

Livrable 3 :

Schéma de la chaine de transmission :

Explication de chaque étape :

Étape 1 : Conversion ASCII-Binaire

Objectif : Cette étape permet de convertir les caractères d'un fichier texte en une suite de données binaires grâce au code ASCII. L'objectif est de rendre les informations compréhensibles par les machines.

Principe de mise en œuvre : Chaque caractère du fichier est associé à une séquence de bits en utilisant la table ASCII. Par exemple, la lettre 'A' correspond à 01000001. On parcourt ainsi tout le fichier pour générer la séquence binaire.

Entrée et sortie : On prend en entrée un fichier texte (par exemple : "Bonjour"), et on obtient en sortie une suite de bits (exemple : 01000010 01101111 01101110 01101010).

Étape 2 : Encodage

Objectif : L'encodage permet d'ajouter une structure aux données binaires afin d'assurer une transmission fiable.

Principe de mise en œuvre : On crée notre propre moyen d'encodage. Un bit sur deux est inversé, en commençant par le premier. C'est à dire qu'un bit sur deux, un 1 devient un 0 et un 0 devient un 1.

Entrée et sortie : L'entrée est une suite binaire brute, et la sortie est une suite encodée (par exemple avec notre encodage : 01000001 devient 11101011).

Étape 3 : Modulation

Objectif : Cette étape permet de transformer les données numériques (suite de 0 et de 1) en un signal analogique continu, nécessaire pour leur transmission sur un canal physique comme un câble. Nous utilisons la modulation AM qui permet de coder ces données numériques en variant l'amplitude du signal porteur, facilitant ainsi la transmission de l'information. Grâce à cette modulation, nous pouvons également dissimuler un message.

Principe de mise en œuvre : Dans cette approche, on utilise la modulation par amplitude (AM) pour encoder les bits. Un bit "0" peut être représenté par une amplitude faible ou nulle de l'onde porteuse, tandis qu'un bit "1" pourrait correspondre à une amplitude plus élevée. Par exemple, pour chaque période de l'onde porteuse, l'amplitude sera ajustée selon la séquence binaire à transmettre, permettant de transformer les données numériques en un signal analogique modulé.

Entrée et sortie : L'entrée est une suite binaire encodée, et la sortie est un signal analogique modulé par amplitude prêt pour la transmission.

Étape 4 : Émetteur (Notre gadget)

Objectif : L'émetteur a pour rôle d'envoyer le signal modulé sur un canal de communication tout en préservant sa qualité.

Principe de mise en œuvre : Il ajuste la puissance du signal et son impédance pour garantir une transmission efficace. Cette étape permet d'éviter que le signal se dégrade lors de son envoi.

Entrée et sortie : L'entrée est un signal analogique modulé, et la sortie est ce signal transmis sur le canal.

Étape 5 : Récepteur (Microphone)

Objectif : Le récepteur récupère le signal transmis et élimine les interférences ou bruits pour le rendre exploitable.

Principe de mise en œuvre : Il amplifie et filtre le signal pour supprimer les perturbations. Cela garantit une meilleure qualité du signal reçu pour la suite du processus.

Entrée et sortie : L'entrée est un signal analogique, et la sortie est le signal analogique.

Étape 6 : Démodulation

Objectif : La démodulation a pour objectif de reconvertir le signal analogique modulé (en AM dans ce cas) en une suite de bits afin de récupérer les données transmises. Elle permet ainsi de comprendre le message dissimulé en retrouvant les données numériques qui ont été envoyées.

Principe de mise en œuvre : Le démodulateur analyse les variations d'amplitude du signal analogique modulé en AM. En détectant les changements d'amplitude, le démodulateur peut traduire ces variations en une séquence de 0 et de 1. Ces variations d'amplitude correspondent aux bits qui ont été encodés lors de la modulation AM, permettant ainsi de reconstruire la suite de données initiales.

Entrée et sortie : L'entrée est le signal analogique propre, et la sortie est une séquence binaire correspondant aux données transmises.

Étape 7 : Décodage

Objectif : Le décodage permet de repasser de notre binaire encodé au binaire vérifié et corrigé.

Principe de mise en œuvre : La méthode d'encodage est connue donc on l'applique de nouveau a notre suite de bits afin de retrouver la suite binaire initiale.

Entrée et sortie : L'entrée est une suite binaire encodée, et la sortie est une suite binaire vérifiée et corrigée.

Étape 8 : Conversion Binaire-ASCII et Écriture dans le Fichier

Objectif : L'objectif de cette étape est de convertir la séquence binaire validée en caractères lisibles à l'aide du code ASCII, qui associe chaque groupe de 8 bits à un symbole spécifique. Une fois la conversion effectuée, les caractères sont organisés pour reformer le contenu initial du fichier texte. Cette étape permet à l'agent de recevoir un texte lisible

Principe de mise en œuvre : Chaque groupe de 8 bits est converti en son caractère ASCII correspondant. Une fois les caractères reconstitués, on obtient à nouveau le fichier initial.

Entrée et sortie : L'entrée est une suite binaire validée, et la sortie est un fichier texte lisible (par exemple, la séquence 01000001 devient la lettre 'A').

Nos choix et nos justifications pour l'envoi d'un message textuel :

Nous avons 3 possibilités avec chacune leurs avantages et leurs inconvénients :

Le message audio avait comme avantage de confirmé l'identité de l'expéditeur mais comme défaut de forcer l'agent à parler, ce qui pourrait le mettre en danger car il pourrait se faire repérer le temps de faire le message audio.

Envoyer **un fichier volumineux** (ici les données volés) avait pour avantage de confirmer que l'agent a mené à bien sa mission et qu'il faut l'aider à s'enfuir, et le fait d'envoyer les données permettait en cas d'échec de l'extraction de l'agent de quand même avoir les données, cette solution avait quand même des défauts car le message mettrait beaucoup plus de temps à être envoyés et serait beaucoup plus facilement repérable.

Envoyer **un message textuel** avait différents avantages tels que la discrétion, le peu d'influence que cela aura sur le réseau et la rapidité d'envoi mais avait pour défaut de ne pas confirmer l'identité de l'agent (si c'est lui ou non qui envoie le message) et si on ne parvient pas à l'extraire de la base ennemie nous n'avons pas les données.

Finalement nous avons choisi le message textuel car ce n'est certes pas le plus efficace pour obtenir les données mais c'est celui qui est le plus rapide, le plus discret et qui garantie le plus la sécurité de l'agent.

La fréquence d'échantillonnage

D'après le théorème de Shannon Nyquist, la fréquence d'échantillonnage f_e doit être au moins égale au double de la fréquence maximale du signal considéré. dans notre cas, on a trouvé dans notre livrable 2 une fréquence propre : $f_0 = 20000 \text{ Hz}$

Donc en utilisant le théorème de Shannon Nyquist on obtient :

$$F_{nyq} > 2 \times f_0$$

$$\Leftrightarrow F_{nyq} > 40000 \text{ hz}$$

$$F_{nyq} = F_e = 44100 \text{ hz} = 44,1 \text{ kHz}$$

$$\Leftrightarrow 44,1 > 40$$

In []:

Processing math: 100%