightarrow \alpha C \quad (1)$$

$$\frac{1}{n} \log M \rightarrow (1 - \alpha)C \quad (2)$$

but not faster, where C is the capacity of the channel. In many applications N is negligible with respect to M , and the header is devoted to a very small fraction α of the transmitted symbols, thereby achieving a growth of M which is essentially given by $\exp(nC)$. Somewhat surprisingly, it turns out that such a rate of information transmission can be sustained even if the amount of information contained in the address is not negligible with respect to the information contained in the message. In fact, it is possible to transmit information at the channel capacity rate as long as the number of bits in the address is equal to the total number of messages.

It is indeed possible to do better than the straightforward strategy of using a separate transmission code for address and message. To see this, first note that each station is interested in finding out whether it is the intended recipient or not; if it is not, then it is not interested in estimating which of the other stations is the intended recipient. Naturally, we immediately recognize from this that an identification code can be used in order to transmit the address. Therefore, Theorem 1 of [1] implies that we can transmit a number of addresses that grows as

$$\frac{1}{n} \log \log N \rightarrow \alpha C. \quad (3)$$

We see that the strategy of juxtaposing an identification code and a transmission code to send address and message respectively, achieves (2) and (3). Therefore, we can achieve

$$\frac{1}{n} \log \log N \rightarrow C \quad (4)$$

if the message transmission rate goes to zero, and

$$\frac{1}{n} \log M \rightarrow C \quad (5)$$

if the address identification rate goes to zero. However, it is possible to achieve (4) and (5) simultaneously by using an Identification + Transmission (IT) code (defined below) where, unlike the aforementioned, address and message are not encoded separately. A decoupled coding strategy is far from optimum because reliable transmission of the message is only required by the intended receiver. Actually, in certain applications a privacy feature may be

desirable whereby any other receiver is unlikely to decode the transmitted message reliably.

Definition An $(n, N, M, \lambda_1, \lambda_2)$ IT code is a mapping $f: \{1, \dots, N\} \times \{1, \dots, M\} \rightarrow A^n$ and a collection of subsets $\{D_{a,m} \subset B^n, a \in \{1, \dots, N\}, m \in \{1, \dots, M\}\}$ such that for all $a = 1, \dots, N$

- 1) $D_{a,m} \cap D_{a,l} = \emptyset$ if $l \neq m$
- 2) $\frac{1}{M} \sum_{m=1}^M W^{(n)}(D_{a,m} | f(a,m)) \geq 1 - \lambda_1$
- 3) $\frac{1}{M} \sum_{m=1}^M W^{(n)}(D_j | f(a,m)) \leq \lambda_2$ if $j \neq a$

where we have used the notation $D_a \triangleq \bigcup_{m=1}^M D_{a,m}$.

The rate-pair of an $(n, N, M, \lambda_1, \lambda_2)$ IT code is $(\frac{1}{n} \log \log N, \frac{1}{n} \log M)$.

Upon reception of the channel output y^n , station a checks whether $y^n \in D_a$. If $y^n \notin D_a$, then the station declares that it is not the intended recipient of the message. If $y^n \in D_a$, then station a searches for the unique (cf. condition 1) $m \in \{1, \dots, M\}$ such that $y^n \in D_{a,m}$ and outputs message m .

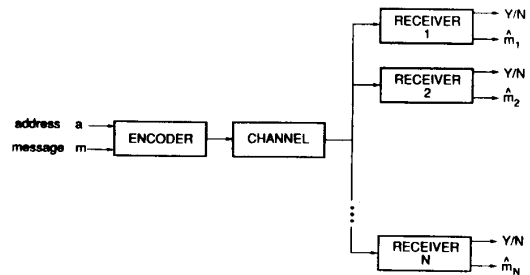
The reliability with which the address is received is equal to the reliability achievable had it been separately encoded with an ID code, whereas the intended recipient decodes the correct message with average probability of error (over the set of equiprobable messages) better than λ_1 . The IT code puts no constraints on the reliability with which unintended stations decode the message.

A very general coding theorem can be proved in this setting: If C is the capacity of the channel, then (C, C) is an achievable IT rate pair, and if (\bar{R}, R) is an achievable IT rate pair then $\bar{R} \leq C$ and $R \leq C$.

This result is shown for any finite-input channel (with any memory structure) using a simple proof. It means that if the central station desires to transmit B bits of information through a noisy channel with capacity C to one of N terminals whose identity is not predetermined, the required number of channel symbols is (asymptotically) $\max\{\log \log N, B\}/C$ rather than the $(\log \log N + B)/C$ symbols that would be required if address and message were separately encoded using an identification and a transmission code respectively.

References

1. R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Information Theory*, vol. IT-35, pp. 15-29, Jan. 1989.



This work was supported by the US Office of Naval Research under Grant N00014-90-J-1734.